STREAMING DEFENSE

Application, Protocol and Detection Guide

See clearly. Detect instantly.
Act with confidence.

Real-time network evidence, explainable detection and customer-controlled response across IT and OT.

212	Application and protocol entries
32 + 3	Behavior definitions and additional correlation chains
78	Sigma starter templates

Voyager observes. Gluon detects. Atlas explains.

A practical guide to what the platform recognizes, what triggers review and how analysts move from evidence to action.

streamingdefense.com

28 November 2026

Contents

1 From network activity to action **3**

1.1 Three detection paths . . . 3

2 Application and protocol visibility **3**

2.1 IT and OT share one evidence pipeline . . . 3

2.2 Encryption and capture position . . . 3

3 Behaviors: explain what fired and why **3**

4 Sigma: customer-controlled live rules **4**

5 Intelligence, identity and response **4**

5.1 Intelligence with communication context . . . 4

5.2 Identity adds operational context . . . 4

5.3 Integrate with the tools already in place . . . 4

6 Investigate, replay, report and validate **5**

7 Complete behavior dictionary **6**

7.1 Additional correlation chains . . . 8

8 Complete Sigma template dictionary **9**

8.1 Policy . . . 9

8.2 Indicator watch . . . 9

8.3 Service exposure . . . 9

8.4 Investigation context . . . 10

8.5 Asset & MAC . . . 10

8.6 Domain & DNS . . . 11

8.7 Application protocol . . . 11

8.8 Encryption posture . . . 12

8.9 Transfer-volume signal . . . 12

9 Complete application and protocol dictionary **14**

9.1 Industrial, utilities, building and embedded services (39) . . . 14

9.2 Enterprise, network infrastructure and shared services (173) . . . 15

10 Using this guide **19**

1 From network activity to action

Voyager captures and identifies. Distributed probes observe host or SPAN/TAP traffic, reconstruct supported network exchanges and publish typed facts. Visible protocol framing and metadata identify services such as SMB, SSH, RDP, BitTorrent and industrial control protocols.

Gluon evaluates activity as it arrives. Streaming processing combines defined behaviors, scoped Sigma rules and exact intelligence matches. Its measured mean local input-to-output latency is sub-millisecond in observed operations. This processing measure is distinct from the time an attack takes to unfold and the time a downstream appliance takes to act.

Atlas turns evidence into decisions. Live visualization, exact replay, Full Take search, Analytics and reporting give analysts a shared view of the activity and its provenance. Authorized automation carries actionable findings into the customer's security tooling.

Three detection paths

- **Behavior:** identify changes, sequences and operation patterns in the observed traffic.
- **Sigma:** turn customer policy and selected evidence into explicit, scoped rules.
- **Threat intelligence:** match observed indicators to named intelligence entries and retain their provenance.

Captured facts, analytical evidence and response eligibility remain distinguishable. Analysts can see what triggered a finding and apply narrow exceptions without turning off visibility for the rest of the network.

2 Application and protocol visibility

Applications here mean network services and wire protocols. SMB, Tor, BitTorrent, SSH and RDP are examples; the catalog is not a list of SaaS brands inferred from addresses or domain ownership.

Voyager's native parsers do the identification before Gluon processing. Atlas exposes the available labels in map tags, observation details and supported investigation/search fields. Application tags prioritize specific recognized application evidence. If no application label is available, the application tag is left blank; the separate protocol view can still show visible transport or encryption context.

IT and OT share one evidence pipeline

For IT, inspect remote administration, identity services, file sharing, web traffic, databases and messaging. For OT, inspect industrial protocols, controller communications, building systems and transitions such as a new Modbus write after established read activity. The same investigation, rule and response workflow applies to both.

Encryption and capture position

TLS, QUIC and DTLS expose supported handshake context; an encrypted inner application is identified only when sufficient evidence is visible. DNS questions, TLS server names and HTTP authorities are distinct facts. A port convention alone does not establish a parsed application.

Place probes where the relevant traffic is visible. Encryption, midstream capture, truncation and packet loss affect reconstruction. Where inspection of decrypted traffic is required, integrate at the customer's authorized F5 decryption point and monitor the exposed traffic path.

3 Behaviors: explain what fired and why

The catalog covers discovery, lateral-movement indicators, recurring callbacks, concentrated transfers, changing network relationships, DNS failures, SMB file operations and OT command changes.

Lateral movement. Address sweeps and port probes reveal discovery. Administrative-service fanout exposes one

source reaching multiple internal peers. Ordered correlations link these stages, while observed SMB operations provide file-change evidence. Analysts can follow the source, targets, services and chronology rather than work from a label alone.

Ransomware-associated file activity. Matched SMB requests and successful replies establish observed writes, renames and deletes. Existing-file rewrite patterns distinguish modification of existing content from a workload that only creates new files.

OT change. A Modbus write following retained read-only history focuses review on a change in controller interaction. Target, unit, function and supporting observations guide the next check.

Noise control. Retained baselines, specific operation conditions, narrowly scoped exceptions and visible priorities let analysts tune routine activity. Baseline-dependent definitions need adequate history; exact thresholds and evidence windows accompany the relevant detection.

4 Sigma: customer-controlled live rules

Start with one of 78 templates, supply the customer's values, choose the Voyager scope and assign a review priority. Templates are editable starting points, not 78 mandatory alerts.

Supported rule fields span destination IPs and networks, ports, ASN/country context, observed frame MACs, parsed application evidence, DNS, visible TLS/QUIC/HTTP metadata, fingerprints and supported wire-fact combinations.

- Combine compatible conditions with AND; supported multivalue fields provide bounded alternatives.
- Select all Voyagers or explicit Voyager scope, enable or disable a rule and retain its creator/revision context.
- Use port watches to monitor exposure, or parsed-application templates to require recognized protocol evidence.
- Where the workflow supports it, require observed communication before escalation and use the authorized Block Now response path.

Customer Sigma content must use the platform's supported fields and condition model. Imported Sigma content is validated against that model.

5 Intelligence, identity and response

Intelligence with communication context

The included Streaming Defense OSINT Threat Intelligence Platform supplies curated indicator context. Configured feed synchronization connects that intelligence to the instance. A published match retains the observed indicator, named entry and provenance. Communication requirements can narrow review to relevant observed activity.

Identity adds operational context

Approved identity integrations and scoped uploads associate devices, addresses and people over a defined time interval. IP and observed MAC evidence remain tied to Voyager and capture context. Routed next-hop MACs are not automatically treated as endpoint identities. Expiry and historical scope keep the association meaningful when addresses change.

Integrate with the tools already in place

Syslog and Gluon export carry findings into SIEMs and operational workflows. Customer-authorized automation can create tickets, update intelligence and request protective action from appliances. Configure the destination, scope and policy, then test the actual receiver and response path.

Hard-block eligibility marks an event for the configured response policy. It does not itself prove that a firewall applied a rule. Record the downstream command, appliance acknowledgement and resulting traffic outcome to close that loop.

6 Investigate, replay, report and validate

Live and replay. Follow the map in real time, tag moments in the local browser and jump to recent detection bookmarks. Exact replay shows counted versus available observations for the selected arrival second. Retained availability is explicit; replay does not silently substitute overlapping records.

Full Take. Search retained connection evidence by time, Voyager and supported conditions, including application/protocol fields. Full Take connection retention and raw packet retention are different capabilities; the catalog does not promise a permanent PCAP archive.

Reports. Comprehensive analyst reports organize findings, supporting evidence, priorities and provenance. Executive reports summarize the selected scope and operational picture. Exports and configured delivery workflows support review and distribution.

Authoritative validation. Red Team exercises run defined scenarios with preflight checks, expected outcomes, negative controls and recorded receipts. Validate capture/processing, Gluon admission and detection evidence; validate appliance enforcement separately through its acknowledgement and traffic outcome.

Private AI. Private-cloud or air-gapped AI supports guidance and research. LLMs do not make authoritative risk decisions for Streaming Defense.

7 Complete behavior dictionary

The following 32 definitions use the same stable identifiers as the current behavior catalog. The three additional correlation chains follow the table.

Behavior / identifier	Observed trigger and retained evidence
Bulk SMB file modification observed SMB_BULK_FILE_MODIFICATION_OBSERVED	Successful writes reach the configured distinct-file threshold in one SMB flow, alongside enough successful renames or deletes in the same window. *Evidence:* Matched SMB requests and successful replies, file IDs, operation counts, and window. Capture gaps and encryption limit visibility.
Ransomware-associated SMB file rewrite pattern SMB_EXISTING_FILE_BULK_REWRITE_OBSERVED	Successful writes reach the configured threshold for file IDs opened as existing, alongside enough successful renames or deletes in one SMB flow window. *Evidence:* Successful SMB operations, existing-file disposition, file IDs, and window. Capture gaps and encryption limit visibility.
TCP address sweep TCP_SYN_ADDRESS_SWEEP	One source sends initial TCP SYNs to distinct destination IPs on the same port within a configured rapid or slow window. *Evidence:* Distinct targets, port, attempt count, window, and representative records. Outside/WAN public pairs require configured customer-side scope.
TCP port probe TCP_SYN_PORT_PROBE	One source sends initial TCP SYNs to distinct ports on one destination IP within a configured rapid or slow window. *Evidence:* Target IP, sampled ports, attempts, and time window. Outside/WAN public pairs require configured customer-side scope.
Regular connection cadence REGULAR_CONNECTION_CADENCE_OBSERVED	Repeated private-to-public TCP first contacts to the same IP and port meet the collector-arrival interval and jitter requirements. *Evidence:* Contact count, mean interval, jitter, and timing basis. Requires a visible private source.
Concentrated outbound payload CONCENTRATED_OUTBOUND_PAYLOAD	Observed outbound L4 payload from one private source to one public destination and port reaches the configured five-minute threshold. *Evidence:* Directional L4 bytes, threshold, port, and evaluation window. Requires private-to-public visibility.
Internal admin-service fanout INTERNAL_ADMIN_SERVICE_FANOUT	One private source makes TCP first contacts to enough distinct private peers on the same recognized admin port in five minutes. *Evidence:* Source, service port, target count, and window. Requires internal endpoint visibility.
Ordered network activity sequence SEQUENTIAL_NETWORK_ACTIVITY_OBSERVED	Within 30 minutes, probing precedes internal admin-service fanout and concentrated outbound transfer for an enrolled endpoint MAC and private source. *Evidence:* Probe-scoped source IP and MAC, ordered evidence references, and timestamps. Requires internal visibility and valid MAC enrollment.
Distinct DNS failures DNS_DISTINCT_NXDOMAIN_BURST	A private client and resolver meet response-volume and distinct failed-name thresholds in one minute. At least 80% of the observed responses are NXDOMAIN. *Evidence:* Scoped client and resolver, response count, distinct failed names, and NXDOMAIN ratio. Requires parsed DNS replies.
New Modbus write operation MODBUS_WRITE_NEW_IN_RETAINED_HISTORY	A parsed Modbus write request follows retained reads without a prior write for the same private client, target, and unit ID. *Evidence:* Retained reads, write request, unit ID, and endpoint pair. Requires visible Modbus traffic and eligible prior history.
New private IP for enrolled endpoint MAC MAC_NEW_PRIVATE_IP_ASSOCIATION	An enrolled endpoint MAC is observed in first-contact traffic using a new private IP after sufficient retained history. *Evidence:* Observed frame MAC, new private IP, prior contacts, and valid enrollment. Routed next-hop MACs do not establish endpoint identity.
Configured SaaS authority requested MAC_CONFIGURED_SAAS_AUTHORITY_REQUEST	Traffic from an enrolled endpoint MAC requests a configured SaaS hostname in visible TLS, QUIC, or HTTP metadata. *Evidence:* Requested hostname, protocol evidence, and MAC enrollment at observation time. Requires visible application metadata.
New internal destination NEW_DESTINATION	A private source contacts an internal peer absent from that source's retained history. *Evidence:* Source and destination in the Voyager's retained history. Requires internal visibility.

Continued on next page

Behavior / identifier	Observed trigger and retained evidence
New public destination NEW_PUBLIC_DESTINATION	A private source contacts a public destination absent from that source's retained history. *Evidence:* Source and destination, with enrichment when available. Novelty is relative to retained history.
New public source NEW_PUBLIC_SOURCE	A private destination receives a TCP SYN from a public IP absent from its retained inbound history. *Evidence:* Source IP, private target, service port, and retained inbound history. Requires visible inbound SYNs.
New source ASN NEW_SOURCE_ASN	A public source of an observed inbound TCP SYN belongs to an ASN absent from the private target's retained inbound history. *Evidence:* Public source IP and ASN, service port, and private target. Requires usable ASN enrichment.
Inbound SYN rate above baseline INBOUND_SYN_RATE_ANOMALY	A private target receives more public-to-private SYN attempts in a closed minute than its learned baseline allows. *Evidence:* Observed SYN volume, learned comparison, and closed window. Counts are attempts.
New destination ASN NEW_ASN	A private source contacts a public destination ASN absent from that source's retained history. *Evidence:* Destination IP and enriched ASN. Novelty depends on enrichment and retained history.
Connection rate above baseline CONNECTION_RATE_ANOMALY	New contacts for the private source exceed its learned connection-rate baseline in a closed minute. *Evidence:* Contact count, baseline comparison, and window. Connection success requires separate evidence.
Outbound volume above baseline OUTBOUND_BYTES_ANOMALY	Observed outbound L4 payload for a private source exceeds its learned volume baseline in a closed minute. *Evidence:* Outbound payload bytes, baseline comparison, and window. Payload contents remain unclassified.
Inbound volume above baseline INBOUND_BYTES_ANOMALY	Observed inbound L4 payload associated with a private source exceeds its learned volume baseline in a closed minute. *Evidence:* Inbound payload bytes, baseline comparison, and window. Capture scope affects measured volume.
Destination fanout above baseline DESTINATION_FANOUT_ANOMALY	The number of distinct destinations contacted by a private source exceeds its learned baseline in a closed minute. *Evidence:* Distinct destination count and retained target samples. Requires sufficient baseline history.
Public source fan-in above baseline SOURCE_FANIN_ANOMALY	The number of distinct public IPs sending SYN attempts to a private target exceeds its inbound baseline in a closed minute. *Evidence:* Distinct public source IP count and retained source samples. The pattern measures attempts.
Service port diversity above baseline SERVICE_PORT_FANIN_ANOMALY	Public SYNs target more distinct private service ports than the target's inbound baseline allows in a closed minute. *Evidence:* Distinct service port count, target, and inbound baseline. The observation leaves service availability unknown.
Source and service pairs above baseline SOURCE_SERVICE_PAIR_FANIN_ANOMALY	Distinct public-source and private-service-port pairs exceed the target's inbound baseline in a closed minute. *Evidence:* Distinct source-port pair count and inbound window. Public source and private target must be visible.
Port fanout above baseline PORT_FANOUT_ANOMALY	The private source contacts more distinct destination ports than its learned baseline allows in a closed minute. *Evidence:* Distinct destination port count, window, and baseline. Requires sufficient history.
Destination and port pairs above baseline PAIR_FANOUT_ANOMALY	Distinct destination IP and port combinations for a private source exceed its learned baseline in a closed minute. *Evidence:* Distinct destination-port pair count, window, and baseline. Requires sufficient history.

Continued on next page

Behavior / identifier	Observed trigger and retained evidence
ASN fanout above baseline ASN_FANOUT_ANOMALY	A private source contacts more distinct destination ASNs than its learned baseline allows in a closed minute. *Evidence:* Distinct enriched ASN count and baseline. Missing enrichment limits coverage.
Source ASN fan-in above baseline SOURCE_ASN_FANIN_ANOMALY	Observed public SYN attempts to a private target come from more distinct ASNs than its inbound baseline allows in a closed minute. *Evidence:* Distinct enriched source ASN count and inbound baseline. Missing enrichment limits coverage.
Inbound condition diversity above baseline INBOUND_CONDITION_DIVERSITY_ANOMALY	Distinct inbound fact-and-predicate clusters for a private target exceed its learned baseline in a closed minute. *Evidence:* Cluster diversity, inbound scope, and baseline. Requires underlying fact coverage.
Behavioral condition diversity above baseline PREDICATE_CLUSTER_FANOUT_ANOMALY	Distinct fact-and-predicate clusters for a private source exceed its learned baseline in a closed minute. *Evidence:* Cluster diversity, source scope, and baseline. Requires underlying fact coverage.
Multiple baseline deviations BASELINE_DEVIATION_HIGH	At least two measured host dimensions cross their learned thresholds in the same closed minute. *Evidence:* Contributing features, window, and learned comparisons. Requires a mature baseline and visible host role.

Additional correlation chains

Discovery followed by administrative fanout

An address sweep is followed by internal admin-service fanout from the same observed source within five minutes.

discovery_with_admin_fanout

Port probing followed by administrative fanout

Port probing is followed by internal admin-service fanout from the same observed source within five minutes.

port_probe_with_admin_fanout

Modbus write after port probing

Port probing is followed by a Modbus write request from the same source to the same exact private target within five minutes.

modbus_write_after_port_probe

8 Complete Sigma template dictionary

Each entry names an available starter template and the conditions it selects. Customer values, scope and rule enablement determine its operation.

Policy

Template / identifier	What it selects
Destination country policy policy_country	Review traffic to a selected destination country; Geo is required.
Country and destination port policy policy_country_port	Review a selected country and observed destination port together.
Country and destination ASN policy policy_country_asn	Review a selected country and enriched destination ASN together.
Country and exact destination IP policy policy_country_ip	Require both the specified destination IP and its enriched country.
Country and destination network policy policy_country_cidr	Require a destination IP range and enriched country.
Destination IP and port policy policy_ip_port	Review an exact destination IP and observed port together.
Destination network and port policy policy_cidr_port	Review a destination IP range and observed port together.
Destination network and ASN policy policy_cidr_asn	Require a destination IP range and enriched ASN.

Indicator watch

Template / identifier	What it selects
Exact destination IP watch watch_ip	Match an analyst-supplied destination IP; a match does not establish maliciousness.
Destination IP range watch watch_cidr	Match an analyst-supplied destination range; a match does not establish maliciousness.
Destination IP and port watch watch_ip_port	Narrow an exact destination IP watch to an observed port.
Destination range and port watch watch_cidr_port	Narrow a destination range watch to an observed port.
Destination IP and ASN watch watch_ip_asn	Require an exact destination IP and enriched ASN.
Destination range and ASN watch watch_cidr_asn	Require a destination range and enriched ASN.

Service exposure

Template / identifier	What it selects
Destination port 22 watch port_ssh	Observe destination port 22; port alone does not prove SSH.
Destination port 53 watch port_dns	Observe destination port 53; port alone does not prove DNS.

Continued on next page

Template / identifier	What it selects
Destination port 80 watch port_http	Observe destination port 80; port alone does not prove HTTP.
Destination port 443 watch port_tls	Observe destination port 443; port alone does not prove TLS or QUIC.
Destination port 445 watch port_smb	Observe destination port 445; port alone does not prove SMB.
Destination port 3389 watch port_rdp	Observe destination port 3389; port alone does not prove RDP.
Destination port 502 watch port_modbus	Observe destination port 502; port alone does not prove Modbus/TCP.
Destination port 4840 watch port_opcua	Observe destination port 4840; port alone does not prove OPC UA.
Destination port 102 watch port_s7	Observe destination port 102; port alone does not prove S7.
Destination port 44818 watch port_enip	Observe destination port 44818; port alone does not prove EtherNet/IP.

Investigation context

Template / identifier	What it selects
Destination ASN context context_asn	Group observations by an enriched destination ASN.
Destination ASN and port context context_asn_port	Review enriched destination ASN and observed port together.
Destination ASN and country context context_asn_country	Require both enriched destination ASN and country.
Destination IP, ASN and port context context_ip_asn_port	Require exact destination IP, enriched ASN and observed port.
Destination range, ASN and country context context_cidr_asn_country	Require destination range, enriched ASN and country.
Destination range, ASN, port and country context context_cidr_asn_port_country	Require all four observed or enriched destination conditions.

Asset & MAC

Template / identifier	What it selects
Observed source frame MAC source_frame_mac	Match the directional source MAC in captured Ethernet frames; this does not prove endpoint or user identity.
Source frame MAC and destination port source_frame_mac_port	Require an observed frame source MAC and destination port in the same flow direction.
Observed destination frame MAC destination_frame_mac	Match the directional destination MAC in captured Ethernet frames; it may belong to a router or bridge.

Domain & DNS

Template / identifier	What it selects
DNS question name dns_name	Match a parsed DNS question name exactly; this is a query, not destination identity.
DNS question domain suffix dns_suffix	Match a parsed DNS question at or below a selected domain.
DNS NXDOMAIN for selected name dns_nxdomain	Require a parsed DNS response for a selected name with response code 3.
DNS SERVFAIL for selected name dns_servfail	Require a parsed DNS response for a selected name with response code 2.
DNS answer address dns_answer_ip	Match an observed A or AAAA answer address in the answer section.
DNS question and answer address dns_name_answer_ip	Require a selected question name and A or AAAA answer IP to co-occur in one parsed response.
DNS question type dns_question_type	Match the numeric question type in a parsed DNS message.
DNS question and destination port dns_name_port	Require a parsed DNS question and observed destination port in the same message.
TLS requested server name tls_sni	Match a visible TLS ClientHello SNI; this is a client request, not server authentication.
TLS requested domain suffix tls_sni_suffix	Match a visible TLS ClientHello SNI at or below a domain.
HTTP request host http_host	Match a parsed HTTP/1 request authority exactly.
QUIC Initial requested server name quic_sni	Match a visible QUIC Initial TLS ClientHello SNI.

Application protocol

Template / identifier	What it selects
Parsed SMB on port 445 app_smb_445	Require parsed SMB metadata and observed destination port 445 in one observation.
Parsed Modbus/TCP on port 502 app_modbus_502	Require parsed Modbus/TCP metadata and observed destination port 502.
Parsed OPC UA on port 4840 app_opcua_4840	Require parsed OPC UA metadata and observed destination port 4840.
Parsed SSH on port 22 app_ssh_22	Require parsed SSH metadata and observed destination port 22.
Parsed MQTT on port 1883 app_mqtt_1883	Require parsed MQTT metadata and observed destination port 1883.
Parsed HTTP/1 on port 80 app_http_80	Require parsed HTTP/1 metadata and observed destination port 80.
Parsed TLS on port 443 app_tls_443	Require parsed TLS metadata and observed destination port 443.
Parsed application protocol app_any	Match one selected parsed Voyager application protocol; any port.

Encryption posture

Template / identifier	What it selects
Negotiated TLS 1.0 or 1.1 tls_legacy	Match a parsed ServerHello selecting TLS 1.0 or 1.1; not client offers.
Negotiated TLS 1.2 tls_12	Match a parsed ServerHello selecting TLS 1.2.
Negotiated TLS 1.3 tls_13	Match a parsed ServerHello selecting TLS 1.3.
Selected TLS cipher suite tls_cipher	Match the exact cipher selected in a parsed ServerHello.
Leaf expired at observation cert_expired	Require validated Voyager fact 14001: visible leaf expired at capture time.
Verified self-signed leaf cert_self_signed	Require validated Voyager fact 10304: leaf self-signature verified.
Expired and verified self-signed leaf cert_expired_self_signed	Require both validated facts on one visible certificate observation.
Visible leaf expiring within 30 days cert_expiring	Match a visible leaf with no more than 30 days remaining at capture time.
Visible leaf not yet valid cert_not_yet_valid	Match a visible leaf whose not-before time follows packet capture time.
ECH extension observed tls_ech	Match an ECH extension in a parsed TLS ClientHello; decryption is not claimed.
Visible ClientHello without SNI tls_no_sni	Require validated Voyager fact 10202: no SNI in a trusted visible ClientHello without ECH.
Visible fatal TLS alert tls_fatal_alert	Require validated Voyager fact 10201: a plaintext fatal TLS alert was parsed.
Client-advertised ALPN tls_alpn_offer	Match a protocol offered in a visible TLS ClientHello; this is not a negotiated ALPN.
TLS ClientHello JA3 fingerprint tls_ja3	Match a visible TLS ClientHello JA3 fingerprint exactly; a match is not endpoint identity.
TLS ClientHello JA4 fingerprint tls_ja4	Match a visible TLS ClientHello JA4 fingerprint exactly; a match is not endpoint identity.
Visible SSH host-key fingerprint ssh_host_key	Match an exact parsed SSH host-key SHA-256 fingerprint.
Visible leaf certificate fingerprint cert_fingerprint	Match a visible leaf certificate SHA-256 fingerprint exactly.
Visible leaf DNS name cert_san	Match a DNS name in a visible leaf certificate SAN list; this is a certificate claim.
Visible RSA leaf below 2048 bits cert_rsa_small	Require a visible RSA leaf with a public key below 2048 bits; customer policy decides severity.
Visible leaf signature algorithm cert_signature_oid	Match a visible certificate signature algorithm OID selected by policy.

Transfer-volume signal

Template / identifier	What it selects
Private-to-public transfer above 100 MiB transfer_outbound_100m	Require observed private source, public destination and 100 MiB cumulative directional L4 payload; investigation signal, not exfiltration proof.
Private-to-public transfer above 1 GiB transfer_outbound_1g	Require observed private source, public destination and 1 GiB cumulative directional L4 payload; investigation signal, not exfiltration proof.
Large outbound transfer to exact IP transfer_ip_1g	Require monitored outbound direction, exact destination IP and 1 GiB cumulative directional L4 payload.

Continued on next page

Template / identifier	What it selects
Large outbound transfer to country transfer_country_1g	Require monitored outbound direction, enriched destination country and 1 GiB cumulative directional L4 payload.
Large outbound transfer to port transfer_port_1g	Require monitored outbound direction, observed destination port and 1 GiB cumulative directional L4 payload.

9 Complete application and protocol dictionary

All 212 entries are listed once. The descriptions identify the recognized wire format or visible metadata. A listed service can occur in IT, OT or a converged network.

Industrial, utilities, building and embedded services (39)

Observed label	Meaning and visible scope
ads	Beckhoff ADS/TwinCAT command metadata.
atg	Automatic tank-gauge command and response framing with recognized function codes.
bacnet	BACnet/IP building-control message metadata.
bsap_ip	Bristol BSAP industrial messages.
c1222	ANSI C12.22 smart-meter message framing.
can_over_ip	CAN-over-IP visible framing.
coap	CoAP method, token, option and response metadata.
dlms	DLMS/COSEM utility-meter framing.
dnp3	DNP3 link and application operation metadata.
easyweather	EasyWeather station telemetry framing.
egd	GE Ethernet Global Data exchange messages.
enip	EtherNet/IP and visible CIP service metadata.
ethersbus	EtherSBus industrial message framing.
ethersio	EtherSIO industrial message framing.
fins	Omron FINS industrial command metadata.
genisys	Genisys industrial-control messages.
hart_ip	HART-IP instrumentation messages.
hislip	HiSLIP instrumentation messages.
iec104	IEC 60870-5-104 telecontrol APDU metadata.
knx	KNXnet/IP building-control messages.
matter	Matter visible commissioning and transport metadata.
melsec	Mitsubishi MC protocol message metadata.
meshtastic	Meshtastic visible mesh framing.
mms	Manufacturing Message Specification service metadata.
modbus_tcp	Modbus/TCP unit, function, range and exception metadata.
mqtt	MQTT connect, publish and control-message metadata.
opc_ua	OPC UA transport, endpoint and visible security headers.
profinet	PROFINET DCP and real-time Ethernet messages.
ptp	IEEE 1588 precision-time messages.
roc_plus	Emerson ROC Plus visible message fields.
rtps	RTPS/DDS real-time publish-subscribe headers.
s7comm	Siemens S7 communication header and operation metadata.
s7plus	Siemens S7comm Plus visible operation metadata.
someip	SOME/IP automotive service messages.

Continued on next page

Observed label	Meaning and visible scope
synchrophasor	IEEE C37.118 synchrophasor messages.
trdp	Train Real-time Data Protocol messages.
tristation	Triconex TriStation industrial messages.
tuya	Tuya device-control message framing.
umas	Schneider UMAS industrial request metadata.

Enterprise, network infrastructure and shared services (173)

Observed label	Meaning and visible scope
afp	Apple Filing Protocol service metadata.
afs_rx	AFS Rx remote-procedure framing.
ajp	AJP web-server connector framing.
amqp	AMQP handshake and frame metadata.
armagetron	Armagetron game-session opening.
bfcp	BFCP floor-control messages.
bfd	Bidirectional Forwarding Detection messages.
bgp	BGP routing message headers.
bitcoin	Bitcoin peer-to-peer message framing.
bittorrent	BitTorrent peer handshake; tracker traffic alone abstains.
bjnp	Canon BJNP printer discovery and control.
capwap	CAPWAP wireless-control headers.
cassandra	Cassandra native database opening.
ceph	Ceph cluster wire opening.
checkmk	Checkmk monitoring-service opening.
citrix_ica	Citrix ICA remote-session opening.
clickhouse	ClickHouse native protocol opening.
collectd	collectd metric-export framing.
corba	CORBA GIOP wire framing.
crossfire_login	CrossFire login-service opening.
dcerpc	DCE/RPC bind and call metadata.
dhcp	DHCPv4 assignment and client-option metadata.
dhcpv6	DHCPv6 provisioning messages and options.
diameter	Diameter AAA message metadata.
dicom	DICOM association negotiation.
dlep	DLEP radio-router link messages.
dns	Domain Name System questions, answers and response codes when the DNS message is visible.
dnscrypt	DNSCrypt certificate and encrypted-message envelope.
drda	DRDA database-access messages.
dtls	Datagram TLS visible handshake metadata.
edonkey	eDonkey peer-to-peer wire handshake.

Continued on next page

Observed label	Meaning and visible scope
egp	Exterior Gateway Protocol messages.
fastcgi	FastCGI request framing.
fix	FIX financial-message session metadata.
flute	FLUTE file-delivery metadata.
ftp	FTP control commands and replies.
gearman	Gearman job-service messages.
git	Git native service-request opening.
glbp	Gateway Load Balancing Protocol messages.
gnutella	Gnutella peer-to-peer handshake and visible messages.
gre	GRE tunnel headers.
gtp	GTP user-plane tunnel headers.
gtp_control	GTP control-plane messages.
gtp_prime	GTP prime charging messages.
guildwars2_sts	Guild Wars 2 STS service opening.
h323	H.323 call-signaling metadata.
hamachi	Hamachi tunnel-control opening.
hcl_notes	HCL Notes/Domino service opening.
hl7	HL7 healthcare-message framing.
hls	HLS playlist markers and media metadata.
hsrp	Hot Standby Router Protocol messages.
http1	HTTP/1 request authority, target, headers and visible response.
http2	HTTP/2 connection preface and visible frame metadata.
iax	IAX telephony signaling.
igmp	IGMP multicast membership messages.
ike	IKE security-association negotiation metadata.
imap	IMAP command and response metadata.
ip_in_ip	IP-in-IP encapsulation headers.
ipsec_ah	IPsec Authentication Header fields.
ipsec_esp	IPsec ESP envelope metadata without decryption.
irc	IRC commands and registration dialogue.
iscsi	iSCSI login and command header metadata.
jrmi	Java RMI wire handshake.
json_rpc	JSON-RPC request and response metadata.
kafka	Kafka API request and response framing.
kcp	KCP reliable-datagram header structure.
kerberos	Kerberos message and principal metadata.
kismet	Kismet remote-capture service framing.
l2tp	L2TP tunnel-control headers.
lagofast	LagoFast tunnel-service opening.
ldap	LDAP operation metadata and visible credential-field presence.

Continued on next page

Observed label	Meaning and visible scope
ldp	Label Distribution Protocol messages.
libp2p	libp2p protocol opening.
lisp	LISP mapping and control messages.
lustre	Lustre distributed-filesystem framing.
megaco	H.248/Megaco media-gateway messages.
memcached	Memcached binary-protocol message metadata.
mgcp	MGCP media-gateway commands.
mikrotik	MikroTik service and discovery messages.
monero	Monero peer-service opening.
mongodb	MongoDB wire-message headers.
mpegdash	MPEG-DASH manifest metadata.
mpegts	MPEG transport-stream packet structure.
ms_rpch	Microsoft RPC-over-HTTP visible framing.
msdo	Microsoft Delivery Optimization framing.
mudfish	Mudfish tunnel-service opening.
munin	Munin monitoring-service opening.
mysql	MySQL handshake and command metadata.
nano	Nano cryptocurrency peer messages.
natpmp	NAT-PMP port-mapping messages.
nats	NATS messaging-protocol opening.
netbios	NetBIOS name-service messages.
netflow	NetFlow and IPFIX exporter header metadata.
nexon	Nexon service opening.
nfs	NFS remote-filesystem operation metadata.
nomachine	NoMachine remote-access handshake.
ntp	NTP time-service headers.
nvme_tcp	NVMe/TCP connection-initialization metadata.
openflow	OpenFlow version negotiation and messages.
openvpn	OpenVPN control and handshake metadata.
openwire	ActiveMQ OpenWire protocol handshake.
oracle_tns	Oracle TNS connection metadata.
ospf	OSPF routing messages.
pcp	Port Control Protocol mapping messages.
pfcp	PFCP mobile-core control messages.
pgm	PGM reliable-multicast headers.
pim	PIM multicast-routing messages.
pop3	POP3 greeting and command metadata.
postgres	PostgreSQL startup and authentication metadata.
pptp	PPTP tunnel-control messages.
proxy	Proxy-protocol visible connection preface.

Continued on next page

Observed label	Meaning and visible scope
quic	QUIC long-header and verified Initial handshake metadata.
radius	RADIUS authentication and accounting message metadata.
radmin	Radmin remote-access opening.
raknet	RakNet game-network message framing.
rdp	RDP connection negotiation metadata.
resp	Redis RESP command and response framing.
rfb	RFB/VNC remote-desktop handshake.
riotgames	Riot Games service opening.
rmcp	RMCP management messages.
roughtime	Roughtime signed-time envelope.
rsync	rsync service handshake.
rtmp	RTMP streaming-media handshake.
rtp	RTP media transport headers.
rtsp	RTSP streaming-session signaling.
samsung_discovery	Samsung device-discovery messages.
sctp	SCTP association and chunk metadata.
sflow	sFlow exporter header metadata.
sip	SIP method, status and signaling headers.
skinny	Cisco Skinny call-control messages.
slp	Service Location Protocol messages.
smb	SMB2/3 visible commands, share and file-operation metadata.
smpp	SMPP SMS-gateway messages.
smtp	SMTP visible mail-session commands and responses.
snmp	SNMP message and visible PDU metadata.
soap	SOAP envelope metadata over visible HTTP.
socks	SOCKS proxy negotiation and destination fields.
softether_discovery	SoftEther VPN discovery/control opening.
source_engine	Source Engine server-query messages.
ssdp	SSDP service-discovery messages.
ssh	SSH banners, algorithm offers and key-exchange metadata.
steam_discovery	Steam local/service discovery messages.
stomp	STOMP messaging frame metadata.
stun	STUN transaction and attribute metadata.
syncthing	Syncthing discovery and transfer framing.
syslog	Syslog message headers.
tacacs	TACACS+ authentication/control metadata.
tailscale_disco	Tailscale discovery messages.
tds	SQL Server TDS connection metadata.
teamspeak	TeamSpeak voice-service opening.
telnet	Telnet negotiation and visible service metadata.

Continued on next page

Observed label	Meaning and visible scope
teredo	Teredo IPv6-over-UDP encapsulation.
tftp	TFTP read/write request and block metadata.
thrift	Apache Thrift message framing.
tls	Visible TLS handshake, SNI, ALPN and certificate metadata.
tplink	TP-Link device-discovery/control messages.
ubiquiti_discovery	Ubiquiti device-discovery messages.
uftp	UFTP multicast file-transfer control.
ultrasurf	UltraSurf service opening.
usenet	NNTP/Usenet service dialogue.
valve_sdr	Valve SDR relay opening.
vrrp	VRRP router-redundancy messages.
vxlan	VXLAN overlay header metadata.
webdav	WebDAV methods and visible HTTP metadata.
wireguard	WireGuard handshake message metadata.
wsd	WS-Discovery messages.
x509	Visible X.509 identity, validity and self-signature metadata.
xdmcp	XDMCP display-manager messages.
xmpp	XMPP stream-opening metadata.
yojimbo_netcode	Yojimbo Netcode session framing.
z3950	Z39.50 information-retrieval messages.
zabbix	Zabbix agent/server protocol opening.
zmtp	ZeroMQ ZMTP handshake.

10 Using this guide

Use the guide to choose relevant traffic, create customer-specific policies and plan a validation session. Start with a known protocol, inspect an observation, tune a rule and run its positive and negative controls. Follow any automated response through to the downstream result.

Catalog edition. 28 November 2026. The guide is generated from the current native application/protocol dictionary, Atlas behavior catalog and Sigma template catalog. Product workflows follow the current Operations Guide. Counts describe catalog entries, not throughput or the number of detections enabled by default.

Learn more. streamingdefense.com