Streaming Defense System Training Guide

Component Methodology, Operating Features, and Competitive Strength

---

AOT | Investigator | n8n Automation | MISP Ticketing | Superset Analytics | ClickHouse Big Data

---

Prepared for broad internal training across Streaming Defense operations, engineering, analyst, and partner teams.

Signal. Structure. Strength.

Contents

1 Purpose and Training Philosophy

This document provides a broad training foundation for the major components of the Streaming Defense operating system. It is intended for executives, analysts, operators, engineers, integration partners, and customer-facing technical teams that need to understand how the system works as an integrated capability rather than as isolated tools.

The Streaming Defense platform should be taught as a connected methodology:

1. **Observe:** capture high-volume network, telemetry, and external signal streams through the Attack Operations Theater and related firehoses.
2. **Classify:** normalize, enrich, and classify events into risk, protocol, entity, geography, infrastructure, and behavioral context.
3. **Investigate:** apply playbooks, triage logic, threat intelligence, and analyst-facing evidence generation through Investigator.
4. **Automate:** use n8n workflows to route outcomes, trigger enrichment, create follow-up actions, and connect external systems.
5. **Ticket:** transform important evidence into structured MISP events, tickets, attributes, and threat-intelligence records.
6. **Analyze:** use Superset to explore operational performance, security posture, risk patterns, trend lines, and executive dashboards.
7. **Persist:** use ClickHouse as the large-scale analytical foundation for high-throughput event storage and low-latency query workloads.

Training Goal

Every learner should leave training able to explain what each component does, how it fits into the full Streaming Defense workflow, what evidence it produces, how operators use it, and why the architecture creates competitive strength.

2 System-Wide Methodology

2.1 Core Operating Model

Streaming Defense is designed around a real-time security and prediction operating loop. The system ingests signals, converts them into structured observations, enriches those observations, evaluates risk, produces analyst-ready outcomes, and enables automation. The result is not only detection, but a repeatable operating methodology for turning raw network and business signals into action.

Stage	Methodology	Training Emphasis
Signal Acquisition	Capture full-take or targeted telemetry from network, application, threat intelligence, and external data sources.	Teach how collection works, what data is available, what is filtered, and where raw versus normalized data exists.
Signal Structuring	Normalize observations into consistent schemas, fields, identifiers, timestamps, and entities.	Teach schema literacy, evidence fields, event identity, and query-safe interpretation.

Context Enrichment	Add protocol, geography, threat intelligence, asset, severity, risk, and relationship context.	Teach enrichment logic and the difference between observed facts and inferred context.
Investigation	Apply playbooks, severity gates, triage logic, event grouping, and repeatable response methods.	Teach how an analyst moves from alert to evidence-backed decision.
Automation	Trigger workflows for enrichment, routing, notification, ticketing, and system-to-system actions.	Teach safe automation design, approval gates, auditability, and rollback.
Ticketing and Intelligence	Convert evidence into structured MISP records and shareable threat-intelligence artifacts.	Teach how an incident becomes an intelligence object, and how tags, attributes, and distribution should be handled.
Analytics	Visualize operational trends, detection performance, investigation throughput, customer posture, and executive metrics.	Teach dashboards, data trust, chart interpretation, and query boundaries.
Big Data Persistence	Store and query high-volume event records in ClickHouse.	Teach partitions, retention, schemas, columnar querying, and high-cardinality analytics.

2.2 Teaching Principles

Training should follow a layered approach. Start with the operational story, then the component, then the interface, then the data model, then a hands-on exercise. This avoids teaching the platform as a list of screens or scripts and instead teaches it as an evidence pipeline.

1. **Begin with the mission:** why the component exists.
2. **Explain the inputs and outputs:** what data comes in and what evidence goes out.
3. **Map the operator workflow:** what an analyst, engineer, or customer does with it.
4. **Show the schema:** what fields matter and how they should be interpreted.
5. **Run a scenario:** use a realistic detection, investigation, ticket, automation, and dashboard path.
6. **Compare competitively:** show what Streaming Defense does differently from conventional SIEM, EDR, NDR, SOAR, BI, and data-lake patterns.

3 Attack Operations Theater (AOT)

3.1 Explanation

The Attack Operations Theater is the Streaming Defense real-time network defense and operations environment. AOT is the primary front-end for observing network behavior, triaging high-risk events, viewing geospatial activity, understanding protocol and flow context, and presenting analyst-ready evidence from live telemetry.

AOT should be understood as more than a dashboard. It is the operational theater where network events become visible, explainable, and actionable. It gives analysts a real-time view into what is happening across monitored environments, while preserving enough structure for downstream investigation, automation, and reporting.

3.2 Methodology

AOT follows a full-take visibility methodology. Instead of depending only on endpoint agents, log forwarding, or sampled events, AOT emphasizes network-derived evidence. This creates a broad observational layer that can see behavior even when endpoint tooling is absent, disabled, incomplete, or outside administrative control.

1. **Collect:** receive network telemetry from probes, collectors, SPAN, TAP, or related ingestion paths.
2. **Decode:** classify protocols, flows, IPs, ports, payload metadata, encryption state, and application context.
3. **Enrich:** add geography, ASN, ISP, threat intelligence, severity, and asset context.
4. **Prioritize:** elevate suspicious events using severity, risk scores, known threat indicators, behavior, and playbook logic.
5. **Display:** present real-time observations, maps, feeds, investigator outcomes, and operational status.
6. **Export:** send structured evidence to Investigator, MISP, automation workflows, analytics, and ClickHouse.

3.3 Core Features

- Real-time network observation and high-volume packet/flow visibility.
- Protocol and application classification.
- Threat stream views for high-risk activity.
- Geospatial and ASN/ISP context.
- Severity and risk-oriented event presentation.
- Integration with threat intelligence and investigator playbooks.
- Support for sovereign, private-cloud, and air-gapped deployments.
- Operator-facing evidence views for rapid triage.

3.4 Training Topics

Topic	What to Teach	Exercise
Live Event Flow	How network events move from collection to UI.	Follow one event from collector input to AOT display.
Risk Context	How severity, score, geography, protocol, and threat intelligence affect triage.	Compare a high-severity event to a low-severity event.
Threat Stream	How analysts use recent high-risk events.	Identify the top three events requiring action.
Geospatial View	How maps help identify infrastructure, destination regions, and anomalous behavior.	Trace external communication by country, ASN, and protocol.
Investigator Integration	How AOT displays enriched investigator outcomes.	Open an investigator result from AOT and explain the evidence.

3.5 Competitive Strength

AOT's competitive strength is that it creates a defensible network-centered source of truth. Traditional SIEM deployments often rely on logs that may be incomplete, delayed, inconsistently formatted, or dependent on upstream systems. Endpoint-centric platforms can miss unmanaged devices, network appliances, shadow IT, third-party systems, OT assets, and externally hosted infrastructure. AOT provides an independent observational layer that is valuable in enterprise, industrial, sovereign, and air-gapped environments.

The strongest competitive argument is that AOT does not merely collect alerts. It captures operational signals, structures them into evidence, and exposes them to investigation, automation, and analytics. This supports faster triage, better visibility, and stronger customer confidence.

4 Investigator

4.1 Explanation

Investigator is the Streaming Defense triage, playbook, and evidence-generation layer. Where AOT shows real-time activity, Investigator applies structured reasoning to selected events and patterns. It converts network observations into investigator outcomes that analysts can understand, explain, ticket, and defend.

Investigator should be taught as the bridge between raw telemetry and analyst decision. It reduces the burden of manually inspecting every event by applying repeatable rules, playbooks, thresholds, suppression logic, enrichment, and outcome classification.

4.2 Methodology

Investigator methodology is based on disciplined evidence development:

1. **Select:** identify candidate events from AOT, ClickHouse, or real-time streams.
2. **Normalize:** standardize event structure so playbooks can evaluate fields consistently.
3. **Enrich:** add threat intelligence, geography, asset context, historical context, and severity.
4. **Evaluate:** apply playbooks, gates, thresholds, and suppression logic.
5. **Explain:** produce an outcome with evidence, reasoning, severity, and recommended handling.
6. **Route:** send significant outcomes to AOT, MISP, n8n, Superset, or other operational systems.

4.3 Core Features

- Detection-specific playbook logic.
- Threat intelligence enrichment.
- Severity and confidence gating.
- Evidence summarization for analysts.
- Suppression and deduplication controls.
- Outcome streams for downstream UI and automation.
- Support for customer-specific operating rules.
- ClickHouse-backed historical investigation and context retrieval.

4.4 Training Topics

Topic	What to Teach	Exercise
Playbook Logic	How detections are transformed into investigation outcomes.	Walk through an exfiltration playbook from raw flow to finding.
Evidence Discipline	Difference between observed fact, enrichment, and inference.	Label each field in a result as observed, enriched, or derived.
Suppression	How repeat events are controlled to avoid analyst fatigue.	Tune a noisy detection without hiding real risk.
Threat Intelligence	How TIP and MISP context influence investigation.	Compare the same flow with and without threat intelligence hits.
Outcome Routing	How findings move to AOT, MISP, and automation.	Trace an investigator outcome into a downstream ticket.

4.5 Competitive Strength

Investigator strengthens Streaming Defense by turning network visibility into explainable outcomes. Many tools generate alerts, but fewer produce evidence that is both operationally useful and defensible. Investigator's strength is its ability to apply customer-specific rules, severity gates, and structured playbooks while retaining the underlying network facts.

This creates competitive differentiation against platforms that rely on opaque risk scoring, black-box AI summaries, or isolated alerts. Investigator emphasizes explainability, evidence lineage, and repeatability.

5 Automation with n8n

5.1 Explanation

n8n is used as the Streaming Defense workflow automation layer. In the broader system, automation is responsible for connecting detection and investigation outcomes to follow-up actions: enrichment, notifications, ticket creation, reporting, routing, approvals, and external integrations.

n8n describes a workflow as a collection of connected nodes that automate a process. This model fits Streaming Defense because security operations frequently require repeatable multi-step routing across APIs, databases, ticketing systems, messaging tools, and customer-specific systems.

5.2 Methodology

Automation training should emphasize safety and control. Security automation must be reliable, auditable, reversible, and bounded. The goal is not to automate every action immediately, but to automate the repeatable actions that reduce time-to-response without creating operational risk.

1. **Trigger:** receive an investigator outcome, scheduled event, webhook, or manual operator action.
2. **Validate:** check required fields, severity, tenant, confidence, and policy constraints.
3. **Enrich:** call additional APIs or databases for context.
4. **Decide:** branch workflow logic based on risk, customer rules, and approval requirements.
5. **Act:** create a MISP event, notify a team, update a record, or start an approval process.
6. **Audit:** log execution status, errors, operator approvals, and final outcome.

5.3 Core Features

- Node-based workflow design.
- Webhook-triggered automation.
- API integration with Streaming Defense services.
- Conditional branching and validation.
- Error handling and retry logic.
- Scheduled jobs for recurring checks.
- Human approval steps for sensitive actions.
- Execution history for troubleshooting and audit.

5.4 Training Topics

Topic	What to Teach	Exercise
Workflow Anatomy	Triggers, nodes, credentials, branches, and executions.	Build a simple webhook-to-notification workflow.
Safe Automation	Approval gates, allowlists, dry-run modes, and rollback.	Add a manual approval step before ticket creation.
Streaming Defense API Calls	How workflows consume investigator outcomes and system APIs.	Pull an outcome and enrich it with a ClickHouse query.
Error Handling	How to handle missing fields, API failures, and retries.	Simulate an API failure and inspect the execution trace.
Auditability	How automation proves what it did and why.	Produce an audit summary from execution metadata.

5.5 Competitive Strength

The competitive strength of n8n within Streaming Defense is flexibility. Instead of hard-coding every integration into the product, Streaming Defense can provide customer-specific workflows that adapt to local policies, ticketing requirements, escalation paths, and compliance environments.

This is especially important for sovereign and air-gapped deployments, where customers may have internal systems that cannot be accessed by cloud-native SOAR products. A self-hosted workflow approach allows Streaming Defense to preserve control, locality, and customization while still enabling modern automation.

6 Ticketing and Threat Intelligence with MISP

6.1 Explanation

MISP is the Streaming Defense ticketing and threat-intelligence collaboration layer. MISP is an open-source platform for collecting, storing, distributing, and sharing cybersecurity indicators and threat information. In Streaming Defense, MISP can be used to transform significant detections, investigator outcomes, and threat indicators into structured records that support response, sharing, and historical intelligence.

MISP should be taught as both a ticketing destination and a threat-intelligence system. A Streaming Defense finding can become a MISP event containing attributes, tags, categories, threat levels, indicators,

and analyst context.

6.2 Methodology

1. **Create event:** generate a structured MISP event from a validated investigator outcome.
2. **Add attributes:** include IPs, domains, URLs, hashes, protocols, ports, ASNs, or other observables.
3. **Apply tags:** mark severity, confidence, tenant, detection type, campaign, sector, or handling instructions.
4. **Control distribution:** set sharing boundaries appropriate to customer and classification rules.
5. **Correlate:** use MISP's correlation capabilities to connect related indicators and events.
6. **Operationalize:** feed confirmed intelligence back into detection, investigation, and reporting workflows.

6.3 Core Features

- Structured cyber-threat intelligence events.
- Indicator and observable management.
- Tags, taxonomies, galaxies, and classifications.
- Distribution and sharing controls.
- Event correlation.
- API-driven ticket and event creation.
- Support for analyst notes and contextual enrichment.
- Integration with detection and monitoring tools.

6.4 Training Topics

Topic	What to Teach	Exercise
MISP Event Model	Events, attributes, tags, threat levels, and distribution.	Create a MISP event from an exfiltration finding.
Indicator Quality	How to distinguish strong indicators from weak context.	Decide which observables should become attributes.
Sharing Controls	Distribution, classification, and customer-specific rules.	Configure a private event versus shareable intelligence.
Correlation	How MISP links related indicators and campaigns.	Find related events by IP or domain.
Feedback Loop	How MISP intelligence improves future detection.	Feed a confirmed malicious indicator back into TIP logic.

6.5 Competitive Strength

MISP gives Streaming Defense a structured threat-intelligence and ticketing model that is open, extensible, and compatible with analyst workflows. Instead of generating unstructured alerts or isolated notifications,

Streaming Defense can create intelligence objects that preserve evidence, context, and sharing controls.

The competitive strength is the ability to move from detection to operational intelligence. This supports customers that need repeatable evidence handling, incident collaboration, sovereign control of intelligence, and integration with broader threat-sharing communities.

7 Analytics with Apache Superset

7.1 Explanation

Apache Superset is the Streaming Defense analytics and visualization layer. Superset is a modern data exploration and data visualization platform that can augment or replace proprietary business intelligence tools. Within Streaming Defense, Superset allows technical and business users to explore ClickHouse-backed security and operations data through dashboards, charts, SQL Lab, filters, and role-based views.

Superset should be taught as the layer that turns operational history into decision support. AOT answers what is happening now; Investigator explains what matters; Superset shows trends, patterns, performance, posture, and outcomes over time.

7.2 Methodology

1. **Define the question:** identify the operational, security, or executive question being answered.
2. **Select the dataset:** use trusted ClickHouse tables or views.
3. **Choose measures:** define counts, rates, percentiles, severities, volumes, or time windows.
4. **Choose dimensions:** group by protocol, asset, tenant, geography, severity, playbook, ASN, or time.
5. **Visualize:** select charts that answer the question clearly.
6. **Validate:** confirm that the dashboard does not misrepresent incomplete, stale, or filtered data.
7. **Operationalize:** publish dashboards for analyst, engineering, executive, or customer use.

7.3 Core Features

- Dashboards and charts for security and operational analytics.
- SQL Lab for advanced investigation and exploration.
- No-code visualization builder for common use cases.
- Integration with ClickHouse and other data sources.
- Role-based access and dashboard sharing.
- Time-series analysis, filters, and drilldowns.
- Executive, analyst, and engineering reporting views.

7.4 Training Topics

Topic	What to Teach	Exercise
Dataset Literacy	How Superset connects to trusted ClickHouse tables.	Build a dataset from a normalized event table.

Dashboard Design	How to match charts to operational questions.	Build a dashboard for high-risk events by severity and region.
SQL Lab	How technical users explore data safely.	Query event volume by protocol and time bucket.
Executive Reporting	How to summarize risk, throughput, and outcomes.	Create a weekly security posture dashboard.
Data Trust	How to identify stale, partial, or misleading views.	Validate dashboard totals against ClickHouse.

7.5 Competitive Strength

Superset gives Streaming Defense a flexible analytics layer without forcing customers into expensive or closed BI ecosystems. The combination of Superset and ClickHouse is powerful because it enables high-volume analytics, custom dashboards, and role-specific views while preserving data locality.

The competitive strength is that Streaming Defense can serve multiple audiences from the same evidence foundation: analysts, engineers, executives, partners, and customers. This reduces the gap between operational data and business decision-making.

8 Big Data with ClickHouse

8.1 Explanation

ClickHouse is the Streaming Defense big-data analytical foundation. ClickHouse is a column-oriented database, meaning data is stored by column rather than by row. This design is highly effective for analytical queries that scan large volumes of events but only need selected fields. In Streaming Defense, ClickHouse is used to persist network events, investigator outcomes, firehose observations, metrics, and other high-volume records.

ClickHouse should be taught as the system of record for high-throughput analytical workloads. It is not simply a storage engine; it is the query substrate that enables historical investigation, dashboarding, replay, aggregation, and evidence validation.

8.2 Methodology

1. **Ingest:** write structured events using batch inserts and schema-safe formats.
2. **Partition:** organize data by time and operational boundaries for efficient retention and query performance.
3. **Compress:** exploit columnar storage and compression for large event volumes.
4. **Query:** aggregate by time, severity, entity, geography, protocol, playbook, or tenant.
5. **Retain:** apply retention policies appropriate to customer, regulatory, and storage requirements.
6. **Serve:** provide data to AOT, Investigator, Superset, automation, and reporting systems.

8.3 Core Features

- Columnar analytical storage.
- High-throughput event insertion.
- Fast aggregation over large datasets.

- Compression-efficient storage for telemetry.
- SQL-based investigation and reporting.
- Time-series and event-history analysis.
- Support for materialized views and summary tables.
- Retention and partition management.

8.4 Training Topics

Topic	What to Teach	Exercise
Columnar Concepts	Why columnar storage helps analytical workloads.	Compare a query that reads three columns versus many columns.
Schema Literacy	Core event fields, timestamp fields, severity, tenant, protocol, and IDs.	Identify required fields for an investigation query.
Batch Inserts	Why batch writes matter for high-volume telemetry.	Review an insert pattern and identify inefficient writes.
Retention	How TTL and partitions manage data lifecycle.	Design a 30-day retention policy for packet-derived events.
Analytical Queries	Aggregations by time, risk, protocol, geography, and asset.	Write a query for top external destinations over 24 hours.

8.5 Competitive Strength

ClickHouse gives Streaming Defense the ability to analyze large volumes of structured event data quickly and economically. This is a major competitive advantage over architectures that rely on expensive SIEM indexing, slow data lakes, or fragmented storage tiers.

Because ClickHouse supports fast analytical queries across high-volume telemetry, Streaming Defense can preserve richer evidence and still support operational responsiveness. This enables historical investigation, performance reporting, customer dashboards, and high-cardinality security analytics.

9 Integrated Training Scenario

9.1 Scenario: Large Data Movement with Threat Intelligence Context

This scenario trains all components together.

1. AOT displays a large outbound movement from an internal source to an external destination.
2. The event contains protocol, geography, ASN, byte count, packet count, and risk context.
3. Investigator evaluates the event using an exfiltration or unusual movement playbook.
4. Investigator enriches the event with threat intelligence and historical context from ClickHouse.
5. If the severity and confidence are sufficient, n8n receives the outcome and validates required fields.
6. n8n creates or updates a MISP event with the destination IP, source context, detection type, and handling tags.
7. ClickHouse retains the full event history for investigation, replay, and trend analysis.

8. Superset displays weekly counts, affected assets, top destinations, escalation outcomes, and analyst throughput.

9.2 Scenario Learning Objectives

- Explain why AOT saw the behavior before a traditional ticket existed.
- Explain how Investigator separated evidence from inference.
- Explain how n8n safely routed the outcome.
- Explain how MISP preserved the incident as a structured intelligence record.
- Explain how ClickHouse enabled historical context and aggregation.
- Explain how Superset turned the incident into management-level reporting.

10 Competitive Positioning Summary

Component	Typical Market Pattern	Streaming Defense Strength
AOT	Dashboards often depend on logs, agents, sampled data, or delayed SIEM pipelines.	Real-time network-centered observation and operational theater for high-volume signal visibility.
Investigator	Alerts may be noisy, opaque, or disconnected from evidence.	Playbook-driven, evidence-backed, explainable investigation outcomes.
n8n Automation	SOAR platforms can be expensive, rigid, or difficult to deploy in private environments.	Flexible, self-hostable, API-driven workflow automation aligned to customer policy.
MISP Ticketing	Tickets are often unstructured and disconnected from threat intelligence.	Structured intelligence events with attributes, tags, sharing controls, and correlation.
Superset Analytics	BI may be separated from security evidence or locked into proprietary platforms.	Open analytics on trusted security data with dashboards for analysts, engineers, and executives.
ClickHouse Big Data	SIEM indexing and generic data lakes may be costly or slow for high-volume telemetry.	Fast columnar analytics for large-scale event persistence, aggregation, and investigation.

11 Recommended Training Program

11.1 Day 1: Platform Overview and AOT

- Streaming Defense mission and architecture.
- AOT user interface and event lifecycle.
- Network visibility methodology.
- Hands-on: identify and explain top high-risk events.

11.2 Day 2: Investigator and Evidence Discipline

- Investigator playbooks and evidence model.
- Severity, confidence, suppression, and enrichment.
- Hands-on: produce a defensible investigation summary.

11.3 Day 3: MISP and n8n

- MISP event and attribute model.
- n8n workflow design and safe automation.
- Hands-on: route an investigator outcome into a MISP event through automation.

11.4 Day 4: ClickHouse and Superset

- ClickHouse schemas, retention, query patterns, and performance concepts.
- Superset datasets, SQL Lab, dashboards, and executive reporting.
- Hands-on: build a dashboard for high-risk network movement by severity, region, and destination.

11.5 Day 5: Integrated Capstone

- End-to-end scenario from live observation to ticket to analytics.
- Team exercise: explain the full evidence chain.
- Competitive positioning workshop.
- Certification-style review questions.

12 Role-Based Learning Paths

Role	Primary Focus	Must Be Able To Explain
Executive	Value, differentiation, customer outcomes, risk reduction.	Why Streaming Defense is more than a dashboard or SIEM replacement.
SOC Analyst	AOT, Investigator, MISP, evidence interpretation.	How to move from event to defensible finding.
Security Engineer	Collection, enrichment, schemas, automation, retention.	How the data moves and where controls are applied.
Data Analyst	ClickHouse and Superset.	How to build trusted dashboards and avoid misleading analytics.
Automation Engineer	n8n workflows, API integrations, approval gates.	How to automate safely without bypassing policy.
Partner Engineer	Integration points and APIs.	How partner tools consume Streaming Defense evidence.
Customer Success	Demonstrations, outcomes, dashboards, reporting.	How to show operational value to customer stakeholders.

13 Review Questions

1. What is the difference between AOT visibility and Investigator evidence?
2. Why does Streaming Defense place emphasis on network-derived evidence?
3. What makes an Investigator outcome defensible?
4. When should n8n automation require a manual approval gate?
5. What fields should be included when converting an investigator outcome into a MISP event?
6. Why is ClickHouse appropriate for high-volume telemetry analytics?
7. What are the risks of building Superset dashboards on incomplete or stale data?
8. How does MISP help transform a detection into reusable threat intelligence?
9. How should an analyst distinguish observed facts from enriched context?
10. What is the competitive advantage of combining AOT, Investigator, MISP, n8n, Superset, and ClickHouse into one operating model?

14 Reference Notes

The component descriptions in this training guide align Streaming Defense operating concepts with publicly documented third-party component roles. MISP is described by its project as an open-source platform for collecting, storing, distributing, and sharing cybersecurity indicators and threat information. ClickHouse documentation describes ClickHouse as a column-oriented database designed around columnar storage. Apache Superset documentation describes Superset as a modern data exploration and visualization platform. n8n documentation describes workflows as connected nodes used to automate a process.

References

[1] MISP Project, *MISP Open Source Threat Intelligence Platform and Open Standards for Threat Information Sharing*, https://www.misp-project.org/.

[2] MISP Project, *MISP Documentation*, https://www.misp-project.org/documentation/.

[3] ClickHouse, *What is ClickHouse?*, https://clickhouse.com/docs/intro.

[4] Apache Superset, *Introduction*, https://superset.apache.org/user-docs/intro/.

[5] n8n Documentation, *Workflows*, https://docs.n8n.io/workflows/.