Streaming Defense Detection Types V5

Aligned to `dpi_risk_scores`

Enhanced Detection Catalog for Hadron and Agentic Investigator API Operations

Document Version	V5
Source Baseline	`dpi_risk_scores`
Prior Document	SD Detection Types V4
Prepared For	Customer, SOC, MSSP and Engineering Review
Prepared By	Streaming Defense / Global Threat Intel LLC
Date	May 11, 2026

Contents

1 Executive Summary

This Version 5 document replaces the older V4 prose-and-score catalog with the current operational source of truth from `dpi_risk_scores`. Each detection now carries the exact current risk identifier, type name, description, severity, total score, client score, server score, operational context, potential impact, and mitigation strategy from the JavaScript catalog. The document also adds platform-specific operating guidance for Hadron and the Agentic Investigator API so that customers, SOC analysts, and engineering teams can understand how the detections are produced, enriched, filtered, correlated, and escalated.

V5 keeps the 61-detection structure of V4, but aligns the final content to the current runtime definitions. This matters because the runtime score and severity are what Hadron injects into normalized HIP/EIP records and what the Agentic Investigator stage uses for gating, clustering, deduplication, campaign detection, and escalation. Where V4 used older labels such as `SDPI_*`, V5 uses the current `DPI_*` and `HADRON_*` type values from the JavaScript source.

2 V5 Alignment Principles

- **JavaScript source of truth:** All detection IDs, names, severities, scores, and context fields are injected from `dpi_risk_scores`.
- **Runtime wording:** Descriptions have been expanded to explain how Hadron enriches records and how the Agentic Investigator API triages, clusters, suppresses, or escalates them.
- **No invented risk IDs:** The document keeps the active ID space from 1 through 61.
- **Operational separation:** Raw DPI risks and Hadron-derived risks are described separately where needed. IDs 57 through 61 represent Streaming Defense enriched detections generated from threat intelligence, cumulative state, fingerprint intelligence, exfiltration heuristics, and fast-flux logic.
- **Analyst usability:** Every detailed detection includes evidence fields, triage guidance, potential impact, and mitigation strategy.

3 Hadron Runtime Alignment

Hadron ingests SD_DPI style UDP flow records, requires a `flow_event_id`, flattens nested `SD_DPI.flow_risk` records into a consistent schema, maps the selected risk through `SD_DPI_risk_scores`, and emits normalized records for AOT visualization and ClickHouse persistence. The normalized records include source and destination addressing, ports, protocol, application protocol, category, host/domain fields, TLS and DNS metadata, ASN/geolocation, asset information, cumulative pair state, risk fields, and threat indicator flags.

Hadron also adds Streaming Defense detections beyond raw SD_DPI flags:

- **Risk 57 - Malicious IP:** produced when the source or destination IP matches the Streaming Defense IP intelligence store.
- **Risk 58 - Malicious Domain:** produced when the observed host or domain matches the Streaming Defense domain intelligence store.
- **Risk 59 - Data Exfiltration:** produced from cumulative flow state when a public destination receives an anomalously large outbound transfer.
- **Risk 60 - Malicious Fingerprint:** produced when JA4/TLS fingerprint intelligence matches known malicious infrastructure or tooling.
- **Risk 61 - Fast Flux:** produced from DNS TTL and domain-to-IP churn behavior consistent with fast-flux hosting.

4 Agentic Investigator API Runtime Alignment

The Agentic Investigator API receives Hadron/AOT events, applies edge gates, deduplication, allowlists, neighbor clustering, and playbook-specific logic. The universal playbook handles the majority of risk IDs. Specialized handling exists for probing, malware infrastructure, sequence correlation, and dynamic allowlist proposal/approval.

Key operational behaviors reflected in this document:

- **Edge gating:** Risk IDs 1 through 61 are allowed by policy, with global score-based bypass for high-scoring records. Selected weak or noisy risks can require supporting fields such as host name or user agent.

- **Neighbor analysis:** The universal playbook checks CIDR neighbors and escalates when local clustering suggests campaign or scanning behavior rather than a single isolated flow.
- **Probing expansion:** Probing Attempt (55) can be expanded into vertical port scan, fan-out/lateral probing, and persistence analysis.
- **Malware infrastructure:** Malware and intelligence-driven risks such as 53, 57, 58, and 61 are treated as malware/C2 infrastructure candidates and can be escalated based on infected host fan-in.
- **Sequence correlation:** The configured attack chain patterns include sequences such as probing, RCE, binary transfer, DGA or malicious domain contact, and data exfiltration.
- **Dynamic allowlists:** CIDR and risk-scoped domain suffix allowlists can be proposed, approved, refreshed, and applied without changing the detection catalog.

5 Detection Score Summary

Severity	Count	Score Range	Operational Interpretation
High / Severe	7	100	High-confidence threat or policy violation. Escalate when not already explained.
Medium	34	50-75	Triage with context, recurrence, asset criticality, and neighbor clusters.
Low	13	10-10	Weak signal. Correlate before escalation unless tied to critical assets or attack chain.

6 Detection Family Matrix

Family	Coverage	Count	Primary Runtime Relevance
Web Application and Content Attacks	1, 2, 3, 4, 11, 13, 14, 25, 40, 44, 47, 54	12	HTTP URL, user agent, header, content, exploit and binary transfer evidence; often validated against HTTP context in Hadron.
TLS, SSH, Encryption and Certificate Posture	6, 7, 8, 9, 10, 15, 18, 19, 21, 22, 24, 31, 32, 33, 34, 51, 52, 56	18	TLS/QUIC/SSH version, cipher, SNI, ALPN, certificate and fingerprint evidence preserved in normalized HIP records.
DNS, Domains, C2 and Resolution Anomalies	12, 16, 23, 27, 37, 38, 42, 58, 61	9	DNS, hostname, domain, response address and fast-flux evidence; Agentic Investigator can require host fields for selected risks.
Network Reconnaissance, Flow Behavior and Transport Anomalies	5, 17, 30, 35, 46, 48, 49, 50, 55, 59	10	Port, packet, byte, duration, cumulative occurrence and neighbor analysis evidence.
Threat Intelligence and Malware Infrastructure	26, 28, 29, 36, 45, 53, 57, 60	8	Streaming Defense TIP, malicious host/domain/fingerprint, malware infrastructure and campaign fan-in analysis.

7 V5 Detection Matrix

ID	Type	Description	Severity	Total	Client	Server	Family
1	DPI_URL_POSSIBLE_XSS	XSS Attack	Severe	100	75	25	Web Application and Content Attacks
2	DPI_URL_POSSIBLE_SQL_INJECTION	SQL Injection	Severe	100	75	25	Web Application and Content Attacks
3	DPI_URL_POSSIBLE_RCE_INJECTION	RCE Injection	Severe	100	75	25	Web Application and Content Attacks
4	DPI_BINARY_APPLICATION_TRANSFER	Binary App Transfer	Severe	100	50	50	Web Application and Content Attacks
5	DPI_KNOWN_PROTOCOL_ON_NON_STANDARD_PORT	Known Proto on Non Std Port	Medium	50	25	25	Network Reconnaissance, Flow Behavior and Transport Anomalies
6	DPI_TLS_SELFSIGNED_CERTIFICATE	Self-signed Cert	Medium	75	50	25	TLS, SSH, Encryption and Certificate Posture
7	DPI_TLS_OBSOLETE_VERSION	Obsolete TLS (v1.1 or older)	Medium	75	50	25	TLS, SSH, Encryption and Certificate Posture
8	DPI_TLS_WEAK_CIPHER	Weak TLS Cipher	Medium	75	50	25	TLS, SSH, Encryption and Certificate Posture
9	DPI_TLS_CERTIFICATE_EXPIRED	TLS Cert Expired	Medium	75	10	65	TLS, SSH, Encryption and Certificate Posture
10	DPI_TLS_CERTIFICATE_MISMATCH	TLS Cert Mismatch	Medium	75	10	65	TLS, SSH, Encryption and Certificate Posture
11	DPI_HTTP_SUSPICIOUS_USER_AGENT	HTTP Susp User-Agent	Medium	50	35	15	Web Application and Content Attacks
12	DPI_NUMERIC_IP_HOST	HTTP/TLS/QUIC Numeric Hostname/SNI	Low	10	5	5	DNS, Domains, C2 and Resolution Anomalies
13	DPI_HTTP_SUSPICIOUS_URL	HTTP Susp URL	Medium	50	35	15	Web Application and Content Attacks
14	DPI_HTTP_SUSPICIOUS_HEADER	HTTP Susp Header	Medium	50	35	15	Web Application and Content Attacks
15	DPI_TLS_NOT_CARRYING_HTTPS	TLS (probably) Not Carrying HTTPS	Low	10	5	5	TLS, SSH, Encryption and Certificate Posture
16	DPI_SUSPICIOUS_DGA_DOMAIN	Susp DGA Domain name	Medium	50	35	15	DNS, Domains, C2 and Resolution Anomalies
17	DPI_MALFORMED_PACKET	Malformed Packet	Low	10	5	5	Network Reconnaissance, Flow Behavior and Transport Anomalies
18	DPI_SSH_OBSOLETE_CLIENT_VERSION_OR_CIPHER	SSH Obsolete Cli Vers/Cipher	High	100	90	10	TLS, SSH, Encryption and Certificate Posture
19	DPI_SSH_OBSOLETE_SERVER_VERSION_OR_CIPHER	SSH Obsolete Ser Vers/Cipher	Medium	50	5	45	TLS, SSH, Encryption and Certificate Posture
20	DPI_SMB_INSECURE_VERSION	SMB Insecure Vers	High	100	90	10	General Network Risk
21	DPI_TLS_SUSPICIOUS_ESNI_USAGE	TLS Susp ESNI Usage	Medium	50	25	25	TLS, SSH, Encryption and Certificate Posture

Continued on next page

ID	Type	Description	Severity	Total	Client	Server	Family
22	DPI_TLS_SUSPICIOUS_ESNI_USAGE	Unsafe Protocol	Low	10	5	5	TLS, SSH, Encryption and Certificate Posture
23	DPI_DNS_SUSPICIOUS_TRAFFIC	Susp DNS Traffic	Medium	50	45	5	DNS, Domains, C2 and Resolution Anomalies
24	DPI_TLS_MISSING_SNI	Missing SNI TLS Extn	Medium	50	25	25	TLS, SSH, Encryption and Certificate Posture
25	DPI_HTTP_SUSPICIOUS_CONTENT	HTTP Susp Content	Medium	50	35	15	Web Application and Content Attacks
26	DPI_RISKY_ASN	Risky ASN	Medium	50	25	25	Threat Intelligence and Malware Infrastructure
27	DPI_RISKY_DOMAIN	Risky Domain Name	Medium	50	25	25	DNS, Domains, C2 and Resolution Anomalies
28	DPI_MALICIOUS_FINGERPRINT	Malicious Fingerpint	Medium	50	25	25	Threat Intelligence and Malware Infrastructure
29	DPI_MALICIOUS_SHA1_CERTIFICATE	Malicious SSL Cert/SHA1 Fingerp.	Medium	50	25	25	Threat Intelligence and Malware Infrastructure
30	DPI_DESKTOP_OR_FILE_SHARING_SESSION	Desktop/File Sharing	Low	10	5	5	Network Reconnaissance, Flow Behavior and Transport Anomalies
31	DPI_TLS_UNCOMMON_ALPN	Uncommon TLS ALPN	Medium	50	25	25	TLS, SSH, Encryption and Certificate Posture
32	DPI_TLS_CERT_VALIDITY_TOO_LONG	TLS Cert Validity Too Long	Medium	50	25	25	TLS, SSH, Encryption and Certificate Posture
33	DPI_TLS_SUSPICIOUS_EXTENSION	TLS Susp Extn	Medium	50	35	15	TLS, SSH, Encryption and Certificate Posture
34	DPI_TLS_FATAL_ALERT	TLS Fatal Alert	Low	10	5	5	TLS, SSH, Encryption and Certificate Posture
35	DPI_SUSPICIOUS_ENTROPY	Susp Entropy	Low	10	5	5	Network Reconnaissance, Flow Behavior and Transport Anomalies
36	DPI_CLEAR_TEXT_CREDENTIALS	Clear-Text Credentials	High	100	90	10	Threat Intelligence and Malware Infrastructure
37	DPI_DNS_LARGE_PACKET	Large DNS Packet (512+ bytes)	Medium	50	25	25	DNS, Domains, C2 and Resolution Anomalies
38	DPI_DNS_FRAGMENTED	Fragmented DNS Message	Medium	50	25	25	DNS, Domains, C2 and Resolution Anomalies
39	DPI_INVALID_CHARACTERS	Non-Printable/Invalid Chars Detected	Medium	50	35	15	General Network Risk
40	DPI_POSSIBLE_EXPLOIT	Possible Exploit Attempt	Severe	100	75	25	Web Application and Content Attacks
41	DPI_TLS_CERTIFICATE_ABOUT_TO_EXPIRE	TLS Cert About To Expire	Medium	50	5	45	General Network Risk
42	DPI_PUNYCODE_IDN	IDN Domain Name	Low	10	1	9	DNS, Domains, C2 and Resolution Anomalies
43	DPI_ERROR_CODE_DETECTED	Error Code	Low	10	1	9	General Network Risk
44	DPI_HTTP_CRAWLER_BOT	Crawler/Bot	Low	10	1	9	Web Application and Content Attacks

Continued on next page

ID	Type	Description	Severity	Total	Client	Server	Family
45	DPI_ANONYMOUS_SUBSCRIBER	Anonymous Subscriber	Medium	50	25	25	Threat Intelligence and Malware Infrastructure
46	DPI_UNIDIRECTIONAL_TRAFFIC	Unidirectional Traffic	Low	10	5	5	Network Reconnaissance, Flow Behavior and Transport Anomalies
47	DPI_HTTP_OBSOLETE_SERVER	HTTP Obsolete Server	Medium	50	5	45	Web Application and Content Attacks
48	DPI_PERIODIC_FLOW	Periodic Flow	Low	10	1	9	Network Reconnaissance, Flow Behavior and Transport Anomalies
49	DPI_MINOR_ISSUES	Minor Issues	Low	10	1	9	Network Reconnaissance, Flow Behavior and Transport Anomalies
50	DPI_MINOR_ISSUES	TCP Connection Issues	Medium	50	25	25	Network Reconnaissance, Flow Behavior and Transport Anomalies
51	DPI_FULLY_ENCRYPTED	Fully Encrypted Flow	Medium	50	25	25	TLS, SSH, Encryption and Certificate Posture
52	DPI_TLS_ALPN_SNI_MISMATCH	ALPN/SNI Mismatch	Medium	50	25	25	TLS, SSH, Encryption and Certificate Posture
53	DPI_MALWARE_HOST_CONTACTED	Client Contacted A Malware Host	Severe	100	75	25	Threat Intelligence and Malware Infrastructure
54	DPI_BINARY_DATA_TRANSFER	Binary File/Data Transfer (Attempt)	Medium	50	25	25	Web Application and Content Attacks
55	DPI_PROBING_ATTEMPT	Probing Attempt	Medium	50	25	25	Network Reconnaissance, Flow Behavior and Transport Anomalies
56	DPI_OBFUSCATED_TRAFFIC	Obfuscated Traffic	Medium	50	35	15	TLS, SSH, Encryption and Certificate Posture
57	HADRON_MALICIOUS_IP_DETECTED	Malicious IP Detected in Network	High	100	25	75	Threat Intelligence and Malware Infrastructure
58	HADRON_MALICIOUS_DOMAIN_DETECTED	Malicious Domain Detected in Network	High	100	25	75	DNS, Domains, C2 and Resolution Anomalies
59	HADRON_DATA_EXFILTRATION	Data Exfiltration	High	100	25	75	Network Reconnaissance, Flow Behavior and Transport Anomalies
60	HADRON_MALICIOUS_FINGERPRINT_DETECTED	Malicious Fingerprint Detected in Network	High	100	25	75	Threat Intelligence and Malware Infrastructure
61	HADRON_FAST_FLUX_DETECTED	Fast Flux Operation Detected	Severe	100	25	75	DNS, Domains, C2 and Resolution Anomalies

8 Detailed V5 Detection Catalog

The following entries are generated from the current JavaScript risk catalog and then expanded with Hadron and Agentic Investigator API operating semantics.

8.1 1. XSS Attack

Risk ID: 1
Runtime Type: `DPI_URL_POSSIBLE_XSS`
Severity and Score: Severe / total 100 / client 75 / server 25
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

Suspicious URLs containing script tags or HTML injections.

Enhanced Description

Identifies potential Cross-Site Scripting (XSS) attacks in URLs or form inputs. Attackers inject malicious scripts into webpages, potentially compromising user sessions or altering site content. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Session hijacking or credential theft.
- Unauthorized modification of website functionality.
- Data leakage or redirection to malicious pages.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Preserve URL, user agent, server endpoint, and any web gateway logs. Confirm whether the targeted service was exposed, patched, and protected by WAF policy.

Mitigation Strategies

- Input Validation/Output Encoding: Sanitize user inputs and encode outputs.
- Content Security Policy (CSP): Limit the sources from which scripts can be loaded.
- Secure Coding Practices: Regularly audit and update web application code.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.2 2. SQL Injection

Risk ID: 2
Runtime Type: `DPI_URL_POSSIBLE_SQL_INJECTION`
Severity and Score: Severe / total 100 / client 75 / server 25
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

HTTP requests containing suspicious database queries or special characters (' OR 1=1, etc.).

Enhanced Description

Flags possible SQL Injection attempts. Attackers manipulate queries to gain unauthorized database access or modify stored data. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Theft or corruption of sensitive database records.
- Complete compromise of web applications.
- Potential lateral movement into other systems.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Preserve URL, user agent, server endpoint, and any web gateway logs. Confirm whether the targeted service was exposed, patched, and protected by WAF policy.

Mitigation Strategies

- Parameterized Queries: Use prepared statements to avoid direct string concatenation.
- WAF Rules: Deploy a Web Application Firewall to filter malicious payloads.
- Regular Code Reviews: Identify insecure database calls or unsanitized inputs.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.3 3. RCE Injection

Risk ID: 3
Runtime Type: `DPI_URL_POSSIBLE_RCE_INJECTION`
Severity and Score: Severe / total 100 / client 75 / server 25
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

HTTP payloads or parameters that include OS-level commands or scripts.

Enhanced Description

Indicates attempts at Remote Code Execution (RCE) through unsanitized user input or vulnerable endpoints. Attackers can execute arbitrary commands on the server. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Participates in sequence correlation. Current configured sequences include reconnaissance followed by RCE, binary transfer, DGA or malicious-domain contact, and exfiltration. This makes the risk more important when it appears as part of a multi-step attack chain.

Potential Impact

- Full control of the affected server.

- Data exfiltration and service disruption.
- Rapid lateral spread within the network.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Preserve URL, user agent, server endpoint, and any web gateway logs. Confirm whether the targeted service was exposed, patched, and protected by WAF policy.

Mitigation Strategies

- Secure Coding: Block system calls or employ strict input validation.
- Least Privilege: Minimize permissions for critical services.
- Patch Management: Update vulnerable frameworks or libraries promptly.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.4 4. Binary App Transfer

Risk ID: 4
Runtime Type: `DPI_BINARY_APPLICATION_TRANSFER`
Severity and Score: Severe / total 100 / client 50 / server 50
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

Downloading/uploading .exe, .apk, or similar binary files over HTTP.

Enhanced Description

Monitors network traffic for the transfer of executable applications. Such files can contain malware or be used for unauthorized software deployment. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Participates in sequence correlation. Current configured sequences include reconnaissance followed by RCE, binary transfer, DGA or malicious-domain contact, and exfiltration. This makes the risk more important when it appears as part of a multi-step attack chain.

Potential Impact

- Introduction of malicious software (e.g., ransomware).
- Inadvertent distribution of unverified code to endpoints.
- Potential compromise of internal systems.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Strict File Checks: Scan all inbound/outbound binaries for malware signatures.
- Access Control: Limit who can transfer or execute binaries on the network.
- Application Whitelisting: Only allow approved binaries to run on critical systems.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.5 5. Known Proto on Non Std Port

Risk ID: 5
Runtime Type: `DPI_KNOWN_PROTOCOL_ON_NON_STANDARD_PORT`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Standard protocols (e.g., HTTP, SSH) running on custom port numbers like 1234 or 8081.

Enhanced Description

Indicates that a recognized protocol is operating on an unusual or non-default port, potentially used to bypass firewalls or hide malicious traffic. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Circumventing of established port-based security policies.
- Hidden channels for malware or exfiltration.
- Decreased visibility and monitoring effectiveness.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Port Policy Enforcement: Restrict protocols to standard ports.
- Firewall/IDS Updates: Monitor and block unexpected port usage.
- Regular Audits: Verify that each service adheres to proper port assignments.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.6 6. Self-signed Cert

Risk ID: 6
Runtime Type: `DPI_TLS_SELFSIGNED_CERTIFICATE`
Severity and Score: Medium / total 75 / client 50 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS certificates not issued by a recognized certificate authority (CA).

Enhanced Description

Identifies the use of self-signed certificates in TLS traffic. While legitimate in testing or internal use, such certificates can also be leveraged for man-in-the-middle attacks if improperly used. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as

TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Susceptibility to spoofing or impersonation.
- Reduced trust in SSL/TLS connections.
- Potential data interception or tampering.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Certificate Validation: Use certificates from trusted CAs.
- Pinning and Monitoring: Confirm certificates match known fingerprints.
- Audit TLS Configurations: Ensure self-signed certs are only used where absolutely necessary.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.7 7. Obsolete TLS (v1.1 or older)

Risk ID: 7
Runtime Type: `DPI_TLS_OBSOLETE_VERSION`
Severity and Score: Medium / total 75 / client 50 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS handshake messages indicating SSLv3, TLS 1.0, or TLS 1.1 usage.

Enhanced Description

Alerts on outdated TLS/SSL protocol versions that have known cryptographic weaknesses and are susceptible to advanced attacks. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Exposure to protocol-specific exploits.
- Compromised secure sessions, allowing attackers to decrypt data.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Upgrade to TLS 1.2 or 1.3: Disable older protocol versions.

- Server Hardening: Ensure backward compatibility is limited or removed.
- Regular Testing: Use SSL/TLS scanners to verify only secure versions are in use.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.8 8. Weak TLS Cipher

Risk ID: 8
Runtime Type: `DPI_TLS_WEAK_CIPHER`
Severity and Score: Medium / total 75 / client 50 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS sessions negotiated with outdated ciphers like RC4, MD5, or other known-weak algorithms.

Enhanced Description

Detects the use of weak or deprecated encryption ciphers that can be cracked or exploited, undermining data confidentiality. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Easier decryption of intercepted traffic.
- Potential data manipulation or session hijacking.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Enforce Strong Cipher Suites: Disable weak cryptographic algorithms.
- Regular Cipher Audits: Align configurations with industry best practices.
- Patch & Update: Keep SSL libraries current (e.g., OpenSSL).

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.9 9. TLS Cert Expired

Risk ID: 9
Runtime Type: `DPI_TLS_CERTIFICATE_EXPIRED`
Severity and Score: Medium / total 75 / client 10 / server 65
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Certificates where the current date exceeds the valid until field.

Enhanced Description

Indicates the use of an expired certificate during a TLS session. This undermines the chain of trust and can be exploited in MitM scenarios. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Connection failures or warnings to end users.
- Potential interception or session hijacking.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Certificate Lifecycle Management: Track and renew expiring certs promptly.
- Auto-Renewal: Automate renewal processes for critical services.
- Enforce Policy: Disallow the use of lapsed certificates in production.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.10 10. TLS Cert Mismatch

Risk ID: 10
Runtime Type: `DPI_TLS_CERTIFICATE_MISMATCH`
Severity and Score: Medium / total 75 / client 10 / server 65
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

A certificates common name (CN) or subject alternative name (SAN) doesnt match the actual host.

Enhanced Description

Flags inconsistencies between a TLS certificate and the domain or hostname in use. Often indicates misconfigurations or malicious redirection. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Triggering browser security alerts or client refusal to connect.
- Potential for man-in-the-middle attacks.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Accurate Certificate Deployment: Ensure CN/SAN fields match intended hosts.
- Certificate Pinning: Bind certificates to specific domains to detect mismatches.
- Regular Monitoring: Alert on any unapproved certificate changes.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.11 11. HTTP Susp User-Agent

Risk ID: 11
Runtime Type: `DPI_HTTP_SUSPICIOUS_USER_AGENT`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

Automated bots with abnormal strings or embedded code in the User-Agent header.

Enhanced Description

Monitors suspicious or malformed User-Agent headers in HTTP. Often indicates botnet traffic, scraping tools, or malicious scanning software. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Unauthorized data harvesting or reconnaissance.
- Targeted exploitation attempts by custom-coded bots.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- User-Agent Filtering: Block known malicious agents.
- Behavioral Analysis: Detect anomalies in HTTP usage patterns.
- Log & Inspect: Investigate unexpected User-Agent strings promptly.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.12 12. HTTP/TLS/QUIC Numeric Hostname/SNI

Risk ID: 12
Runtime Type: `DPI_NUMERIC_IP_HOST`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

Clients connecting via raw IP addresses (e.g., http://192.168.1.10/) instead of domain names.

Enhanced Description

Flags usage of numeric hostnames or SNI fields. This may indicate attempts to bypass DNS-based filtering or obfuscate traffic. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron preserves DNS and hostname context, including query/answer counts, response type, reply code, response addresses, host_name, and domain_name. Agentic Investigator can require host fields for DGA-class events to reduce weak-signal false positives.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Reduced visibility in domain-based blocking tools.
- Potential malicious communications that evade standard DNS controls.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- DNS Enforcement: Require valid domain usage.
- Firewall Rules: Inspect numeric IP host connections more rigorously.
- Monitoring: Watch for repetitive numeric connections indicating possible stealth activities.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0.`

8.13 13. HTTP Susp URL

Risk ID: 13
Runtime Type: `DPI_HTTP_SUSPICIOUS_URL`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

URLs with embedded escape sequences, abnormal parameters, or hidden encodings.

Enhanced Description

Identifies suspicious or potentially malicious URLs within HTTP requests, often used for phishing, drive-by downloads, or exploit attempts. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Redirection to sites hosting malware.
- Credential theft via phishing pages.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- URL Filtering/Reputation: Compare URLs against threat intel.
- Content Analysis: Block or inspect encoded or obfuscated URLs.
- User Education: Promote awareness around unexpected or odd-looking links.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.14 14. HTTP Susp Header

Risk ID: 14
Runtime Type: `DPI_HTTP_SUSPICIOUS_HEADER`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

Headers containing strange keys like X-Osname, X-TLS_Version or unexpected user-defined fields.

Enhanced Description

Monitors for anomalies in HTTP headers that deviate from standard usage. May reveal attempts to inject commands or exfiltrate data. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Data leakage or injection attacks.
- Potential bypass of typical security filters.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Header Validation: Strictly parse and validate allowed headers.
- Security Tools: Use WAF/IDS to detect abnormal header usage.

- Regular Audits: Cross-check suspicious headers in logs.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.15 15. TLS (probably) Not Carrying HTTPS

Risk ID: 15
Runtime Type: `DPI_TLS_NOT_CARRYING_HTTPS`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS sessions that carry encrypted traffic not associated with normal HTTPS web browsing (e.g., VPN-like tunnels).

Enhanced Description

Detects encrypted channels over TLS not serving the standard HTTP(S). Could indicate custom encryption, tunneling, or alternative protocols. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Obscured traffic flows hamper security visibility.
- Potential malicious exfiltration hidden in TLS streams.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Deep Packet Inspection: Identify application-layer data.
- Whitelist Known Services: Restrict TLS usage to known ports/protocols.
- Monitor for Abuse: Flag repeated or high-volume non-HTTPS TLS flows.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.16 16. Susp DGA Domain name

Risk ID: 16
Runtime Type: `DPI_SUSPICIOUS_DGA_DOMAIN`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

Domains with randomized strings (e.g., aj9q2b1l4.com) commonly generated by malware.

Enhanced Description

Identifies Domain Generation Algorithm (DGA) domains often used by botnets to circumvent static blocking lists. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron preserves DNS and hostname context, including query/answer counts, response type, reply code, response addresses, host_name, and domain_name. Agentic Investigator can require host fields for DGA-class events to reduce weak-signal false positives.

Agentic Investigator API Handling

Participates in sequence correlation. Current configured sequences include reconnaissance followed by RCE, binary transfer, DGA or malicious-domain contact, and exfiltration. This makes the risk more important when it appears as part of a multi-step attack chain. Subject to neighbor and benign-cluster suppression tuning. Agentic Investigator can raise thresholds or suppress known-good provider domains where the raw signal is common in large CDNs or software update ecosystems.

Potential Impact

- Sustained malware command and control communications.
- Evasion of typical domain-based defenses.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on host_name, domain_name, DNS response addresses, recurrence, and internal sources. Review DNS resolver logs and block/sinkhole when confirmed malicious.

Mitigation Strategies

- Threat Intelligence Feeds: Block known DGA patterns.
- DNS Sinkholing: Redirect suspicious domains to safe endpoints.
- Behavioral Analysis: Correlate DGA usage with other suspicious signals.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0.`

8.17 17. Malformed Packet

Risk ID: 17
Runtime Type: `DPI_MALFORMED_PACKET`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Packets with invalid headers, truncated data, or unrecognized protocol fields.

Enhanced Description

Flags traffic that doesnt conform to standard protocol formats. May be caused by misconfigurations or intentional fuzzing by attackers. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Disruption of normal communication.
- Potential discovery of unpatched vulnerabilities.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Packet Inspection Tools: Filter or drop malformed traffic.
- Network Logging: Investigate recurring anomalies.
- Apply Latest Patches: Ensure services can gracefully handle invalid packets.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.18 18. SSH Obsolete Cli Vers/Cipher

Risk ID: 18
Runtime Type: `DPI_SSH_OBSOLETE_CLIENT_VERSION_OR_CIPHER`
Severity and Score: High / total 100 / client 90 / server 10
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

SSH client negotiates older protocol versions (e.g., SSH-1) or uses deprecated ciphers (DES, 3DES).

Enhanced Description

Alerts when an SSH client relies on legacy protocol versions or weak encryption, exposing sessions to compromise. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Easier brute-force or MitM attacks.
- Possible unauthorized remote access.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Update SSH Clients: Enforce modern SSH versions (SSH-2).
- Disable Weak Ciphers: Restrict or remove outdated cipher sets.
- Hardening Policies: Regularly audit client/server SSH configs.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.19 19. SSH Obsolete Ser Vers/Cipher

Risk ID: 19
Runtime Type: `DPI_SSH_OBSOLETE_SERVER_VERSION_OR_CIPHER`
Severity and Score: Medium / total 50 / client 5 / server 45
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Server-side usage of SSH v1 or known-weak ciphers.

Enhanced Description

Indicates the SSH server is configured with obsolete protocol versions or ciphers, leaving it open to known exploits. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Malicious sessions hijacking.
- Potential data theft or lateral movement.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Server Upgrades: Enforce SSH-2 and modern crypto.
- Regular Patch Cycles: Address documented vulnerabilities.
- Harden Configuration: Disable older SSH options in /etc/ssh/sshd_config.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.20 20. SMB Insecure Vers

Risk ID: 20
Runtime Type: `DPI_SMB_INSECURE_VERSION`
Severity and Score: High / total 100 / client 90 / server 10
Detection Family: General Network Risk

Observed Pattern or Example

Use of SMBv1 or other deprecated SMB protocol versions.

Enhanced Description

Flags usage of outdated SMB versions with well-known vulnerabilities (e.g., EternalBlue). In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Rapid spread of ransomware (e.g., WannaCry).
- Exposure of file shares and sensitive data.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Disable SMBv1: Enforce SMBv2 or SMBv3 on all systems.
- Patch Windows Servers: Regularly apply critical updates.
- Network Segmentation: Limit SMB traffic to internal subnets only.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.21 21. TLS Susp ESNI Usage

Risk ID: 21
Runtime Type: `DPI_TLS_SUSPICIOUS_ESNI_USAGE`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Encrypted SNI usage that deviates from typical patterns, possibly used to hide malicious domain connections.

Enhanced Description

Detects suspicious usage of Encrypted Server Name Indication (ESNI). While ESNI can preserve privacy, unusual patterns might indicate an attempt to evade monitoring. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Reduced visibility into target domains.
- Potential for hidden malicious communications.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Behavioral Monitoring: Correlate ESNI usage with other traffic indicators.
- Advanced TLS Inspection: Analyze encrypted handshake metadata.
- Threat Intelligence: Flag ESNI usage known to be exploited by attackers.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.22 22. Unsafe Protocol

Risk ID: 22
Runtime Type: `DPI_TLS_SUSPICIOUS_ESNI_USAGE`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Encrypted SNI usage that deviates from typical patterns, possibly used to hide malicious domain connections.

Enhanced Description

Detects suspicious usage of Encrypted Server Name Indication (ESNI). While ESNI can preserve privacy, unusual patterns might indicate an attempt to evade monitoring. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Reduced visibility into target domains.
- Potential for hidden malicious communications.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Behavioral Monitoring: Correlate ESNI usage with other traffic indicators.
- Advanced TLS Inspection: Analyze encrypted handshake metadata.
- Threat Intelligence: Flag ESNI usage known to be exploited by attackers.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.23 23. Susp DNS Traffic

Risk ID: 23
Runtime Type: `DPI_DNS_SUSPICIOUS_TRAFFIC`
Severity and Score: Medium / total 50 / client 45 / server 5
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

DNS lookups returning unexpected record types or containing very long subdomain strings.

Enhanced Description

Signals anomalous DNS queries or responses. May be used for DNS tunneling or malicious communications. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron preserves DNS and hostname context, including query/answer counts, response type, reply code, response addresses, host_name, and domain_name. Agentic Investigator can require host fields for DGA-class events to reduce weak-signal false positives.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Covert data exfiltration.
- Malware command and control via DNS.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on host_name, domain_name, DNS response addresses, recurrence, and internal sources. Review DNS resolver logs and block/sinkhole when confirmed malicious.

Mitigation Strategies

- DNS Monitoring: Inspect queries for abnormal patterns.
- Block Known Malicious Domains: Use up-to-date threat intel.
- Limit Allowed Record Types: Deny rarely used or obsolete DNS records.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0.`

8.24 24. Missing SNI TLS Extn

Risk ID: 24
Runtime Type: `DPI_TLS_MISSING_SNI`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS connections where the client omits the Server Name Indication extension.

Enhanced Description

Absence of SNI can hinder host-based policies and sometimes indicates traffic obfuscation or older client implementations. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Difficulty applying virtual host routing or SSL policies.
- Potential evasion of security filters reliant on SNI.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Enforce SNI: Require modern TLS client configurations.
- Deep Packet Inspection: Investigate repeated missing SNI traffic.
- Correlation: Check for other suspicious TLS traits.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.25 25. HTTP Susp Content

Risk ID: 25
Runtime Type: `DPI_HTTP_SUSPICIOUS_CONTENT`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

HTTP header states text/html but the actual payload is binary or heavily obfuscated.

Enhanced Description

Identifies mismatches or anomalies in HTTP content type. Attackers often mislabel or obfuscate harmful payloads to slip past basic checks. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Hidden malware downloads.
- Drive-by exploit attempts.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Content Inspection: Validate that content matches declared MIME types.
- AV/Anti-Malware: Scan suspicious binaries or scripts in transit.
- Security Gateways: Enforce strict filtering on mismatched content.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.26 26. Risky ASN

Risk ID: 26
Runtime Type: `DPI_RISKY_ASN`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

Traffic routed through autonomous systems known for malicious hosting or frequent abuse reports.

Enhanced Description

Flags connections to or from ASNs with documented cybercriminal activity (spam, phishing, malware distribution). In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Increased risk of encountering malware or exploit kits.
- Potential for data exfiltration or fraudulent transactions.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- ASN-Based Blocking: Integrate threat intelligence on high-risk ASNs.
- Monitor Traffic: Investigate repeated connections to suspicious ASNs.
- Network Segmentation: Restrict outbound traffic to known-good networks.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.27 27. Risky Domain Name

Risk ID: 27
Runtime Type: `DPI_RISKY_DOMAIN`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

Domains flagged by threat intelligence as malicious (e.g., phishing, malware hosting).

Enhanced Description

Detects domain names identified as risky due to prior malicious campaigns or compromise. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron preserves DNS and hostname context, including query/answer counts, response type, reply code, response addresses, host_name, and domain_name. Agentic Investigator can require host fields for DGA-class events to reduce

weak-signal false positives.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Phishing, credential theft, or data breaches.
- Potential for malware downloads.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- DNS Filtering: Block or closely monitor known malicious domains.
- User Education: Train employees to avoid suspicious links.
- Threat Intel Feeds: Continuously update blocklists.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0.`

8.28 28. Malicious Fingerpint

Risk ID: 28
Runtime Type: `DPI_MALICIOUS_FINGERPRINT`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

TLS JA3 fingerprints matching known malware or intrusion campaigns.

Enhanced Description

Indicates cryptographic signatures (fingerprints) associated with malicious software or threat actor tooling. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Compromised systems or infiltration by known malicious variants.
- Stealthy persistent threats.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Signature-Based Detection: Block or quarantine traffic matching malicious fingerprints.
- Endpoint Protection: Inspect logs for known fingerprinting tools.
- Continuous Updates: Incorporate new fingerprints from threat intel sources.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.29 29. Malicious SSL Cert/SHA1 Fingerp.

Risk ID: 29
Runtime Type: `DPI_MALICIOUS_SHA1_CERTIFICATE`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

Certificates flagged by SHA1 hashes known to be used by malware or fraudulent sites.

Enhanced Description

Identifies SSL certs (by SHA1 hash) on blocklists or recognized as malicious. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Man-in-the-middle attacks or impersonation of legitimate services.
- Degraded trust in secure communications.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Certificate Reputation: Check certs against known-bad lists.
- Enforce Strong Hashing: Avoid SHA1-based certificates.
- Revoke & Replace: Promptly eliminate compromised certs.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.30 30. Desktop/File Sharing

Risk ID: 30
Runtime Type: `DPI_DESKTOP_OR_FILE_SHARING_SESSION`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Traffic from tools like RDP, VNC, TeamViewer, or SMB file sharing sessions.

Enhanced Description

Monitors sessions that allow remote control or file access. Unauthorized usage may indicate data exfiltration or lateral movement. In operations, this is normally a context signal. It becomes more important when paired with suspicious

domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Theft of intellectual property or sensitive data.
- Deployment of ransomware or unauthorized software.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Access Controls: Restrict remote desktop/file sharing to authorized users.
- Logging & Alerts: Monitor for unusual session durations or file transfer volumes.
- Network Segmentation: Isolate critical systems from broad RDP/SMB access.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.31 31. Uncommon TLS ALPN

Risk ID: 31
Runtime Type: `DPI_TLS_UNCOMMON_ALPN`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS negotiations referencing unexpected protocols (e.g., non-HTTP ALPN strings).

Enhanced Description

Flags unusual Application-Layer Protocol Negotiation values that may mask non-standard or tunneled traffic. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Concealed malicious data streams.
- Bypass of standard security controls.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- ALPN Whitelisting: Allow only known/legitimate protocol identifiers.
- Advanced TLS Inspection: Investigate anomalies in handshake parameters.
- Regular Auditing: Align allowed ALPN with organizational policy.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.32 32. TLS Cert Validity Too Long

Risk ID: 32
Runtime Type: `DPI_TLS_CERT_VALIDITY_TOO_LONG`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Certificates valid far beyond recommended periods (e.g., multi-year validity).

Enhanced Description

Excessive certificate lifespans can increase risk if a cert is compromised and not reissued promptly. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Extended window for exploitation if keys are leaked.
- Non-compliance with modern PKI best practices.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Short-Lived Certs: Enforce ~1-year maximum validity.
- Automated Renewal: Implement tooling for frequent certificate rotation.
- Policy Enforcement: Audit and revoke certificates exceeding allowable durations.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.33 33. TLS Susp Extn

Risk ID: 33
Runtime Type: `DPI_TLS_SUSPICIOUS_EXTENSION`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS handshake includes unrecognized or non-standard extensions potentially used for tunneling.

Enhanced Description

Detects suspicious or malformed TLS extensions that could indicate protocol abuse or advanced evasion tactics. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Hidden command and control sessions.
- Difficulty applying traditional inspection or filtering.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Extension Validation: Limit or block unrecognized TLS extensions.
- Protocol Auditing: Investigate any repeated anomalies in client/server hellos.
- Threat Hunting: Correlate suspicious TLS extensions with other indicators.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.34 34. TLS Fatal Alert

Risk ID: 34
Runtime Type: `DPI_TLS_FATAL_ALERT`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Clients/servers exchanging fatal alert messages during the handshake, indicating immediate session termination.

Enhanced Description

Signals that a TLS handshake has failed critically, possibly due to mismatched configs, expired certs, or active probing. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Session disruption and potential attack reconnaissance.
- Gaps in encrypted communication.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Logging & Analysis: Determine root cause of repeated fatal alerts.
- TLS Policy Enforcement: Ensure consistent cipher suites and protocol versions.
- Configuration Audits: Check for misalignment between client/server setups.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.35 35. Susp Entropy

Risk ID: 35
Runtime Type: `DPI_SUSPICIOUS_ENTROPY`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

ICMP or other packets carrying high-entropy data, possibly indicating covert exfiltration or encrypted payloads.

Enhanced Description

Highlights unusually random or high-entropy traffic that could be disguised tunneling or exfiltration. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Subject to neighbor and benign-cluster suppression tuning. Agentic Investigator can raise thresholds or suppress known-good provider domains where the raw signal is common in large CDNs or software update ecosystems.

Potential Impact

- Undetected data leakage.
- Stealthy malware comms hidden in benign protocols.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Entropy Analysis: Flag sustained high-entropy flows.
- Correlate with Context: Check if legitimate encryption or compression is in play.
- Block/Investigate: Quarantine traffic with no valid justification for high entropy.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.36 36. Clear-Text Credentials

Risk ID: 36
Runtime Type: `DPI_CLEAR_TEXT_CREDENTIALS`
Severity and Score: High / total 100 / client 90 / server 10
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

HTTP POST carrying username/password in plain text, FTP logins with no encryption, etc.

Enhanced Description

Unencrypted credentials are easily intercepted, enabling unauthorized access or credential harvesting. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Account compromise, escalation of privileges, data breaches.
- Violations of compliance mandates (PCI-DSS, HIPAA, etc.).

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- SSL/TLS Enforcement: Force HTTPS or secure protocols for all credential exchanges.
- User Training: Educate on the dangers of sending passwords unencrypted.
- Monitoring: Continuously scan traffic for any clear-text authentication attempts.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.37 37. Large DNS Packet (512+ bytes)

Risk ID: 37
Runtime Type: `DPI_DNS_LARGE_PACKET`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

UDP-based DNS packets exceeding the 512-byte limit, possibly used for DNS-based tunneling.

Enhanced Description

Detects abnormally large DNS responses that can hide data exfiltration or malicious payloads. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron preserves DNS and hostname context, including query/answer counts, response type, reply code, response

addresses, host_name, and domain_name. Agentic Investigator can require host fields for DGA-class events to reduce weak-signal false positives.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Covert channel for data leaks.
- Evasion of standard firewall/DNS filtering.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on host_name, domain_name, DNS response addresses, recurrence, and internal sources. Review DNS resolver logs and block/sinkhole when confirmed malicious.

Mitigation Strategies

- DNS Size Limit: Enforce maximum packet sizes.
- Monitor & Alert: Investigate large or fragmented DNS messages.
- Tunneling Protection: Deploy DNS-level intrusion detection.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0.`

8.38 38. Fragmented DNS Message

Risk ID: 38
Runtime Type: `DPI_DNS_FRAGMENTED`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

DNS queries or responses split across multiple fragments, unusual in typical DNS usage.

Enhanced Description

May indicate DNS tunneling or attempts to bypass standard security measures. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron preserves DNS and hostname context, including query/answer counts, response type, reply code, response addresses, host_name, and domain_name. Agentic Investigator can require host fields for DGA-class events to reduce weak-signal false positives.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Covert exfiltration of sensitive data.
- Evasion of standard DNS oversight.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on host_name, domain_name, DNS response addresses, recurrence, and internal sources. Review DNS resolver logs and block/sinkhole when confirmed malicious.

Mitigation Strategies

- DNS Reassembly: Use security tools that recombine and inspect DNS fragments.
- Block Suspicious Fragments: Disallow rarely-used or excessive fragmentation.
- Correlate with Other Alerts: Investigate repeated fragmentation events.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0.`

8.39 39. Non-Printable/Invalid Chars Detected

Risk ID: 39
Runtime Type: `DPI_INVALID_CHARACTERS`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: General Network Risk

Observed Pattern or Example

DNS hostnames or TLS fields containing unexpected Unicode or control characters.

Enhanced Description

Indicates protocol fields containing invalid or non-printable characters. Often an attempt to obfuscate malicious payloads or exploit parsing logic. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Disruption of normal traffic handling.
- Bypassing of naive validation routines.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Strict Input Validation: Reject non-compliant or suspicious characters.
- Protocol-Conforming Parsers: Enforce RFC-compliant data fields.
- Investigate: Review logs for repeated invalid character usage.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.40 40. Possible Exploit Attempt

Risk ID: 40
Runtime Type: `DPI_POSSIBLE_EXPLOIT`
Severity and Score: Severe / total 100 / client 75 / server 25
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

Indicators resembling known exploits (e.g., Log4Shell strings, shell injection patterns).

Enhanced Description

Flags network traffic that strongly suggests an attempt to exploit a known software or service vulnerability. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Remote code execution or system compromise.
- Data theft, service disruption, or privilege escalation.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Preserve URL, user agent, server endpoint, and any web gateway logs. Confirm whether the targeted service was exposed, patched, and protected by WAF policy.

Mitigation Strategies

- Patch & Update: Immediately apply fixes for known CVEs.
- IDS/WAF: Block or alert on exploit payload patterns.
- Incident Response: Investigate impacted hosts for compromise.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.41 41. TLS Cert About To Expire

Risk ID: 41
Runtime Type: `DPI_TLS_CERTIFICATE_ABOUT_TO_EXPIRE`
Severity and Score: Medium / total 50 / client 5 / server 45
Detection Family: General Network Risk

Observed Pattern or Example

Certificates nearing their valid until date (e.g., within 30 days of expiration).

Enhanced Description

Warns that a TLS certificate is approaching its expiry window, risking service disruptions and potential security lapses. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Unexpected downtime or SSL errors for users.
- Decreased trust if not renewed on time.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Certificate Renewal Workflow: Ensure certificates are renewed proactively.
- Automated Alerts: Implement scripts or dashboards monitoring expiration dates.
- Compliance & Policy: Enforce timely renewal to avoid security gaps.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.42 42. IDN Domain Name

Risk ID: 42
Runtime Type: `DPI_PUNYCODE_IDN`
Severity and Score: Low / total 10 / client 1 / server 9
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

Domains that use Punycode for internationalized characters, e.g., xn–exmple-jza.com.

Enhanced Description

Flags the usage of Internationalized Domain Names, which can be abused for homograph attacks or phishing. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron preserves DNS and hostname context, including query/answer counts, response type, reply code, response addresses, host_name, and domain_name. Agentic Investigator can require host fields for DGA-class events to reduce weak-signal false positives.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Users tricked into visiting malicious look-alike domains.
- Credential theft or session hijacking.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on host_name, domain_name, DNS response addresses, recurrence, and internal sources. Review DNS resolver logs and block/sinkhole when confirmed malicious.

Mitigation Strategies

- IDN Homograph Detection: Compare visually similar characters.
- DNS Filtering: Block suspicious or newly registered IDN domains.
- User Education: Train staff to inspect URLs carefully.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0.`

8.43 43. Error Code

Risk ID: 43
Runtime Type: `DPI_ERROR_CODE_DETECTED`
Severity and Score: Low / total 10 / client 1 / server 9
Detection Family: General Network Risk

Observed Pattern or Example

HTTP status codes indicating server errors (5xx), DNS SERVFAIL, or other abnormal result codes.

Enhanced Description

Reports unusual or unexpected error codes. While often benign, repeated or systematically triggered errors can be signs of reconnaissance or misconfigurations. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- System instability or partial service disruption.
- Indication of exploit attempts or scanning.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Log Monitoring: Investigate recurring errors or suspicious patterns.
- Configuration Reviews: Fix underlying misconfigurations.
- Correlate with Other Alerts: Check for scans or exploit activity.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.44 44. Crawler/Bot

Risk ID: 44
Runtime Type: `DPI_HTTP_CRAWLER_BOT`
Severity and Score: Low / total 10 / client 1 / server 9
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

Automated agents scanning pages at high speed, ignoring robots.txt, or using known crawler signatures.

Enhanced Description

Highlights traffic from web crawlers, scraping tools, or other bots that can be benign (search engines) or malicious (reconnaissance). In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Unauthorized data harvesting.
- Increased load on web infrastructure.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Rate Limiting: Throttle request rates from suspected bots.
- User-Agent Filtering: Block known malicious crawlers.
- Bot Management: Distinguish legitimate crawlers from harmful ones.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.45 45. Anonymous Subscriber

Risk ID: 45
Runtime Type: `DPI_ANONYMOUS_SUBSCRIBER`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

IP addresses identified as anonymized proxies, iCloud private relay endpoints, or Tor exit nodes.

Enhanced Description

Alerts on traffic from users/connections that obscure their origin or identity, possibly hiding malicious activity. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Difficulty attributing actions to real individuals.
- Potential for covert infiltration or data theft.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Multi-Factor Authentication: Strengthen identity checks.
- Geolocation/ASN Filtering: Restrict known anonymizer IP ranges.

- Logging & Correlation: Link suspect sessions with other threat indicators.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.46 46. Unidirectional Traffic

Risk ID: 46
Runtime Type: `DPI_UNIDIRECTIONAL_TRAFFIC`
Severity and Score: Low / total 10 / client 5 / server 5
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

TCP flows showing data only in one direction, no acknowledgment from the other side.

Enhanced Description

Unidirectional flows can indicate scanning, data exfiltration, or abnormal configurations. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Possible hidden data transfers.
- Reduced visibility into true session behavior.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Flow Analysis: Check for large outbound transmissions without inbound requests.
- Firewall Rules: Restrict connections lacking proper handshake.
- Investigate Patterns: Look for repeated unidirectional flows as a sign of exfiltration.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.47 47. HTTP Obsolete Server

Risk ID: 47
Runtime Type: `DPI_HTTP_OBSOLETE_SERVER`
Severity and Score: Medium / total 50 / client 5 / server 45
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

HTTP Server header revealing outdated server software (e.g., Apache 1.x, old IIS versions).

Enhanced Description

Indicates usage of an obsolete or end-of-life HTTP server stack with unpatched vulnerabilities. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- High risk of exploits targeting known CVEs.
- Web defacements, data breaches, or resource hijacking.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Upgrade Server Software: Use supported versions with security patches.
- Security Hardening: Apply best practices (disable directory listing, default admin pages, etc.).
- Regular Testing: Scan externally facing services for known vulnerabilities.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.48 48. Periodic Flow

Risk ID: 48
Runtime Type: `DPI_PERIODIC_FLOW`
Severity and Score: Low / total 10 / client 1 / server 9
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Connections reoccurring at fixed intervals (e.g., every 10 seconds) suggest automated processes.

Enhanced Description

Flags traffic that appears in a strict, repeating schedule. This may indicate bot communications, scheduled tasks, or data exfiltration. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Unnoticed malicious C2 or data-laundering channels.
- Resource exhaustion if tasks are frequent and large.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the

same time window.

Mitigation Strategies

- Behavioral Analysis: Detect suspiciously regular flows.
- Correlate with Known Jobs: Determine if traffic matches legitimate cron-like tasks.
- Block/Alert: Investigate unexplained periodic traffic.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.49 49. Minor Issues

Risk ID: 49
Runtime Type: `DPI_MINOR_ISSUES`
Severity and Score: Low / total 10 / client 1 / server 9
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Connection resets, half-open sessions, or frequent handshake failures.

Enhanced Description

Reports irregularities or problems in TCP connections that might result from scans, DDoS attempts, or system misconfigurations. In operations, this is normally a context signal. It becomes more important when paired with suspicious domains, external destinations, high data volume, repeated recurrence, or critical asset involvement.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Service instability, partial outages, or performance degradation.
- Opening for stealthy scanning or reconnaissance.

Triage Guidance

Treat as a weak signal; correlate with recurrence, asset criticality, and neighboring events before escalation. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Network Monitoring Tools: Alert on recurring TCP errors.
- Firewall/IPS: Block suspicious scanning behavior.
- System Audits: Fix misconfigurations leading to handshake issues.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.50 50. TCP Connection Issues

Risk ID: 50
Runtime Type: `DPI_MINOR_ISSUES`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Connection resets, half-open sessions, or frequent handshake failures.

Enhanced Description

Reports irregularities or problems in TCP connections that might result from scans, DDoS attempts, or system misconfigurations. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Service instability, partial outages, or performance degradation.
- Opening for stealthy scanning or reconnaissance.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Network Monitoring Tools: Alert on recurring TCP errors.
- Firewall/IPS: Block suspicious scanning behavior.
- System Audits: Fix misconfigurations leading to handshake issues.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.51 51. Fully Encrypted Flow

Risk ID: 51
Runtime Type: `DPI_FULLY_ENCRYPTED`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Traffic where no plaintext metadata is visible, making it difficult to identify protocol or content.

Enhanced Description

Indicates an entirely encrypted channel that can mask malicious data exfiltration or malicious commands. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Limited visibility for intrusion detection.
- Possible use as a covert tunnel.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Encrypted Traffic Analysis: Use metadata/behavior to detect anomalies.
- SSL Inspection: Where compliant, decrypt to inspect contents.
- Zero-Trust Segmentation: Restrict fully encrypted flows to known-approved endpoints.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.52 52. ALPN/SNI Mismatch

Risk ID: 52
Runtime Type: `DPI_TLS_ALPN_SNI_MISMATCH`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

TLS handshake advertises one protocol in ALPN but the SNI indicates a different service.

Enhanced Description

Highlights inconsistencies between the advertised Application-Layer Protocol Negotiation and the Server Name Indication, suggesting misconfiguration or potential evasion. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Confusion in server routing or policy enforcement.
- Possible malicious use of mismatches to bypass detection.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Align Configurations: Ensure ALPN and SNI fields match intended service.
- Monitor: Alert on repeated mismatch occurrences.
- Protocol Consistency Checks: Restrict traffic that violates normal handshake protocols.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.53 53. Client Contacted A Malware Host

Risk ID: 53
Runtime Type: `DPI_MALWARE_HOST_CONTACTED`
Severity and Score: Severe / total 100 / client 75 / server 25
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

Connections to IPs known to distribute malware, as flagged by real-time threat intel feeds.

Enhanced Description

Indicates a client has reached out to a confirmed malicious host often used for payload delivery or command and control. In operations, this should be considered an actionable signal when seen on production systems, exposed services, privileged segments, or unmanaged assets.

Hadron Runtime Handling

Hadron flattens the DPI flow_risk object, maps the risk_id through dpi_risk_scores, enriches it with ASN, geolocation, asset, protocol, port, cumulative flow metrics, and writes the normalized HIP record to ClickHouse for investigation.

Agentic Investigator API Handling

Handled by the malware infrastructure playbook family. Agentic Investigator measures fan-in from internal hosts to the same destination or domain and escalates when the event suggests shared malware infrastructure or campaign behavior.

Potential Impact

- Malware infection or lateral spread.
- Data theft or ransomware encryption.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Pivot on the indicator across ClickHouse, endpoint telemetry, proxy logs, and MISP/TIP. Isolate or block if the internal host initiated contact.

Mitigation Strategies

- Immediate Block: Quarantine or cut off communication to the malicious host.
- Endpoint Investigation: Scan the contacting system for compromise.
- Threat Intel Integration: Stay updated with blacklists of active malware domains/IPs.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.54 54. Binary File/Data Transfer (Attempt)

Risk ID: 54
Runtime Type: `DPI_BINARY_DATA_TRANSFER`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Web Application and Content Attacks

Observed Pattern or Example

HTTP or other protocols carrying .bin, .exe, or other binary payloads.

Enhanced Description

Detects attempts to upload or download binary files that could include malicious code or sensitive data. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron requires useful HTTP context for selected web exploit classes before high-confidence write paths proceed. Relevant fields include HTTP URL, user agent, content type, HTTP status, host_name, category, and application_protocol.

Agentic Investigator API Handling

Subject to neighbor and benign-cluster suppression tuning. Agentic Investigator can raise thresholds or suppress known-good provider domains where the raw signal is common in large CDNs or software update ecosystems.

Potential Impact

- Potential infiltration of malware or exfiltration of proprietary files.
- Violations of data handling policies.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Pivot on source_ip, destination_ip, port, application_protocol, host_name, ASN, asset labels, and neighboring events in the same time window.

Mitigation Strategies

- Content Inspection: Scan binary data with anti-malware engines.
- DLP Systems: Block unauthorized file transfers.
- Access Control: Restrict where and how binaries can be introduced into the environment.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.55 55. Probing Attempt

Risk ID: 55
Runtime Type: `DPI_PROBING_ATTEMPT`
Severity and Score: Medium / total 50 / client 25 / server 25
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Repeated port scans, connection attempts with no real data exchange, or service enumeration.

Enhanced Description

Indicates reconnaissance activity aimed at mapping open ports or identifying service vulnerabilities. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron preserves port, endpoint, protocol, flow state, packet count, and cumulative connection context. The Agentic Investigator layer expands this into scan confirmation with distinct-port, fan-out, and persistence tests.

Agentic Investigator API Handling

Handled by the probing playbook family. Agentic Investigator expands this signal into vertical port scan, fan-out, and persistence checks. Operational thresholds include a distinct destination port threshold and a short lookback window for scan confirmation. Participates in sequence correlation. Current configured sequences include reconnaissance followed by RCE, binary transfer, DGA or malicious-domain contact, and exfiltration. This makes the risk more important when it appears as part of a multi-step attack chain.

Potential Impact

- Attackers gain information to plan targeted exploits.
- Potential infiltration if vulnerabilities are found.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Confirm scan intent, scanner ownership, source/destination scope, and whether the scan was authorized. Escalate unexpected internal or public probing.

Mitigation Strategies

- IDS/IPS: Immediately flag and block scanning attempts.
- Honeypots: Divert and gather intelligence on attackers.

- Network Hardening: Close unused ports and employ strict ACLs.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id.`

8.56 56. Obfuscated Traffic

Risk ID: 56
Runtime Type: `DPI_OBFUSCATED_TRAFFIC`
Severity and Score: Medium / total 50 / client 35 / server 15
Detection Family: TLS, SSH, Encryption and Certificate Posture

Observed Pattern or Example

Unusual encryption layers, disguised protocols, or encoded data not matching typical patterns.

Enhanced Description

Identifies traffic deliberately made hard to analyze (beyond normal encryption), often to hide malicious operations or data exfiltration. In operations, this signal is most valuable when repeated, clustered in a subnet, associated with a critical asset, or combined with other risk IDs in a short time window.

Hadron Runtime Handling

Hadron flattens the DPI TLS or SSH risk into a single risk_id/risk_type pair and preserves supporting fields such as TLS version, cipher, ALPN, SNI, issuer, subject, fingerprints, and unsafe cipher indicators for downstream validation.

Agentic Investigator API Handling

Processed by the universal detection playbook. Agentic Investigator deduplicates recent resolved pairs, checks CIDR neighbors, applies dynamic allowlists, and escalates when clustering, score, or context justifies analyst attention.

Potential Impact

- Stealthy attacks remain undetected.
- Extended dwell times for adversaries.

Triage Guidance

Treat as triage-worthy when repeated, clustered, or observed on critical assets. Validate protocol posture against approved crypto baselines and check whether the endpoint is sanctioned, legacy, or externally reachable.

Mitigation Strategies

- Advanced Traffic Inspection: Use ML/behavioral analytics to identify suspicious flows.
- Decryption Capabilities: Where feasible, decrypt or decode suspicious payloads.
- Correlate with Threat Intelligence: Compare patterns to known obfuscation signatures.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, tls_version, tls_cipher, tls_ja3_fingerprint, tls_ja4_fingerprint, tls_server_names, tls_negotiated_alpn, tls_certificate_issuer_dn, tls_certificate_subject_dn.`

8.57 57. Malicious IP Detected in Network

Risk ID: 57
Runtime Type: `HADRON_MALICIOUS_IP_DETECTED`
Severity and Score: High / total 100 / client 25 / server 75
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

Traffic to/from IPs flagged by advanced threat intel as part of known malicious infrastructures.

Enhanced Description

Raises an alert when a known bad IP is observed on the network, potentially indicating infiltration or exfiltration. Within Streaming Defense, this detection is a Hadron-enriched signal. It is not merely a label from a single packet; it is produced or elevated by local state, threat intelligence, fingerprint intelligence, or DNS behavior before the Agentic Investigator stage performs correlation.

Hadron Runtime Handling

Hadron sets this detection when the public source or destination IP matches the Streaming Defense IP intelligence store. The enriched record carries public_ip, source/destination ASN, geolocation, threat indicator flags, cumulative bytes and packets, and the SD score fields injected from this V5 catalog.

Agentic Investigator API Handling

Handled by the malware infrastructure playbook family. Agentic Investigator measures fan-in from internal hosts to the same destination or domain and escalates when the event suggests shared malware infrastructure or campaign behavior. Hadron-originated or Hadron-enriched detection. It is produced from Streaming Defense threat intelligence, cumulative flow state, JA4 intelligence, or DNS fast-flux heuristics rather than being only a raw DPI risk bit.

Potential Impact

- Increased risk of data theft, malware, or infiltration attempts.
- Could be part of a botnet or malicious campaign.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Pivot on the indicator across ClickHouse, endpoint telemetry, proxy logs, and MISP/TIP. Isolate or block if the internal host initiated contact.

Mitigation Strategies

- Immediate Blocking: Terminate connections to/from malicious IP.
- Incident Analysis: Investigate endpoints communicating with the IP.
- Update Blocklists: Keep threat databases in sync with new malicious IPs.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, threat_indicator_ip_source, threat_indicator_ip_destination, threat_indicator_domain, threat_indicator_exfiltration, ja4T, ffT, source_ip_cumulative_bytes, destination_ip_cumulative_bytes.`

8.58 58. Malicious Domain Detected in Network

Risk ID: 58
Runtime Type: `HADRON_MALICIOUS_DOMAIN_DETECTED`
Severity and Score: High / total 100 / client 25 / server 75
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

DNS queries or HTTP requests matching domains recognized as malicious or flagged by intel feeds.

Enhanced Description

Indicates attempted contact with domains known to host malware, phishing campaigns, or C2 services. Within Streaming Defense, this detection is a Hadron-enriched signal. It is not merely a label from a single packet; it is produced or elevated by local state, threat intelligence, fingerprint intelligence, or DNS behavior before the Agentic Investigator stage performs correlation.

Hadron Runtime Handling

Hadron sets this detection when the observed hostname or domain matches the Streaming Defense domain intelligence store. The event is enriched with host_name/domain_name, application protocol, ASN/geolocation of the public endpoint, and the domain threat indicator flag.

Agentic Investigator API Handling

Handled by the malware infrastructure playbook family. Agentic Investigator measures fan-in from internal hosts to the same destination or domain and escalates when the event suggests shared malware infrastructure or campaign behavior. Participates in sequence correlation. Current configured sequences include reconnaissance followed by RCE, binary transfer, DGA or malicious-domain contact, and exfiltration. This makes the risk more important when it appears as part of a multi-step attack chain. Hadron-originated or Hadron-enriched detection. It is produced from Streaming Defense threat intelligence, cumulative flow state, JA4 intelligence, or DNS fast-flux heuristics rather than being only a raw DPI risk bit.

Potential Impact

- Inbound malware downloads or outbound data exfiltration.
- Potential compromise or infiltration of the network.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Pivot on host_name, domain_name, DNS response addresses, recurrence, and internal sources. Review DNS resolver logs and block/sinkhole when confirmed malicious. Pivot on the indicator across ClickHouse, endpoint telemetry, proxy logs, and MISP/TIP. Isolate or block if the internal host initiated contact.

Mitigation Strategies

- Real-Time DNS Blackholing: Block or redirect traffic to malicious domains.
- User Awareness: Train employees not to click suspicious links.
- Threat Intel Integration: Continuously update domain blacklists.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0, threat_indicator_ip_source, threat_indicator_ip_destination, threat_indicator_domain, threat_indicator_exfiltration, ja4T, ffT, source_ip_cumulative_bytes, destination_ip_cumulative_bytes.`

8.59 59. Data Exfiltration

Risk ID: 59
Runtime Type: `HADRON_DATA_EXFILTRATION`
Severity and Score: High / total 100 / client 25 / server 75
Detection Family: Network Reconnaissance, Flow Behavior and Transport Anomalies

Observed Pattern or Example

Large outbound file transfers, suspicious encryption patterns, or unusual DNS queries indicative of data extraction.

Enhanced Description

Suggests unauthorized transfer of sensitive data outside the network often a key stage of cyberattacks. Within Streaming Defense, this detection is a Hadron-enriched signal. It is not merely a label from a single packet; it is produced or elevated by local state, threat intelligence, fingerprint intelligence, or DNS behavior before the Agentic Investigator stage performs correlation.

Hadron Runtime Handling

Hadron derives this from flow state. The current heuristic looks for a public destination with a large outbound payload increase, using cumulative source/destination byte tracking to identify abnormal transfer behavior that may represent exfiltration.

Agentic Investigator API Handling

Participates in sequence correlation. Current configured sequences include reconnaissance followed by RCE, binary transfer, DGA or malicious-domain contact, and exfiltration. This makes the risk more important when it appears as part of a multi-step attack chain. Hadron-originated or Hadron-enriched detection. It is produced from Streaming Defense threat intelligence, cumulative flow state, JA4 intelligence, or DNS fast-flux heuristics rather than being only a raw DPI risk bit.

Potential Impact

- Theft of intellectual property, PII, or financial records.
- Regulatory penalties and reputational damage.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Validate data volume, duration, destination ASN, country, application protocol, and whether the destination is approved for bulk data transfer.

Mitigation Strategies

- DLP Solutions: Monitor and block suspicious outbound data flows.
- Network Segmentation: Limit data access to minimize exfiltration risk.
- Incident Response: Investigate source and extent of exfiltration immediately.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, threat_indicator_ip_source, threat_indicator_ip_destination, threat_indicator_domain, threat_indicator_exfiltration, ja4T, ffT, source_ip_cumulative_bytes, destination_ip_cumulative_bytes.`

8.60 60. Malicious Fingerprint Detected in Network

Risk ID: 60
Runtime Type: `HADRON_MALICIOUS_FINGERPRINT_DETECTED`
Severity and Score: High / total 100 / client 25 / server 75
Detection Family: Threat Intelligence and Malware Infrastructure

Observed Pattern or Example

Matching known malicious TLS handshake fingerprints or other unique indicators of advanced threats.

Enhanced Description

Reveals recognized malicious fingerprinting in network traffic, possibly indicating advanced or targeted attacks. Within Streaming Defense, this detection is a Hadron-enriched signal. It is not merely a label from a single packet; it is produced or elevated by local state, threat intelligence, fingerprint intelligence, or DNS behavior before the Agentic Investigator stage performs correlation.

Hadron Runtime Handling

Hadron sets this detection when the TLS JA4 fingerprint matches the Streaming Defense JA4 threat intelligence store. It preserves TLS/QUIC fingerprint fields and annotates the event with the JA4 threat indicator flag for downstream triage.

Agentic Investigator API Handling

Hadron-originated or Hadron-enriched detection. It is produced from Streaming Defense threat intelligence, cumulative flow state, JA4 intelligence, or DNS fast-flux heuristics rather than being only a raw DPI risk bit.

Potential Impact

- Undetected infiltration with stealthy tactics.
- Potential data corruption or theft at scale.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Pivot on the indicator across ClickHouse, endpoint telemetry, proxy logs, and MISP/TIP. Isolate or block if the internal host initiated contact.

Mitigation Strategies

- Threat Intel Feeds: Continuously scan for known malicious fingerprints.
- Quarantine Host: Investigate any system generating malicious signatures.
- Update Security Tools: Ensure recognition of newly discovered threat fingerprints.

Primary Evidence Fields

`risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, threat_indicator_ip_source, threat_indicator_ip_destination, threat_indicator_domain, threat_indicator_exfiltration, ja4T, ffT, source_ip_cumulative_bytes,`

destination_ip_cumulative_bytes.

8.61 61. Fast Flux Operation Detected

Risk ID: 61
Runtime Type: HADRON_FAST_FLUX_DETECTED
Severity and Score: Severe / total 100 / client 25 / server 75
Detection Family: DNS, Domains, C2 and Resolution Anomalies

Observed Pattern or Example

DNS records for the same domain changing IP addresses very rapidly, typical of botnet or phishing infrastructure.

Enhanced Description

Fast flux is a technique used by attackers to cycle through multiple IPs or hosts, making takedowns and blacklisting more difficult. Within Streaming Defense, this detection is a Hadron-enriched signal. It is not merely a label from a single packet; it is produced or elevated by local state, threat intelligence, fingerprint intelligence, or DNS behavior before the Agentic Investigator stage performs correlation.

Hadron Runtime Handling

Hadron derives this from DNS behavior. It tracks domain-to-IP churn, low TTL conditions, and rapid address changes to identify fast-flux style infrastructure before the event is forwarded to the AOT and Agentic Investigator layers.

Agentic Investigator API Handling

Handled by the malware infrastructure playbook family. Agentic Investigator measures fan-in from internal hosts to the same destination or domain and escalates when the event suggests shared malware infrastructure or campaign behavior. Hadron-originated or Hadron-enriched detection. It is produced from Streaming Defense threat intelligence, cumulative flow state, JA4 intelligence, or DNS fast-flux heuristics rather than being only a raw DPI risk bit.

Potential Impact

- Persistent malicious infrastructure, resilient to blocking.
- Facilitated botnet command and control channels.

Triage Guidance

Treat as analyst-actionable unless an allowlist or known maintenance window explains the activity. Pivot on host_name, domain_name, DNS response addresses, recurrence, and internal sources. Review DNS resolver logs and block/sinkhole when confirmed malicious.

Mitigation Strategies

- DNS Monitoring: Flag domains with rapidly shifting DNS records.
- Collaboration: Work with ISPs or security groups to dismantle fast flux networks.
- Block & Investigate: Stop traffic to suspicious domains; trace any infected hosts.

Primary Evidence Fields

risk_id, risk_type, risk_score_total, risk_severity, source_ip, destination_ip, source_port, destination_port, application_protocol, host_name, domain_name, confidence_id, dns_number_of_queries, dns_number_of_answers, dns_reply_code, dns_response_address_0, threat_indicator_ip_source, threat_indicator_ip_destination, threat_indicator_domain, threat_indicator_exfiltration, ja4T, ffT, source_ip_cumulative_bytes, destination_ip_cumulative_bytes.

9 Operational Notes and Known Engineering Considerations

- **Score alignment:** V5 scores are the current JavaScript values. Older V4 labels that showed different scores for selected TLS, HTTP, obfuscation, Hadron intelligence, and fast-flux detections are superseded by this catalog.
- **Raw risk versus enriched risk:** IDs 1 through 56 are primarily DPI-originated risk types. IDs 57 through 61 are Streaming Defense enriched detections surfaced by Hadron using threat intelligence, stateful flow analysis, fingerprint intelligence, and DNS fast-flux behavior.
- **Suppression is not deletion:** Dynamic allowlists and edge gates reduce noise but do not remove the detection

definition. The V5 catalog remains the governing dictionary for scoring and field naming.

- **Customer communication:** For SOC and MSSP reporting, use the V5 ID, runtime type, score, severity, affected source/destination, domain/host, and Agentic Investigator result. This keeps customer-facing evidence aligned with the runtime pipeline.
- **Validation path:** To validate a detection in production, query ClickHouse by `risk_id`, `risk_type`, source/destination pair, and event time; then pivot to AOT, Agentic Investigator results, and external ticketing or MISP artifacts if the event was escalated.

10 Conclusion

Streaming Defense Detection Types V5 provides the updated, runtime-aligned detection taxonomy for the Streaming Defense platform. It should be treated as the canonical customer-facing and analyst-facing reference for detection IDs, risk names, severity, score, operational meaning, triage handling, and mitigation expectations. The catalog supports analyst investigation, automated playbooks, AOT visualization, ClickHouse analytics, SIEM forwarding, and executive reporting from the same source-aligned structure.