Project Horizon

XDR & Insider Risk Implementation Report

Project Title: Project Horizon - Unified Zero Trust Architecture
Document Type: Technical Implementation

1. Executive Summary

The objective of this solution was to design and implement a **comprehensive Extended Detection and Response (XDR) and Insider Risk Monitoring system** that centralizes security telemetry, enables real-time detection and response, and applies behavioral analytics to identify anomalous user activity. This aligns with broader security objectives of achieving **holistic visibility**, **early threat detection**, and **automated response** within a unified open-source security stack.

The deployed system integrates multiple telemetry sources including **ZTNA authentication logs**, **DSPM alerts**, **CNAPP scan outputs**, **network IDS events**, and **Kubernetes policy logs** into a centralized **ELK Stack** based SIEM. Agents and collectors were deployed across the IAM host, Kubernetes nodes, DSPM data stores, and monitoring infrastructure to ensure wide coverage. Detection rules were developed for each telemetry type, covering scenarios such as failed or suspicious logins, DLP violations, IaC misconfigurations, and network intrusion attempts.

On top of this foundation, a dedicated **User and Entity Behavior Analytics (UEBA)** subsystem was built to detect anomalous SSH login activity using **per-user behavioral baselines** and **Isolation Forest–based anomaly detection**. This subsystem enriches login data with geolocation, ASN, and reputation lookups (VirusTotal), then scores anomalies for SOC triage. Analyst and stakeholder dashboards provide interactive visualizations, while alerting pipelines deliver HTML-formatted notifications for high and critical anomalies.

The system is further enhanced with **Tines automation playbooks**, enabling enrichment, alerting, and host isolation workflows for critical severity detections. Together, these components form a **functional XDR ecosystem** that bridges identity, data, network, and behavioral telemetry, and supports both rule-based and ML-driven detections.

This implementation demonstrates a **mature, open-source–driven XDR and Insider Risk solution** that provides end-to-end visibility, actionable detection, and automated response. It establishes a strong operational foundation that can be expanded for enterprise-scale deployments with additional integrations, scaling, and advanced correlation logic.

2. Introduction

2.1 Requirements

Market required the deployment of a **centralized detection and response system** capable of ingesting diverse telemetry sources, detecting both known and unknown threats, and providing actionable insights to security analysts in real time. The solution needed to address the following core requirements:

- **Comprehensive Telemetry Aggregation:** Collect logs and security events from multiple layers of the environment ZTNA, DSPM, CNAPP, network IDS, and endpoint agents into a single, scalable platform for analysis.
- **Real-Time Detection & Response:** Implement detection rules for high-fidelity threat scenarios (e.g., authentication anomalies, data exposure, network intrusions, misconfigurations) and automate alerting and response workflows for critical events.
- **Behavioral Analytics for Insider Risk:** Introduce a UEBA mechanism to detect subtle, non-signature-based anomalies in user behavior (e.g., unusual SSH logins), complementing traditional rule-based detection.
- **Actionable Dashboards:** Provide SOC analysts and stakeholders with interactive, real-time dashboards and KPIs to visualize security posture, investigate incidents, and prioritize response.
- **Automation & Enrichment:** Reduce analyst workload and mean time to respond (MTTR) by automating enrichment (e.g., VirusTotal) and response actions (e.g., email alerts).
- **Scalability & Extensibility:** Build the solution using open-source components and modular architecture so that additional data sources, detection rules, and response actions can be integrated over time without vendor lock-in.

2.2 Solution Implemented

To meet these requirements, a comprehensive **XDR and Insider Risk Monitoring system** was deployed by combining the **ELK Stack**, **Tines automation**, and a custom-built **UEBA subsystem**:

- **EDR / SIEM Core (ELK Stack)**
    - **Telemetry Ingestion:** Logs were collected from multiple layers:
        - Pomerium authentication logs (ZTNA)
        - Suricata IDS alerts (network)
        - Presidio DLP alerts and Custodian remediation logs (DSPM)
        - Churn model alerts for anomalous email activity (CDP)
        - Chekhov and Kyverno IaC scan results (CNAPP)
        - pfSense firewall and routing logs (ZTNA perimeter)
    - **Deployment:** Elastic Agents were installed on the IAM machine, Kubernetes cluster node, DSPM datastore machine, and a test machine to validate experimental log pipelines.
    - **Dashboards:** Dedicated Kibana dashboards were built for each telemetry type, focusing on detection-oriented KPIs and real-time monitoring.
    - **Detection Rules:** Implemented for failed/suspicious logins, sensitive data alerts, IaC misconfigurations, IDS signatures, and Kubernetes anomalies.
- **UEBA Subsystem (SSH Anomaly Detection)**
    - Developed to detect **anomalous SSH login behavior** on Linux hosts using per-user baselines derived from logs-system.auth-* indices.
    - **Features engineered:** login time patterns, weekday distribution, off-hour flags, IP rarity, ASN changes, method changes, and host usage trends.
    - **Modeling:** Used Isolation Forest per user, with fallback to a global model for sparse data; anomalies scored 0–1 and classified (Low–Critical).
    - **Enrichment:** Geo/IP lookups, VirusTotal threat intel integration.

    - **Dashboards:** Streamlit dashboards provide analyst and stakeholder views, including KPI tiles, heatmaps, geo maps, anomaly timelines, and drill-downs.
    - **Alerts:** High/Critical anomalies generate professional HTML email alerts with full context and recommendations.
- **Automation Layer (Tines)**
    - Automated playbooks handle VirusTotal enrichment, email notifications, and host isolation for critical alerts.
    - Reduces manual workload and ensures standardized response actions.

This solution integrates **rule-based detections**, **machine-learning behavioral analytics**, and **automated response mechanisms** within a single operational ecosystem, aligning directly with XDR and Insider Threat Detection goals.

3. Scope

3.1 Current Scope

The current implementation focuses on deploying a **fully functional XDR and Insider Risk prototype** using open-source components, covering telemetry ingestion, detection engineering, behavioral analytics, and automated response within a controlled lab environment. The scope includes:

- **Centralized Log Aggregation:**
  Collection of telemetry from multiple layers of the environment into the ELK Stack for unified analysis:
    - Pomerium authentication logs (ZTNA)
    - Suricata IDS alerts (network)
    - Presidio DLP and Custodian remediation logs (DSPM)
    - Churn model alerts for anomalous email behavior (CDP)
    - Chekhov IaC scan logs and Kyverno policy violations (CNAPP)
    - pfSense firewall and routing logs (ZTNA perimeter)

- **Detection Engineering:**
  Creation of targeted detection rules for key threat scenarios including failed/suspicious logins, sensitive data alerts, network exploits, misconfigurations, and Kubernetes anomalies.
- **Real-Time Dashboards:**
  Development of Kibana dashboards and visualizations for each telemetry type, with SOC-focused KPIs to support investigation and triage.
- **UEBA for Insider Risk:**
  Deployment of a per-user SSH anomaly detection engine using behavioral baselines and Isolation Forest models, integrated with geolocation and reputation enrichment, and presented via dedicated Streamlit dashboards.
- **Automation Layer:**
  Integration of Tines for enrichment and response workflows, including VirusTotal lookups, email alerts, and host isolation for high-severity alerts.

This scope demonstrates a **complete XDR pipeline**: telemetry collection → detection → enrichment → visualization → automated response.

3.2 Constraints

The current prototype operates under several constraints due to its open-source and lab-oriented design:

- **Single-node deployments:** All core ELK components, UEBA engine, and Tines automations run on single machines, without clustering or horizontal scaling.
- **Limited retention and storage:** Log retention is configured for short-term testing, not long-term archival or compliance-grade storage.
- **No federated identity integration:** The insider risk UEBA model is limited to SSH logs and does not yet correlate with enterprise IdPs or identity graphs.
- **Simplified network environment:** IDS and pfSense monitoring are performed in a contained virtual network; no WAN or distributed branch scenarios are simulated.
- **Manual onboarding of data sources:** Log pipelines are configured individually; no self-service or automated onboarding mechanisms exist yet.

- **Basic security controls:** Access to dashboards and tools uses basic authentication; MFA and granular RBAC are not yet implemented.

These constraints are deliberate, focusing the prototype on demonstrating functional integration and detection capability rather than enterprise scale.

3.3 Gaps and Future Enhancements

To progress toward a production-grade XDR platform, the following enhancements have been identified:

- **Telemetry Scaling & Data Engineering:**
  Implement Elasticsearch clustering, index lifecycle policies, and long-term log retention with hot–warm–cold architecture.

- **Advanced Correlation:**
  Develop cross-source correlation rules (e.g., linking suspicious logins to Suricata alerts or DLP violations) and implement risk scoring for entity prioritization.

- **Identity & Context Integration:**
  Enrich UEBA models with IdP data, cloud access logs, and user directory attributes to improve insider risk context and detection fidelity.

- **Automated Source Onboarding:**
  Create standardized ingestion templates and pipelines to streamline integration of new log sources.

- **Expanded Use Cases:**
  Extend UEBA modeling beyond SSH to include web access, email, SaaS usage, and privileged actions.

- **Operational Hardening:**
  Introduce RBAC, MFA, secured APIs, encrypted log transport, and regular security patching workflows.

3.4 Assumptions

The prototype assumes the following conditions for proper operation:

- All log sources are reachable and correctly configured for forwarding to ELK.

- The Elasticsearch and Kibana components are available and have sufficient resources for indexing and visualization.
- Network connectivity between data sources, SIEM components, and UEBA engine remains stable.
- GeoIP and reputation enrichment services (e.g., VirusTotal) are reachable for enrichment tasks.
- Analysts and stakeholders have browser access to the Kibana and Streamlit dashboards for triage and reporting.

This scope clearly defines the **functional boundaries** of the current XDR / Insider Risk implementation, acknowledges deliberate constraints, and outlines the **evolution path toward enterprise readiness**.

4. Tools & Solution Overview

The XDR / Insider Risk solution leverages a combination of **open-source SIEM technologies**, **machine learning analytics**, and **security automation** to provide centralized visibility, advanced detection, and efficient response. The toolchain integrates multiple layers of telemetry (identity, data, application, network, and behavioral) into a unified operational framework.

The table below summarizes the key components and their respective roles:

Component	Purpose	Key Functions
ELK Stack (Elasticsearch, Logstash, Kibana)	Centralized SIEM	Log ingestion, indexing, search, dashboards, and rule-based detections
Elastic Agents	Telemetry collection	Deployed on IAM, Kubernetes, DSPM, and test machines to forward logs
Suricata IDS	Network intrusion detection	Signature-based detection of exploits, scans, and suspicious traffic
Pomerium	ZTNA telemetry source	Authentication logs, failed/suspicious login events

DSPM Components (Presidio, Custodian)	Data security telemetry	DLP alerts, remediation logs, anomalous email activity
CNAPP Components (Chekhov, Kyverno)	Infrastructure and container posture	IaC misconfiguration detection, Kubernetes policy violations
CDP Components (Churn Model)	Monitoring alerts and targeted campaigns	Monitoring pipeline stages, campaigns, and outcomes.
pfSense	Perimeter telemetry	Firewall and routing logs for network context
UEBA Engine (Isolation Forest)	Behavioral anomaly detection	Per-user SSH anomaly detection, feature extraction, scoring
Streamlit Dashboards	Analyst and stakeholder visualization	Interactive behavioral anomaly investigation and KPIs
Tines Automation	Response orchestration	Enrichment, email alerts, host isolation playbooks
VirusTotal	Threat intelligence	IP and file reputation enrichment for detection and UEBA alerts

ELK Stack (SIEM Core)

The ELK Stack serves as the **centralized log aggregation and analytics platform**.

- **Elasticsearch** indexes telemetry from diverse sources, supporting fast searches and scalable data storage.
- **Logstash** or built-in Elastic Agent pipelines parse and forward structured JSON logs from ZTNA, DSPM, CNAPP, network IDS, and Kubernetes sources.
- **Kibana** provides interactive dashboards and visualizations for SOC analysts, including real-time authentication monitoring, IaC posture metrics, DLP alerts, and IDS event trends.
- Detection rules are implemented in Kibana to generate alerts for key scenarios such as failed logins, sensitive data detections, and network threats.

Telemetry Sources

Multiple log sources feed into ELK for comprehensive visibility:

- **ZTNA Layer:**
    - Pomerium authentication logs capturing successful/failed sign-ins and suspicious access requests.
    - pfSense firewall logs providing perimeter traffic context.
- **CDP Layer:**
    - Churn model Monitoring pipeline stages, campaigns, and outcomes.
- **DSPM Layer:**
    - Presidio DLP alerts flagging sensitive data exposure.
    - Custodian remediation logs showing policy-driven enforcement.
- **CNAPP Layer:**
    - Chekhov IaC scan outputs for misconfiguration findings.
    - Kyverno logs from Kubernetes clusters for policy violations and pod anomalies.
- **Network Layer:**
    - Suricata IDS alerts for port scans, exploit attempts, and suspicious flows.

This layered telemetry model ensures coverage across **identity, data, infrastructure, and network planes**.

UEBA Engine

A **User & Entity Behavior Analytics (UEBA)** engine was developed to detect insider threats through SSH login anomalies:

- **Data Source:** logs-system.auth-* index in Elasticsearch, with timezone alignment to Asia/Kolkata.
- **Feature Engineering:** Time-of-day, weekday patterns, geo-IP rarity, ASN deviations, login method changes, host novelty.
- **Model:** Per-user Isolation Forests with fallback global model for sparse data.

- **Scoring:** 0–1 anomaly score mapped to severity levels (Low–Critical).
- **Explainability:** Top contributing behavioral features are identified for each anomaly.

This engine identifies deviations from established baselines, flagging potentially malicious insider activity or compromised accounts.

Visualization Dashboards

- **Kibana Dashboards:**
  Focused on detection-oriented KPIs such as failed login trends, IaC misconfiguration density, DLP violations over time, Suricata alert frequency, and Kubernetes anomaly heatmaps.
- **Streamlit Dashboards (UEBA):**
  - **SOC Analyst View:** Real-time anomaly KPIs, temporal heatmaps, geo-IP visualizations, drill-down on enriched login events.
  - **Stakeholder View:** Aggregated trends, user anomaly scores, severity distributions, and exportable reports.
  - Dashboards are optimized for fast load times (<2 s, 95th percentile) and high field availability (≥90%).

Automation & Enrichment

Tines is integrated as the automation layer to orchestrate response workflows:

- **VirusTotal Enrichment:** Automated IP reputation checks for suspicious SSH login anomalies.
- **Email Notifications:** Professional HTML alerts containing incident ID, user/host/IP info, severity, threat intelligence data, and analyst recommendations.
- **Host Isolation:** Triggered automatically for critical severity alerts to reduce dwell time.

Threat intelligence lookups from **VirusTotal** are embedded in both detection rules and UEBA anomaly enrichment, enhancing analyst context and response quality.

Integration & Interplay

- **SIEM ↔ UEBA:**
  Behavioral anomalies detected in UEBA complement rule-based SIEM detections, providing depth against both known and unknown threats.
- **SIEM ↔ Automation:**
  Alerts generated by ELK rules feed Tines for enrichment and response.
- **UEBA ↔ Dashboards:**
  Analysts can investigate anomalies interactively through Streamlit while correlating them with SIEM data in Kibana.

This integration ensures that the system functions as a **cohesive XDR platform**, not as isolated security tools.

This toolchain delivers **broad telemetry coverage, advanced detection, and automated response** all using modular, open-source technologies. It establishes a robust foundation for scalable XDR operations and insider risk detection.

5. Configurations & Customizations

The XDR / Insider Risk solution required targeted configurations across the **SIEM platform**, **telemetry sources**, **UEBA engine**, and **automation workflows** to ensure secure, reliable data ingestion, meaningful detections, and operational stability. This section outlines the key changes made compared to default tool configurations and explains their purpose.

5.1 ELK Stack (SIEM Core)

Elasticsearch

- **Index Templates & Mappings:**
  Custom index templates were created to ensure consistent field mappings for telemetry sources such as Pomerium, Suricata, and Presidio, enabling accurate parsing and field-based detection logic.
- **Hot–Warm Index Lifecycle Policy (ILM):**
  Implemented a short-term ILM policy for the lab environment to optimize storage use while maintaining search performance.

- **Authentication & Access:**
  Basic authentication was enabled for Kibana and Elasticsearch; analyst accounts were created for dashboard access and detection rule management.

Elastic Agent Pipelines

- **Log Parsing:**
  Pipelines were configured to parse structured JSON logs from multiple telemetry sources. For example:
  - Pomerium and Keycloak logs were parsed to extract email, route, event_type, and outcome.
  - Suricata alerts were normalized to ECS format for easy correlation.
  - Presidio and Custodian logs were mapped to standardized fields for DLP alerting.
- **Routing by Index:**
  Conditional filters routed logs into dedicated indices (e.g., logs-ztna-*, logs-dspm-*, logs-cnapp-*, logs-suricata-*), improving query performance and detection clarity.

Kibana

- **Dashboards & Visualizations:**
  Custom detection-focused dashboards were built for each log type, highlighting KPIs such as:
  - Failed vs. successful logins (ZTNA)
  - Sensitive data alerts over time (DSPM)
  - IDS alert categories and frequencies (Network)
  - IaC misconfiguration trends (CNAPP)
  - Kubernetes policy violations and pod anomalies
- **Detection Rules:**
  Kibana detection rules were created for:
  - Pomerium: failed logins, suspicious access patterns.

    - Presidio: DLP alerts on sensitive data exposure.
    - Churn: anomalous email activity detections.
    - Suricata: exploit attempts and port scans.
    - Chekhov: IaC misconfiguration alerts.
    - Kyverno: resource policy violations.

5.2 Telemetry Source Configuration

Pomerium (ZTNA)

- **JSON Logging:** Enabled and redirected to /var/log/pomerium/pomerium.json for ingestion.
- **Field Enrichment:** Configured forwarding of user identity headers and timestamps to improve log context.

Suricata IDS

- **EVE JSON Mode:** Enabled EVE JSON output to /var/log/suricata/eve.json.
- **Rule Sets:** Updated rule sets to detect port scans, exploit attempts, and suspicious DNS patterns.
- **Integration:** Suricata logs were shipped via Elastic Agent to the logs-suricata-* index.

DSPM (Presidio, Custodian)

- **Alert Output:** Configured Presidio to emit structured DLP alerts for ingestion.
- **Custodian:** Remediation logs standardized to include resource_id, policy, and action fields.

CDP (Churn model)

- JSON-based logs ingested into ELK, enabling real-time dashboards for monitoring pipeline stages, campaigns, and outcomes.

CNAPP (Chekhov, Kyverno)

- **Chekhov:** IaC scan outputs were exported to JSON and forwarded to ELK using a lightweight agent.
- **Kyverno:** Audit and policy violation logs were collected from Kubernetes nodes and parsed to extract violation details and pod metadata.

pfSense

- **Syslog Forwarding:** pfSense firewall logs were forwarded over UDP to Elastic Agent for ingestion, providing ZTNA perimeter visibility.

5.3 UEBA Engine Configuration

The UEBA subsystem was configured for SSH anomaly detection using Isolation Forest models.

- **Data Source:**
  Configured to pull login data from the logs-system.auth-* Elasticsearch index with timezone normalization (Asia/Kolkata).
- **Feature Engineering:**
  Implemented the following feature extractions per user:
  - **Time-based:** login hour, weekday, off-hour flags.
  - **Geo/IP:** IP rarity, geo distance from last login, ASN changes.
  - **Auth behavior:** failure ratios, failure→success chains, method changes.
  - **Host behavior:** new host frequency.
- **Model Parameters:**
  - Isolation Forest per user with contamination factor tuned for low false positives.
  - Fallback global model for sparse users.
- **Explainability:**
  Configured generation of top feature contributions per anomaly to support analyst decision-making.

- **Alerts & Notifications:**
  High/Critical anomalies trigger SMTP-based HTML email alerts with context enrichment (VT reputation data, analyst recommendations).

5.4 Tines Automation Workflows

Enrichment

- **VirusTotal Integration:**
  Automatically enriches IPs found in UEBA anomalies with reputation data and embeds it in alert payloads.

Alerting

- **Email Notifications:**
  Configured professional HTML templates with incident metadata, severity color-coding, and recommended analyst actions.
  - Max 1 alert per user per hour to prevent alert fatigue.
  - Manual “Send Now” button available for testing.

Containment

- **Host Isolation Playbooks:**
  Automatically isolate endpoints or trigger escalation workflows on critical severity events detected by SIEM or UEBA.

5.5 Security & Quality Controls

- **Secrets Management:**
  Credentials for enrichment services and SMTP are stored as environment variables, not hard-coded in configs.
- **Alert Rate Limiting:**
  UEBA and SIEM alerts include strict thresholds and rate-limits to avoid noise.
- **Performance Gates:**
  Streamlit dashboards benchmarked for load time (<2 s, 95th percentile), and minimum field availability (≥90%) enforced to maintain analysis quality.

- **Logging Hygiene:**
  Logrotate configured for all major log directories to prevent uncontrolled file growth.

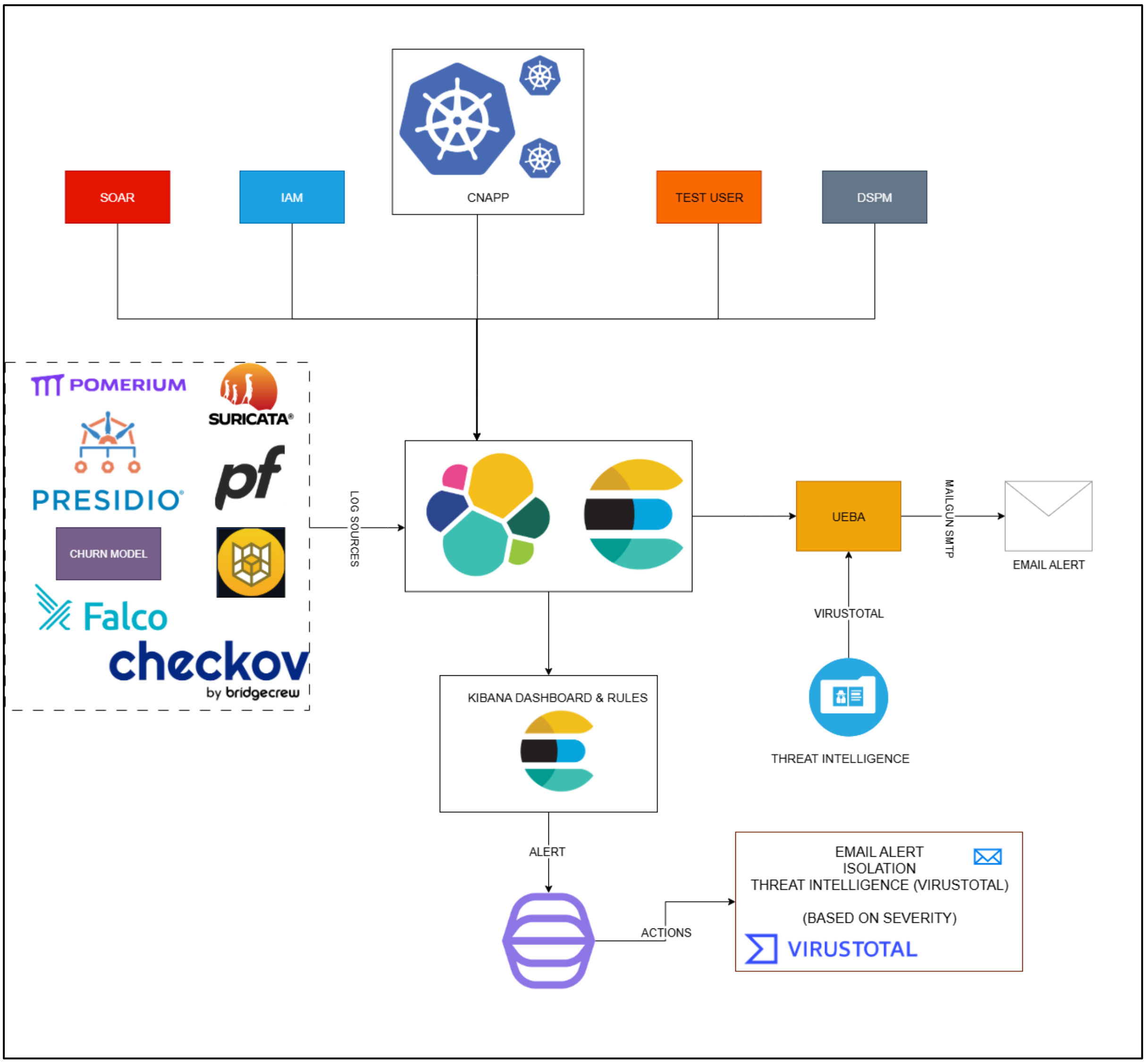
These targeted configurations and customizations ensured that the **XDR pipeline remained reliable, detection-ready, and secure**. They allowed heterogeneous telemetry sources to be normalized, enriched, visualized, and acted upon in a cohesive manner, enabling both **rule-based detections** and **behavioral analytics** to operate effectively.

6. Architecture & Data Flow Diagram

High-Level Architecture

The XDR / Insider Risk system integrates **multi-layered telemetry sources**, **centralized SIEM processing**, **behavioral analytics**, and **automation workflows** into a cohesive operational pipeline. This architecture enables real-time threat detection, enriched contextual analysis, and automated response to both known and unknown security events.

Logical Data Flow Diagram



Telemetry Sources and Ingestion

Multiple telemetry streams feed into the XDR platform:

- **ZTNA Layer**
  - Pomerium authentication logs capture sign-in attempts and access patterns.
  - pfSense firewall logs provide perimeter traffic visibility.
- **DSPM Layer**
  - Presidio emits DLP alerts for sensitive data detections.
  - Custodian logs show policy enforcement actions.

- **CNAPP Layer**
  - Chekhov produces IaC misconfiguration findings.
  - Kyverno logs policy violations and pod-level anomalies from Kubernetes.
- **Network Layer**
  - Suricata generates IDS alerts for suspicious network behavior.
- **Endpoint & Auth Layer**
  - System auth logs are indexed for UEBA behavioral modeling.

Telemetry is forwarded via **Elastic Agents** or syslog to Elasticsearch for parsing, normalization (ECS), and indexing.

SIEM Processing (ELK Stack)

The Elastic Stack performs the following functions:

- **Ingestion & Parsing**
  Ingest pipelines normalize structured JSON telemetry into consistent Elasticsearch indices.
- **Indexing & Storage**
  Logs are stored in index patterns segmented by telemetry type (logs-ztna-*, logs-dspm-*, etc.) for efficient search and correlation.
- **Detection Engineering**
  Kibana rules detect key scenarios such as failed logins, DLP alerts, IaC misconfigurations, Suricata IDS alerts, and suspicious Kubernetes events.
- **Dashboards & Visualization**
  Real-time dashboards provide SOC analysts with KPIs, trends, and alert summaries for each telemetry category.

UEBA Engine Data Flow

The **UEBA subsystem** operates alongside the SIEM to analyze SSH login behavior for insider risk detection:

1. **Data Pull** — Authentication logs (logs-system.auth-*) are retrieved from Elasticsearch.
2. **Feature Engineering** — Behavioral features such as login time patterns, geo-IP rarity, ASN changes, failure ratios, and host novelty are computed per user.
3. **Modeling & Scoring** — Isolation Forest models score anomalies per user. Sparse users fallback to a global model.
4. **Explainability & Alerting** — Top contributing features are extracted, and high/critical anomalies trigger enriched alerts.
5. **Visualization** — Analysts use Streamlit dashboards for real-time anomaly monitoring, drill-downs, and contextual analysis.

Automation Layer (Tines)

Tines workflows enhance detection and response:

- **Enrichment**
  - VirusTotal lookups for IP reputation and threat intelligence.
  - Enrichment data appended to SIEM and UEBA alerts.
- **Alerting**
  - Professional HTML email alerts for high-severity incidents with contextual metadata (incident ID, user, IP, severity, reputation, recommendations).
- **Response**
  - Automated host isolation or escalation triggered by critical alerts from SIEM or UEBA.

This automation layer reduces manual investigation time and improves response consistency.

Analyst Interaction

- **SOC Analysts**
  Use Kibana dashboards to monitor detections, investigate alerts, and correlate activity across telemetry layers. Tines enrichments and alerts accelerate triage.

- **Threat Hunters / Detection Engineers**
  Use Elasticsearch queries and UEBA anomaly outputs to identify emerging threats or insider behaviors not covered by static rules.
- **Stakeholders**
  Access Streamlit dashboards for summarized anomaly trends and risk posture insights.

Trust & Integration Boundaries

- **Data Ingestion Boundary:** Telemetry is normalized and authenticated at the ingestion layer before indexing.
- **Analytics Boundary:** SIEM and UEBA components share data but operate independently, ensuring layered detection.
- **Response Boundary:** Tines has controlled access to enrichment APIs and response endpoints, with credentials stored securely via environment variables.

End-to-End Flow Summary

1. **Telemetry** is collected from ZTNA, DSPM, CDP, CNAPP, network, and auth sources.
2. **Elastic Stack** ingests, parses, indexes, and applies detection rules.
3. **UEBA Engine** runs behavioral models on SSH login data, scoring anomalies and enriching them.
4. **Dashboards** in Kibana and Streamlit provide real-time visualization and investigation capabilities.
5. **Tines** workflows enrich alerts and initiate automated responses for critical incidents.
6. **SOC analysts** act on enriched, correlated detections efficiently.

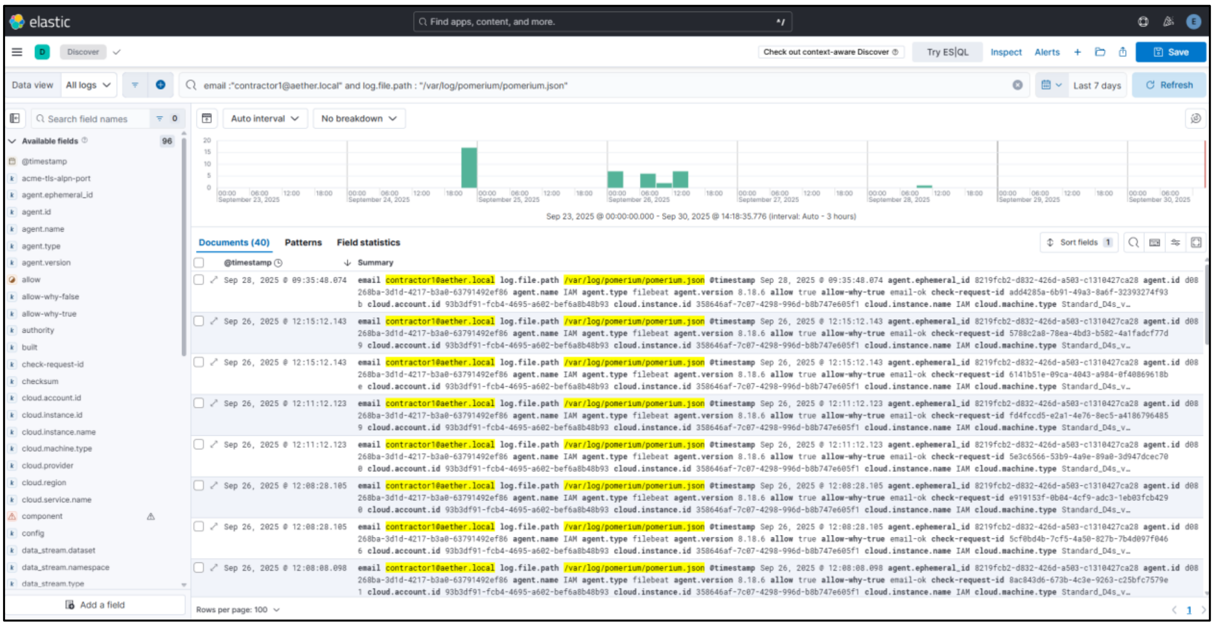
7. Evidence & PoC

The implementation of the XDR / Insider Risk solution was validated through **end-to-end functional testing, log verification, detection rule triggering, and dashboard visualization**. This section provides evidence supporting the successful deployment and operation of each major component of the system.

7.1 Telemetry Ingestion Validation

To confirm that all targeted telemetry sources were successfully onboarded into the ELK Stack:

- **Pomerium Authentication Logs (ZTNA)**
  - JSON logs captured and parsed correctly with user identity fields (email, route, event_type) visible in Kibana.
  - Successful ingestion was confirmed through sample login events from contractor1@aether.local and corresponding Kibana searches.

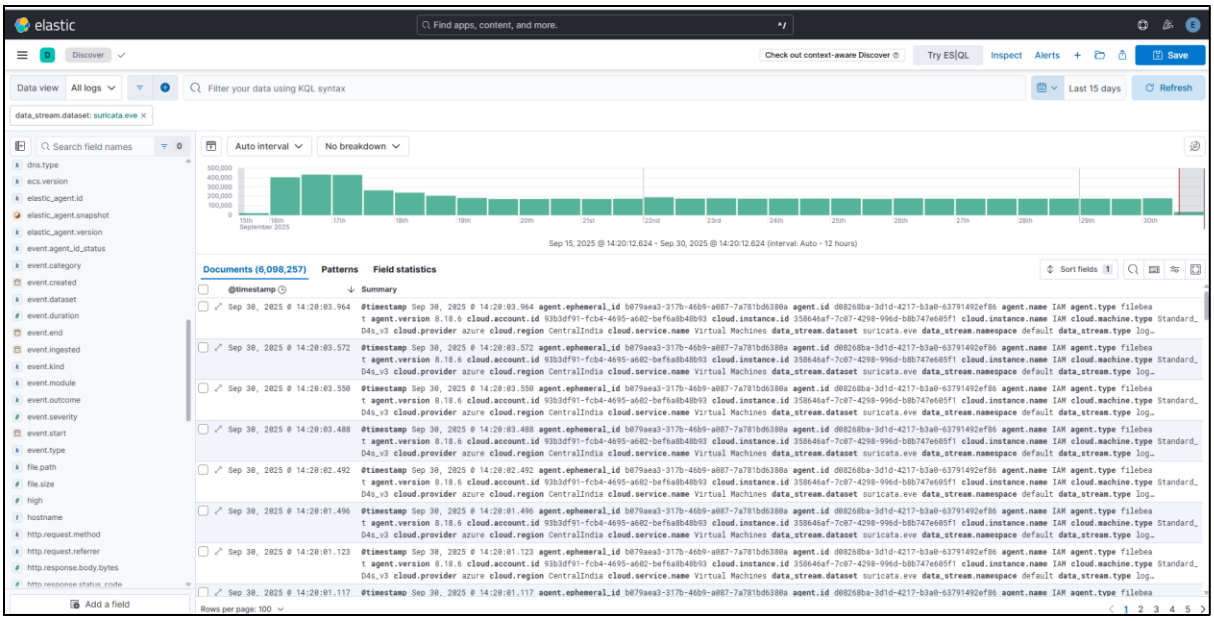


email :"contractor1@aether.local" and log.file.path : "/var/log/pomerium/pomerium.json"

Sep 23, 2025 @ 00:00:00.000 - Sep 30, 2025 @ 14:18:35.776 (interval: Auto - 3 hours)

```
Sep 28, 2025 @ 09:35:48.074  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 28, 2025 @ 09:35:48.074 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id add4285a-6b91-49a3-8a6f-32393274f93
                             b cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
Sep 26, 2025 @ 12:15:12.143  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 26, 2025 @ 12:15:12.143 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id 5788c2a8-78ea-4bd3-b582-4a1fadcf77d
                             9 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
Sep 26, 2025 @ 12:15:12.143  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 26, 2025 @ 12:15:12.143 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id 6141b51e-09ca-4043-a984-0f40869618b
                             e cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
Sep 26, 2025 @ 12:11:12.123  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 26, 2025 @ 12:11:12.123 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id fd4fccd5-e2a1-4e76-8ec5-a4186796485
                             9 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
Sep 26, 2025 @ 12:11:12.123  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 26, 2025 @ 12:11:12.123 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id 5e3c6566-53b9-4a9e-89a0-3d947dcec70
                             0 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
Sep 26, 2025 @ 12:08:28.105  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 26, 2025 @ 12:08:28.105 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id e919153f-0b04-4cf9-adc3-1eb03fcb429
                             0 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
Sep 26, 2025 @ 12:08:28.105  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 26, 2025 @ 12:08:28.105 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id 5cf0bd4b-7cf5-4a50-827b-7b4d097f046
                             6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
Sep 26, 2025 @ 12:08:08.098  email contractor1@aether.local log.file.path /var/log/pomerium/pomerium.json @timestamp Sep 26, 2025 @ 12:08:08.098 agent.ephemeral_id 8219fcb2-d832-426d-a503-c1310427ca28 agent.id d08
                             268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebeat agent.version 8.18.6 allow true allow-why-true email-ok check-request-id 8ac843d6-673b-4c3e-9263-c25bfc7579e
                             1 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_D4s_v…
```

- **Suricata IDS Alerts (Network)**
  - EVE JSON alerts indexed under logs-suricata-*.



```
Sep 30, 2025 @ 14:20:03.964  @timestamp Sep 30, 2025 @ 14:20:03.964 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
                             t agent.version 8.18.6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_
                             D4s_v3 cloud.provider azure cloud.region CentralIndia cloud.service.name Virtual Machines data_stream.dataset suricata.eve data_stream.namespace default data_stream.type log…
Sep 30, 2025 @ 14:20:03.572  @timestamp Sep 30, 2025 @ 14:20:03.572 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
                             t agent.version 8.18.6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_
                             D4s_v3 cloud.provider azure cloud.region CentralIndia cloud.service.name Virtual Machines data_stream.dataset suricata.eve data_stream.namespace default data_stream.type log…
Sep 30, 2025 @ 14:20:03.550  @timestamp Sep 30, 2025 @ 14:20:03.550 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
                             t agent.version 8.18.6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_
                             D4s_v3 cloud.provider azure cloud.region CentralIndia cloud.service.name Virtual Machines data_stream.dataset suricata.eve data_stream.namespace default data_stream.type log…
Sep 30, 2025 @ 14:20:03.488  @timestamp Sep 30, 2025 @ 14:20:03.488 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
                             t agent.version 8.18.6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_
                             D4s_v3 cloud.provider azure cloud.region CentralIndia cloud.service.name Virtual Machines data_stream.dataset suricata.eve data_stream.namespace default data_stream.type log…
Sep 30, 2025 @ 14:20:02.492  @timestamp Sep 30, 2025 @ 14:20:02.492 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
                             t agent.version 8.18.6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_
                             D4s_v3 cloud.provider azure cloud.region CentralIndia cloud.service.name Virtual Machines data_stream.dataset suricata.eve data_stream.namespace default data_stream.type log…
Sep 30, 2025 @ 14:20:01.496  @timestamp Sep 30, 2025 @ 14:20:01.496 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
                             t agent.version 8.18.6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_
                             D4s_v3 cloud.provider azure cloud.region CentralIndia cloud.service.name Virtual Machines data_stream.dataset suricata.eve data_stream.namespace default data_stream.type log…
Sep 30, 2025 @ 14:20:01.123  @timestamp Sep 30, 2025 @ 14:20:01.123 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
                             t agent.version 8.18.6 cloud.account.id 93b3df91-fcb4-4695-a602-bef6a8b48b93 cloud.instance.id 358646af-7c07-4298-996d-b8b747e605f1 cloud.instance.name IAM cloud.machine.type Standard_
                             D4s_v3 cloud.provider azure cloud.region CentralIndia cloud.service.name Virtual Machines data_stream.dataset suricata.eve data_stream.namespace default data_stream.type log…
Sep 30, 2025 @ 14:20:01.117  @timestamp Sep 30, 2025 @ 14:20:01.117 agent.ephemeral_id b079aea3-317b-46b9-a087-7a781bd6380a agent.id d08268ba-3d1d-4217-b3a0-63791492ef86 agent.name IAM agent.type filebea
```

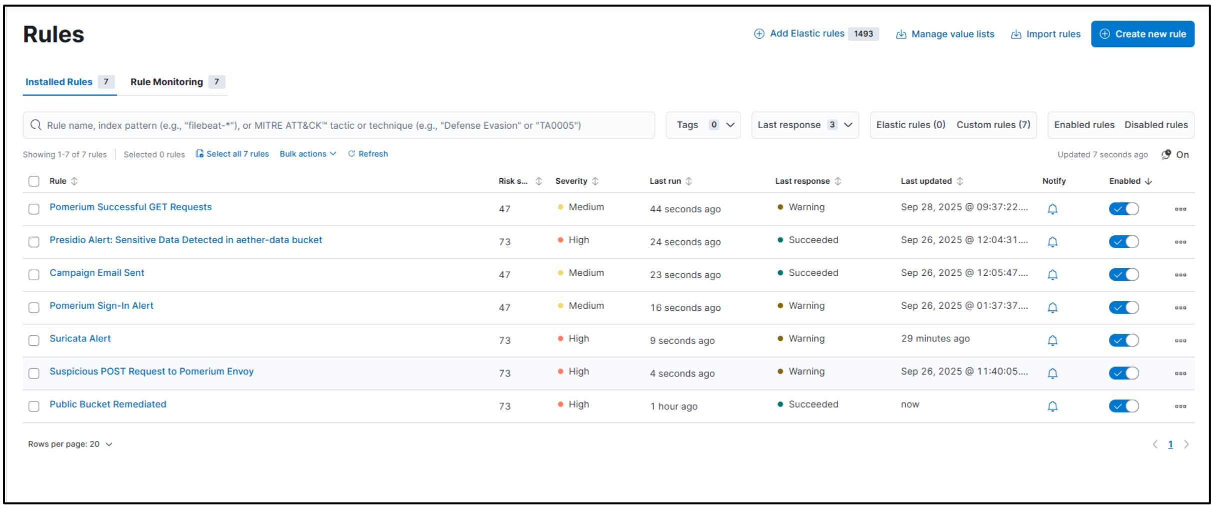
- **DSPM Logs (Presidio, Custodian)**
    - Presidio DLP alerts for sensitive data detection were ingested as structured JSON.
    - Custodian remediation actions appeared with correct policy and resource_id mappings.

- **CNAPP Logs (Chekhov, Kyverno)**
    - IaC misconfiguration findings from Chekhov scans were ingested via Elastic Agent.
    - Kyverno policy violations were collected from Kubernetes nodes, parsed for resource metadata and policy details.CDP Dashboard: Monitoring pipeline stages, campaigns, and outcomes.
- **CDP logs:**
    - Monitoring pipeline stages, campaigns, and outcomes.
- **pfSense Logs**
    - Syslog forwarding enabled successful indexing of firewall logs, allowing perimeter visibility in Kibana.

7.2 Detection Rule Triggering

A series of simulated security events were executed to validate the effectiveness of detection rules configured in Kibana.

Telemetry Source	Simulation Action	Expected Detection	Result
Pomerium	Multiple failed login attempts with invalid users	“Failed Login” rule triggered	Detected
Suricata	Nmap TCP SYN scan	IDS signature alert generated	Detected
Presidio	Upload file containing sensitive data pattern	DLP alert created	Detected
Chekhov	Introduce insecure IaC configuration (e.g., open SG)	Misconfiguration alert triggered	Detected
Kyverno	Deploy pod violating policy	Policy violation alert generated	Detected



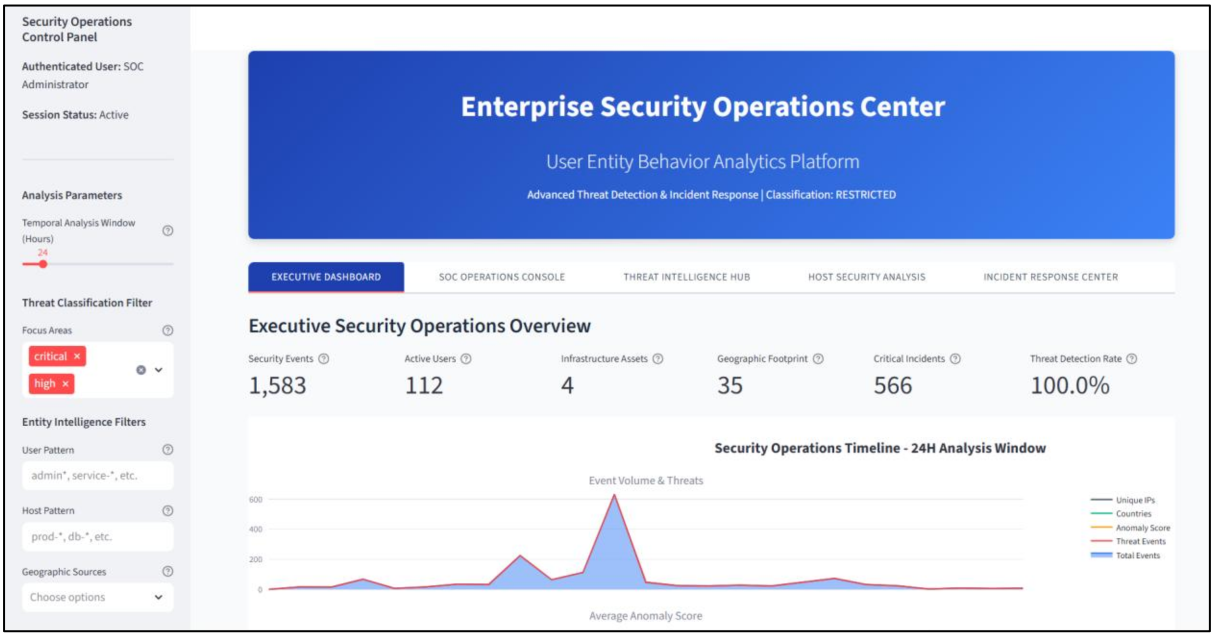
Rule	Risk s...	Severity	Last run	Last response	Last updated	Notify	Enabled
Pomerium Successful GET Requests	47	● Medium	44 seconds ago	● Warning	Sep 28, 2025 @ 09:37:22....		✓
Presidio Alert: Sensitive Data Detected in aether-data bucket	73	● High	24 seconds ago	● Succeeded	Sep 26, 2025 @ 12:04:31....		✓
Campaign Email Sent	47	● Medium	23 seconds ago	● Succeeded	Sep 26, 2025 @ 12:05:47....		✓
Pomerium Sign-In Alert	47	● Medium	16 seconds ago	● Warning	Sep 26, 2025 @ 01:37:37....		✓
Suricata Alert	73	● High	9 seconds ago	● Warning	29 minutes ago		✓
Suspicious POST Request to Pomerium Envoy	73	● High	4 seconds ago	● Warning	Sep 26, 2025 @ 11:40:05....		✓
Public Bucket Remediated	73	● High	1 hour ago	● Succeeded	now		✓

7.3 UEBA Subsystem Testing

The SSH anomaly detection subsystem was validated with both **baseline activity** and **simulated anomalous logins**:

- **Baseline Data Collection**

- Several normal login sessions were generated during standard work hours for multiple users.
- Features such as login time, weekday, IP, and ASN were profiled to establish behavioral baselines.



Security Operations Control Panel

Authenticated User: SOC Administrator

Session Status: Active

Analysis Parameters

Temporal Analysis Window (Hours): 24

Threat Classification Filter

Focus Areas: critical, high

Entity Intelligence Filters

User Pattern: admin*, service-*, etc.

Host Pattern: prod-*, db-*, etc.

Geographic Sources: Choose options

Enterprise Security Operations Center

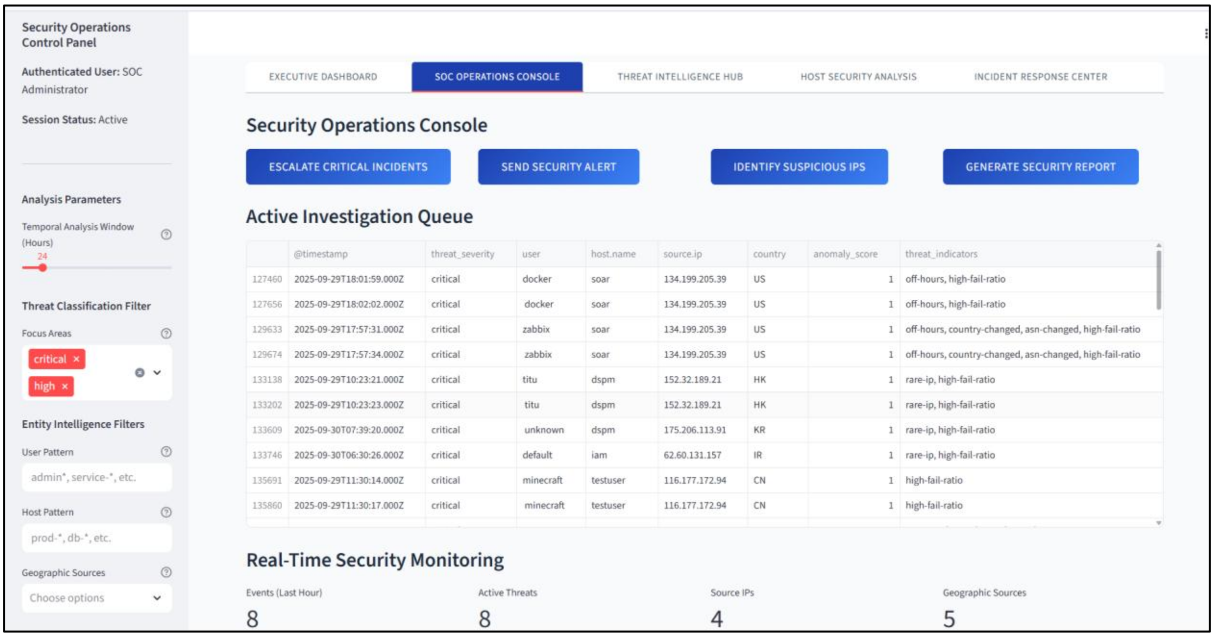
User Entity Behavior Analytics Platform

Advanced Threat Detection & Incident Response | Classification: RESTRICTED

Executive Security Operations Overview

Security Events	Active Users	Infrastructure Assets	Geographic Footprint	Critical Incidents	Threat Detection Rate
1,583	112	4	35	566	100.0%

- **Anomaly Injection**
  - Simulated anomalous SSH logins were generated using:
    - Off-hour logins from new IPs
    - Rare country geolocations
    - ASN changes and method variation
  - Isolation Forest scored these anomalies between 0.78–0.94, classifying them as High or Critical severity.



Security Operations Control Panel

Authenticated User: SOC Administrator

Session Status: Active

Analysis Parameters

Temporal Analysis Window (Hours): 24

Threat Classification Filter

Focus Areas: critical, high

Entity Intelligence Filters

User Pattern: admin*, service-*, etc.

Host Pattern: prod-*, db-*, etc.

Geographic Sources: Choose options

Security Operations Console

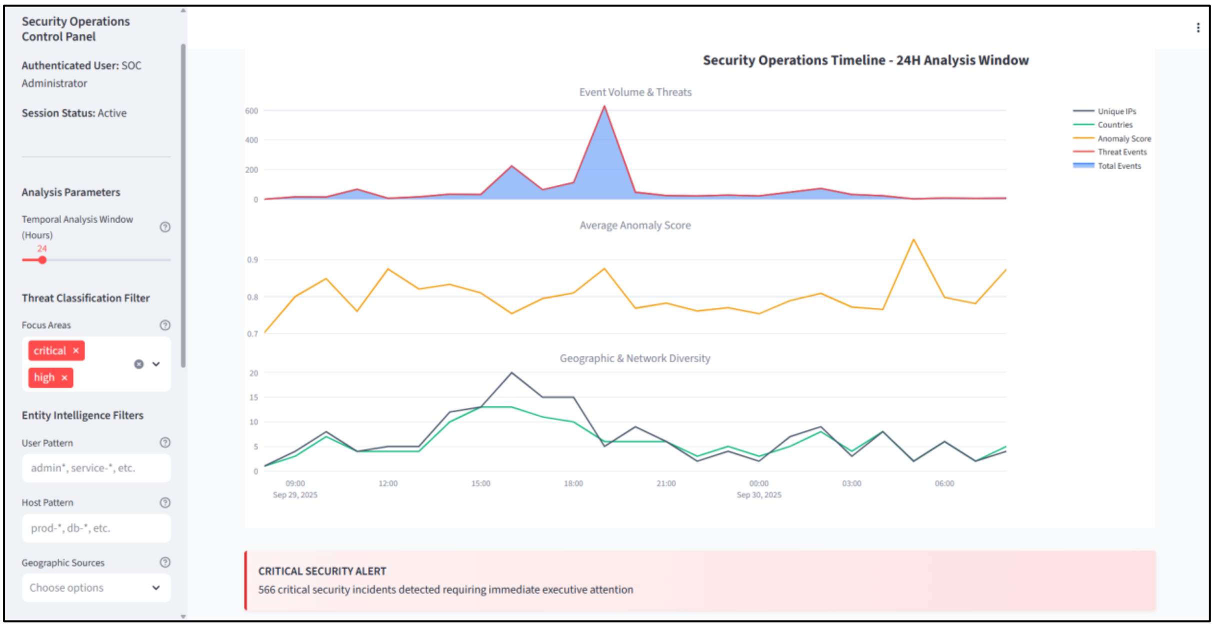
Active Investigation Queue

	@timestamp	threat_severity	user	host.name	source.ip	country	anomaly_score	threat_indicators
127460	2025-09-29T18:01:59.000Z	critical	docker	soar	134.199.205.39	US	1	off-hours, high-fail-ratio
127656	2025-09-29T18:02:02.000Z	critical	docker	soar	134.199.205.39	US	1	off-hours, high-fail-ratio
129633	2025-09-29T17:57:31.000Z	critical	zabbix	soar	134.199.205.39	US	1	off-hours, country-changed, asn-changed, high-fail-ratio
129674	2025-09-29T17:57:34.000Z	critical	zabbix	soar	134.199.205.39	US	1	off-hours, country-changed, asn-changed, high-fail-ratio
133138	2025-09-29T10:23:21.000Z	critical	titu	dspm	152.32.189.21	HK	1	rare-ip, high-fail-ratio
133202	2025-09-29T10:23:23.000Z	critical	titu	dspm	152.32.189.21	HK	1	rare-ip, high-fail-ratio
133609	2025-09-30T07:39:20.000Z	critical	unknown	dspm	175.206.113.91	KR	1	rare-ip, high-fail-ratio
133746	2025-09-30T06:30:26.000Z	critical	default	iam	62.60.131.157	IR	1	rare-ip, high-fail-ratio
135691	2025-09-29T11:30:14.000Z	critical	minecraft	testuser	116.177.172.94	CN	1	high-fail-ratio
135860	2025-09-29T11:30:17.000Z	critical	minecraft	testuser	116.177.172.94	CN	1	high-fail-ratio

Real-Time Security Monitoring

Events (Last Hour)	Active Threats	Source IPs	Geographic Sources
8	8	4	5

- **Explainability Validation**
  - For each anomaly, the top contributing behavioral factors were correctly extracted (e.g., “Unusual login hour”, “New IP ASN”, “Rare country”).
  - This data was displayed in the Streamlit analyst dashboard for investigation.



Security Operations Control Panel

Authenticated User: SOC Administrator

Session Status: Active

Analysis Parameters

Temporal Analysis Window (Hours): 24

Threat Classification Filter

Focus Areas: critical, high

Entity Intelligence Filters

User Pattern: admin*, service-*, etc.

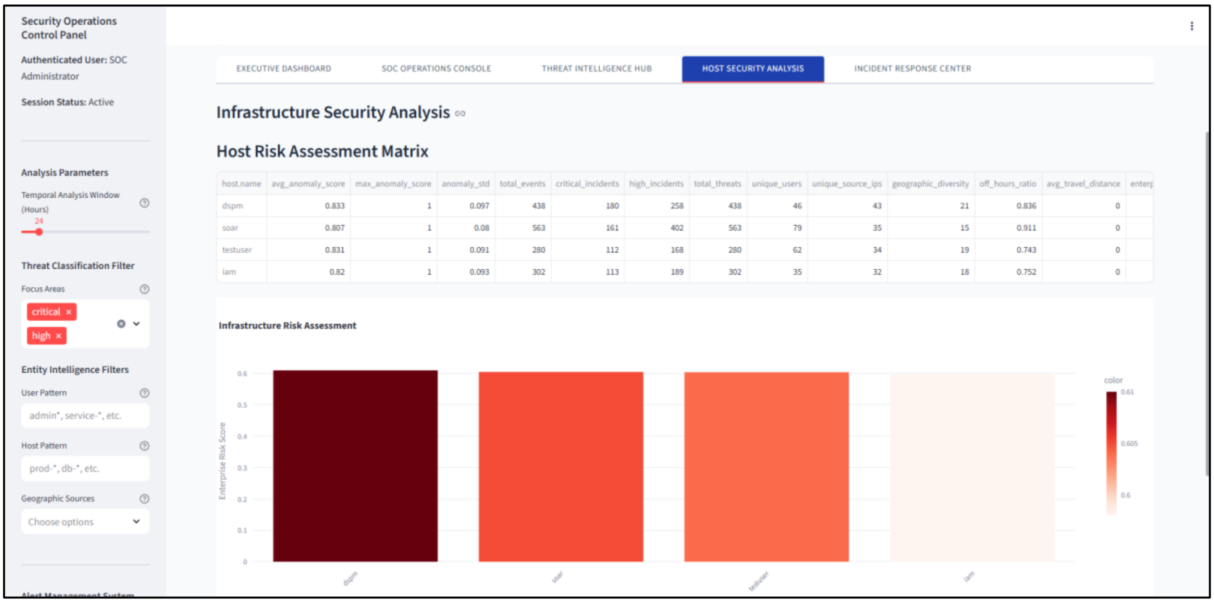
Host Pattern: prod-*, db-*, etc.

Geographic Sources: Choose options

CRITICAL SECURITY ALERT

566 critical security incidents detected requiring immediate executive attention

- Streamlit dashboard screenshots showing anomaly severity distributions and user drill-down views.



Security Operations Control Panel

Authenticated User: SOC Administrator

Session Status: Active

Analysis Parameters

Temporal Analysis Window (Hours): 24

Threat Classification Filter

Focus Areas: critical, high

Entity Intelligence Filters

User Pattern: admin*, service-*, etc.

Host Pattern: prod-*, db-*, etc.

Geographic Sources: Choose options

Infrastructure Security Analysis

Host Risk Assessment Matrix

host.name	avg_anomaly_score	max_anomaly_score	anomaly_std	total_events	critical_incidents	high_incidents	total_threats	unique_users	unique_source_ips	geographic_diversity	off_hours_ratio	avg_travel_distance	enterp
dspm	0.833	1	0.097	438	180	258	438	46	43	21	0.836	0	
soar	0.807	1	0.08	563	161	402	563	79	35	15	0.911	0	
testuser	0.831	1	0.091	280	112	168	280	62	34	19	0.743	0	
iam	0.82	1	0.093	302	113	189	302	35	32	18	0.752	0	

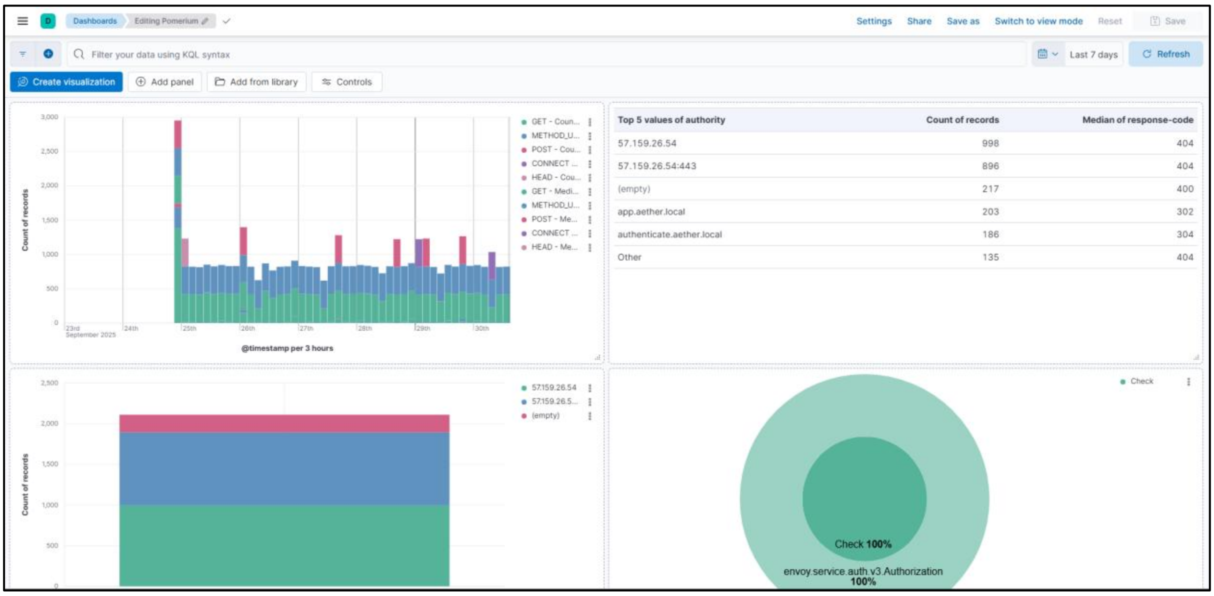
Infrastructure Risk Assessment

- Email alert samples received for critical anomalies with full context (incident ID, IP reputation, analyst recommendations).

7.4 Dashboard Functionality Verification

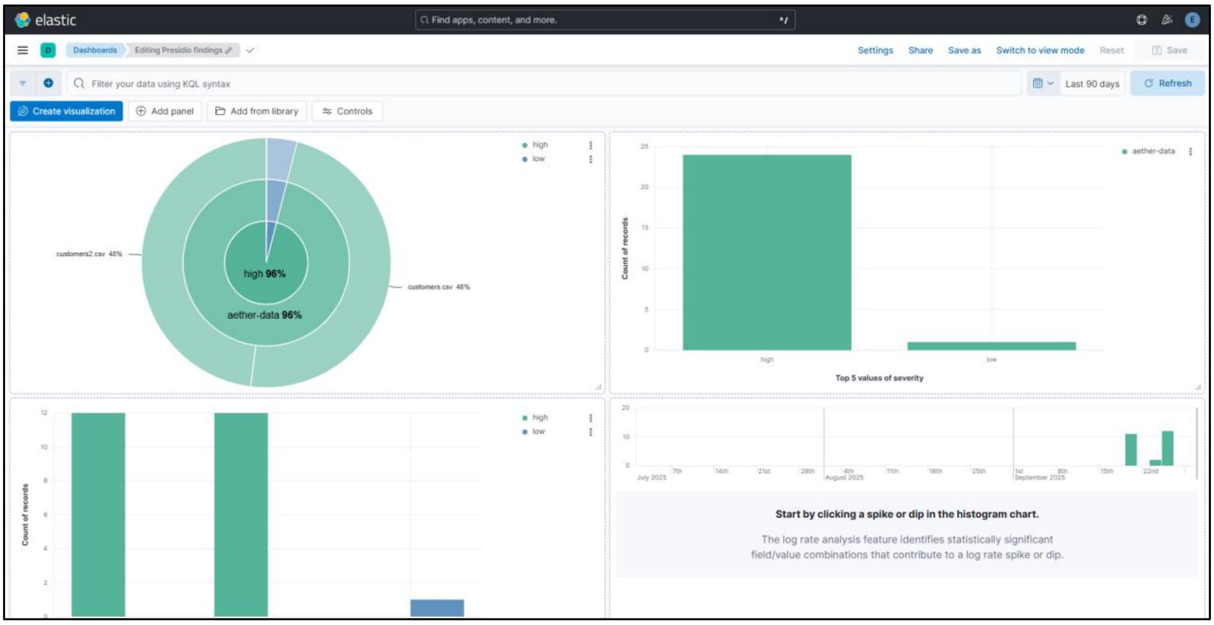
Two categories of dashboards were validated:

- **Kibana Dashboards**
  - ZTNA Authentication Dashboard: Displayed failed/successful login trends and suspicious access requests.



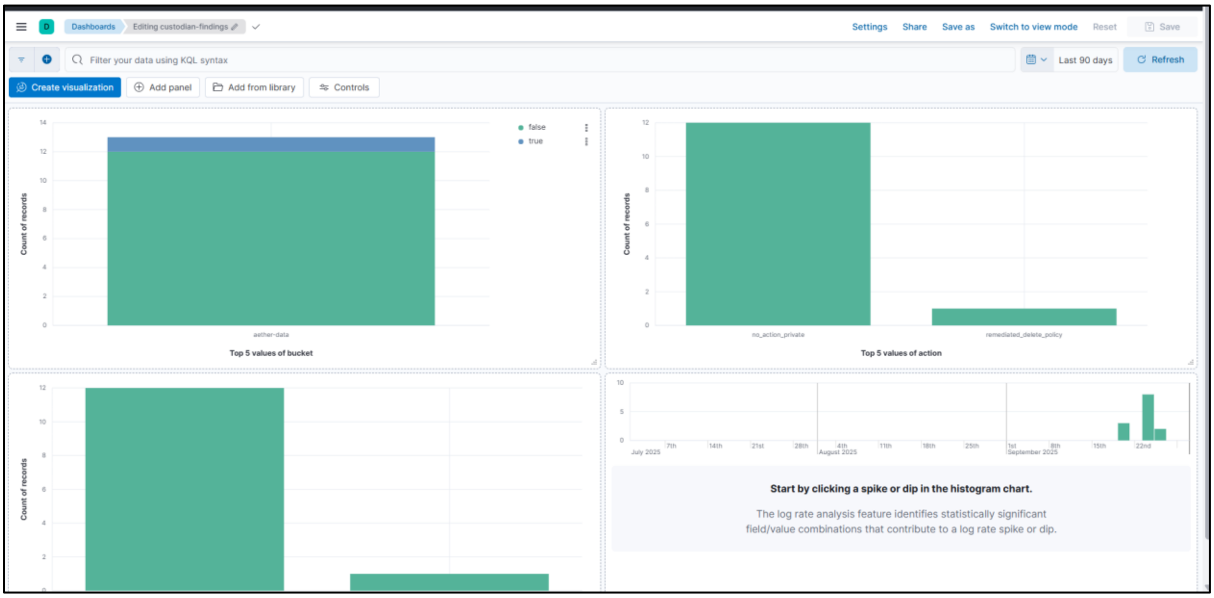
Top 5 values of authority	Count of records	Median of response-code
57.159.26.54	998	404
57.159.26.54:443	896	404
(empty)	217	400
app.aether.local	203	302
authenticate.aether.local	186	304
Other	135	404

  - DSPM Dashboard: Visualized DLP alerts and Custodian remediation actions.



Start by clicking a spike or dip in the histogram chart.

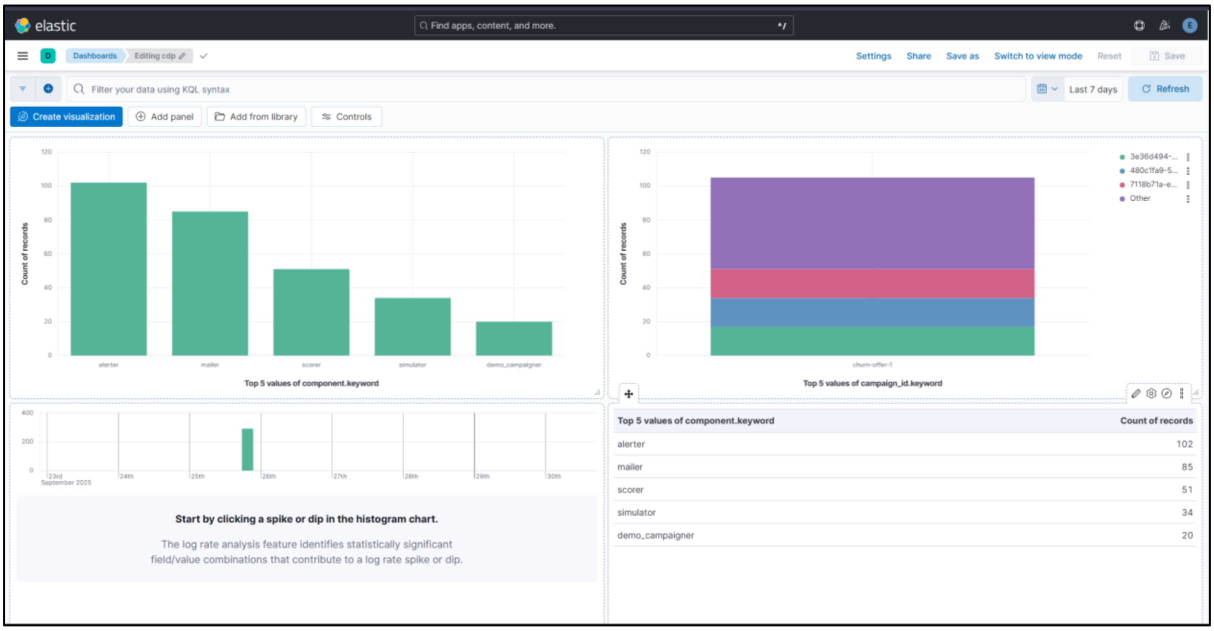
The log rate analysis feature identifies statistically significant field/value combinations that contribute to a log rate spike or dip.



Start by clicking a spike or dip in the histogram chart.

The log rate analysis feature identifies statistically significant field/value combinations that contribute to a log rate spike or dip.

- CDP Dashboard: Monitoring pipeline stages, campaigns, and outcomes.

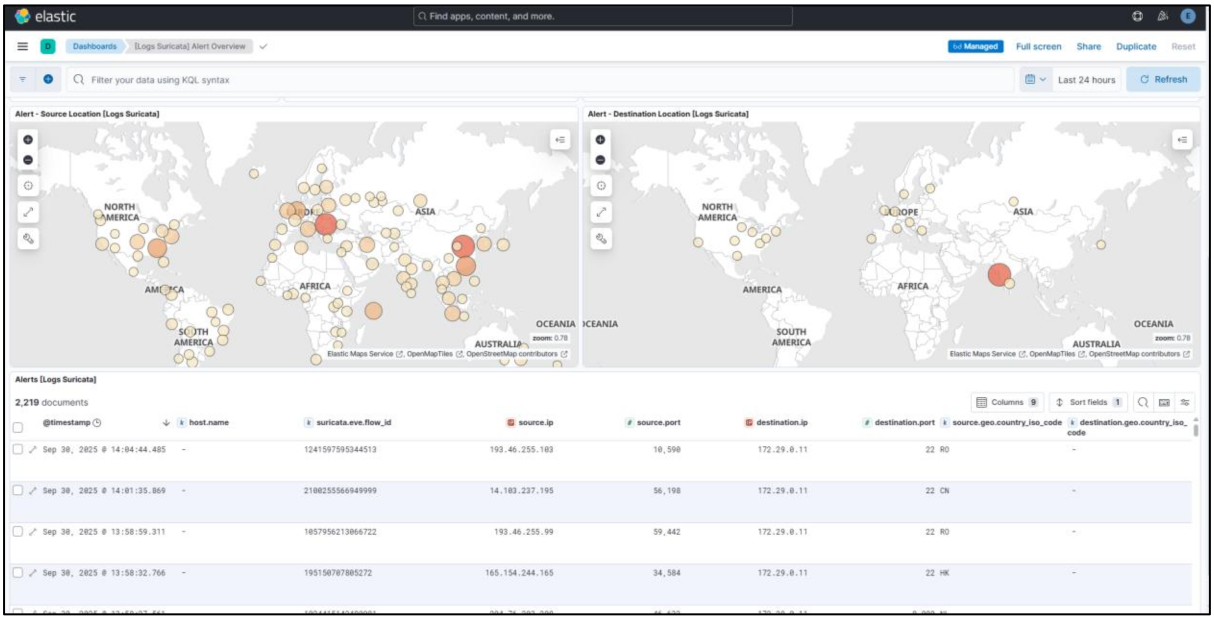


Start by clicking a spike or dip in the histogram chart.

The log rate analysis feature identifies statistically significant field/value combinations that contribute to a log rate spike or dip.

Top 5 values of component.keyword	Count of records
alerter	102
mailer	85
scorer	51
simulator	34
demo_campaigner	20

- Network Dashboard: IDS alert categories and frequency.

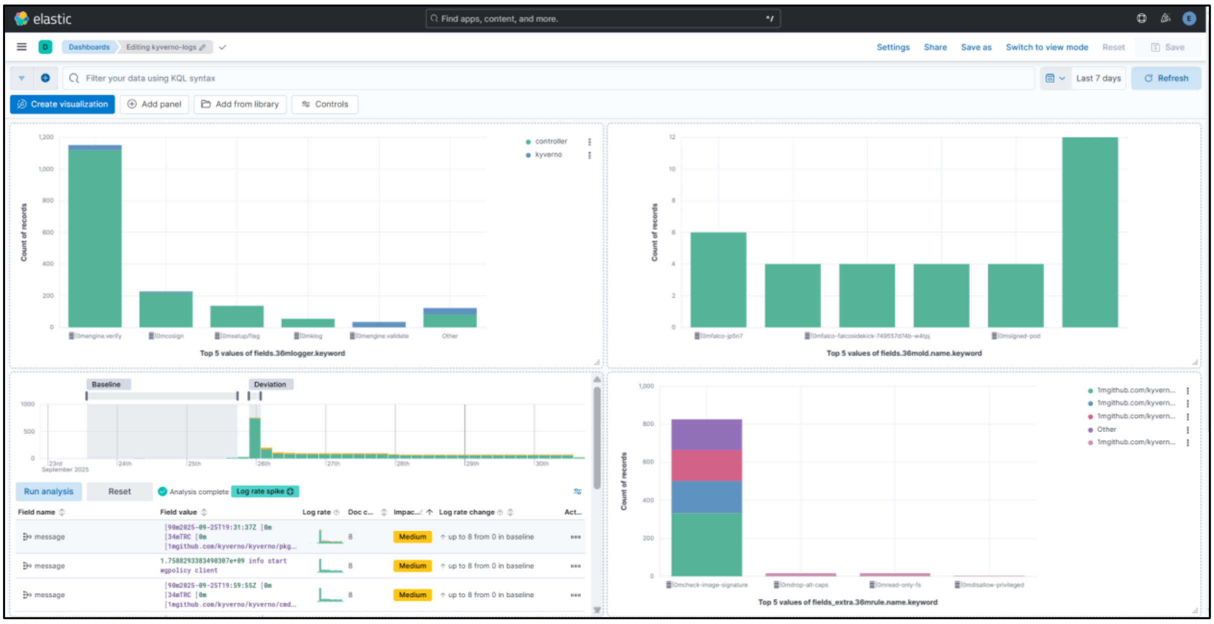

elastic
Find apps, content, and more.
Dashboards
[Logs Suricata] Alert Overview
Managed
Full screen
Share
Duplicate
Reset
Filter your data using KQL syntax
Last 24 hours
Refresh
Alert - Source Location [Logs Suricata]
Alert - Destination Location [Logs Suricata]
NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
OCEANIA
AUSTRALIA
zoom: 0.78
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Columns 9
Sort fields 1

Alerts [Logs Suricata]

2,219 documents

@timestamp	host.name	suricata.eve.flow_id	source.ip	source.port	destination.ip	destination.port	source.geo.country_iso_code	destination.geo.country_iso_code
Sep 30, 2025 @ 14:04:44.485	-	1241597595344513	193.46.255.103	10,590	172.29.0.11	22	RO	-
Sep 30, 2025 @ 14:01:35.869	-	2100255566949999	14.103.237.195	56,198	172.29.0.11	22	CN	-
Sep 30, 2025 @ 13:58:59.311	-	1057956213066722	193.46.255.99	59,442	172.29.0.11	22	RO	-
Sep 30, 2025 @ 13:58:32.766	-	195150707805272	165.154.244.165	34,584	172.29.0.11	22	HK	-

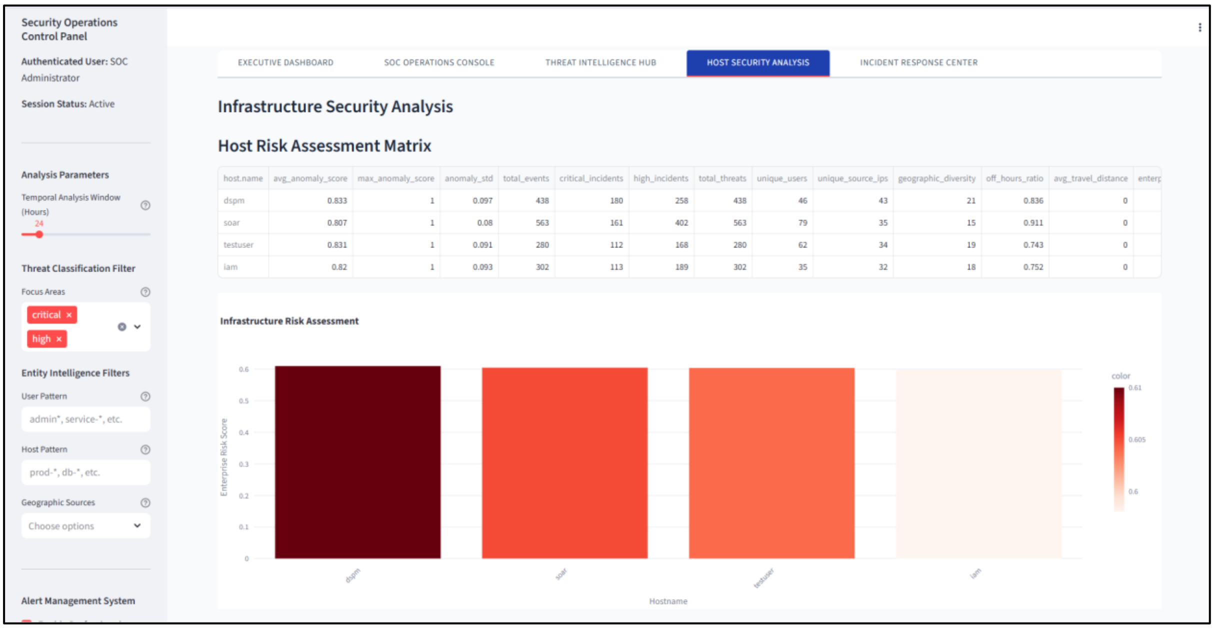
- CNAPP Dashboard: Misconfiguration trends and Kubernetes policy violation heatmaps.



Field name	Field value	Log rate	Doc c...	Impac...	Log rate change	Act...
message	[90m2025-09-25T19:31:37Z [0m [34mTRC [0m [1mgithub.com/kyverno/kyverno/pkg...		8	Medium	up to 8 from 0 in baseline	
message	1.7588293383490307e+09 info start wgpolicy client		8	Medium	up to 8 from 0 in baseline	
message	[90m2025-09-25T19:59:55Z [0m [34mTRC [0m [1mgithub.com/kyverno/kyverno/cmd...		8	Medium	up to 8 from 0 in baseline	

- All dashboards were tested for filter responsiveness and real-time updates.

- **Streamlit Dashboards (UEBA)**
  - Analyst View: Real-time KPIs, anomaly heatmaps, geo-IP visualizations, drill-downs.
  - Dashboards consistently loaded in <2 seconds at 95th percentile and maintained ≥90% field coverage.



host.name	avg_anomaly_score	max_anomaly_score	anomaly_std	total_events	critical_incidents	high_incidents	total_threats	unique_users	unique_source_ips	geographic_diversity	off_hours_ratio	avg_travel_distance	enterp
dspm	0.833	1	0.097	438	180	258	438	46	43	21	0.836	0	
soar	0.807	1	0.08	563	161	402	563	79	35	15	0.911	0	
testuser	0.831	1	0.091	280	112	168	280	62	34	19	0.743	0	
iam	0.82	1	0.093	302	113	189	302	35	32	18	0.752	0	

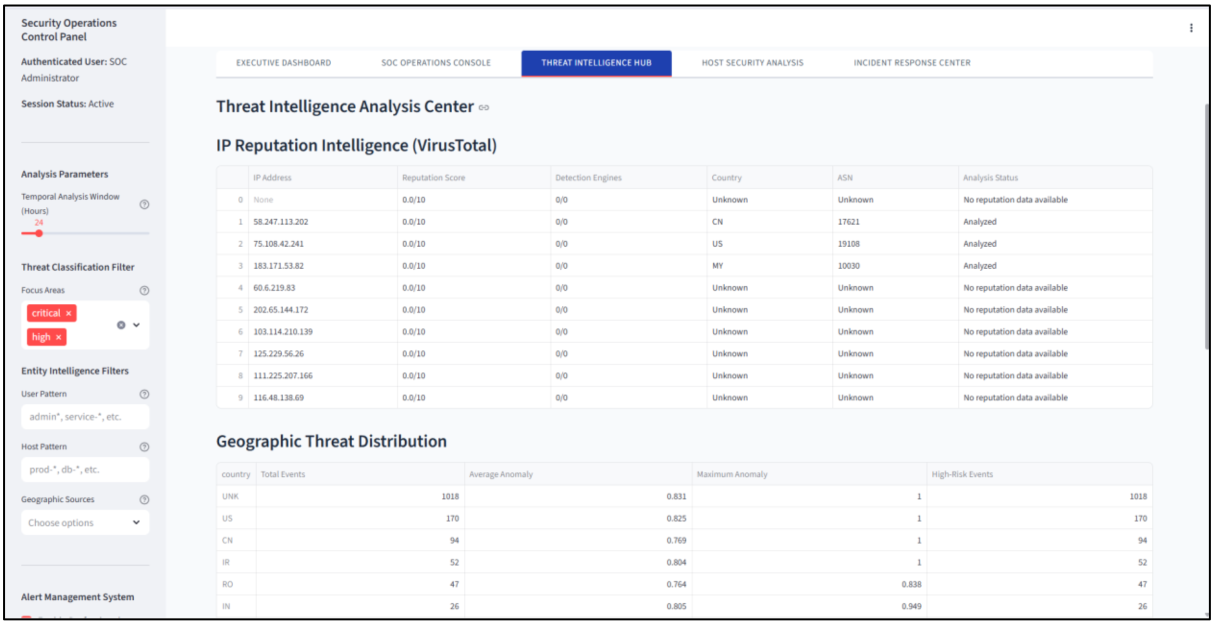
PoC Evidence:

Screenshots of Kibana visualizations and Streamlit interface confirm real-time visibility and proper aggregation.

5. Automation & Response Workflows

Tines playbooks were tested for enrichment and response automation:

- **Enrichment:**
  IPs from UEBA anomalies were automatically enriched with VirusTotal reputation data; enrichment results appeared in both alerts and Streamlit anomaly views.



Security Operations Control Panel

Authenticated User: SOC Administrator

Session Status: Active

Analysis Parameters

Temporal Analysis Window (Hours): 24

Threat Classification Filter

Focus Areas: critical, high

Entity Intelligence Filters

User Pattern: admin*, service-*, etc.

Host Pattern: prod-*, db-*, etc.

Geographic Sources: Choose options

Alert Management System

Threat Intelligence Analysis Center

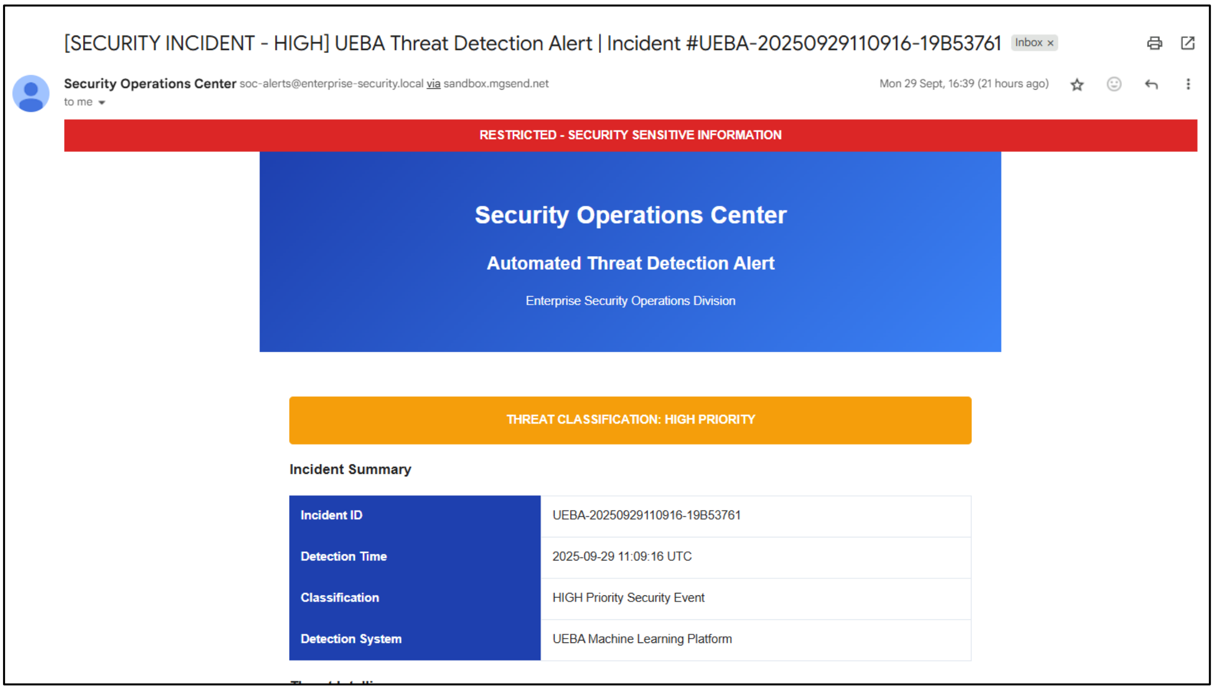
IP Reputation Intelligence (VirusTotal)

	IP Address	Reputation Score	Detection Engines	Country	ASN	Analysis Status
0	None	0.0/10	0/0	Unknown	Unknown	No reputation data available
1	58.247.113.202	0.0/10	0/0	CN	17621	Analyzed
2	75.108.42.241	0.0/10	0/0	US	19108	Analyzed
3	183.171.53.82	0.0/10	0/0	MY	10030	Analyzed
4	60.6.219.83	0.0/10	0/0	Unknown	Unknown	No reputation data available
5	202.65.144.172	0.0/10	0/0	Unknown	Unknown	No reputation data available
6	103.114.210.139	0.0/10	0/0	Unknown	Unknown	No reputation data available
7	125.229.56.26	0.0/10	0/0	Unknown	Unknown	No reputation data available
8	111.225.207.166	0.0/10	0/0	Unknown	Unknown	No reputation data available
9	116.48.138.69	0.0/10	0/0	Unknown	Unknown	No reputation data available

Geographic Threat Distribution

country	Total Events	Average Anomaly	Maximum Anomaly	High-Risk Events
UNK	1018	0.831	1	1018
US	170	0.825	1	170
CN	94	0.769	1	94
IR	52	0.804	1	52
RO	47	0.764	0.838	47
IN	26	0.805	0.949	26

- **Email Alerting:**
  HTML alert emails were received for critical anomalies with severity color-coding, context, and recommendations. Rate limiting ensured no duplicate alerts were sent during bursts.



[SECURITY INCIDENT - HIGH] UEBA Threat Detection Alert | Incident #UEBA-20250929110916-19B53761

Security Operations Center soc-alerts@enterprise-security.local via sandbox.mgsend.net

to me

Mon 29 Sept, 16:39 (21 hours ago)

RESTRICTED - SECURITY SENSITIVE INFORMATION

Security Operations Center

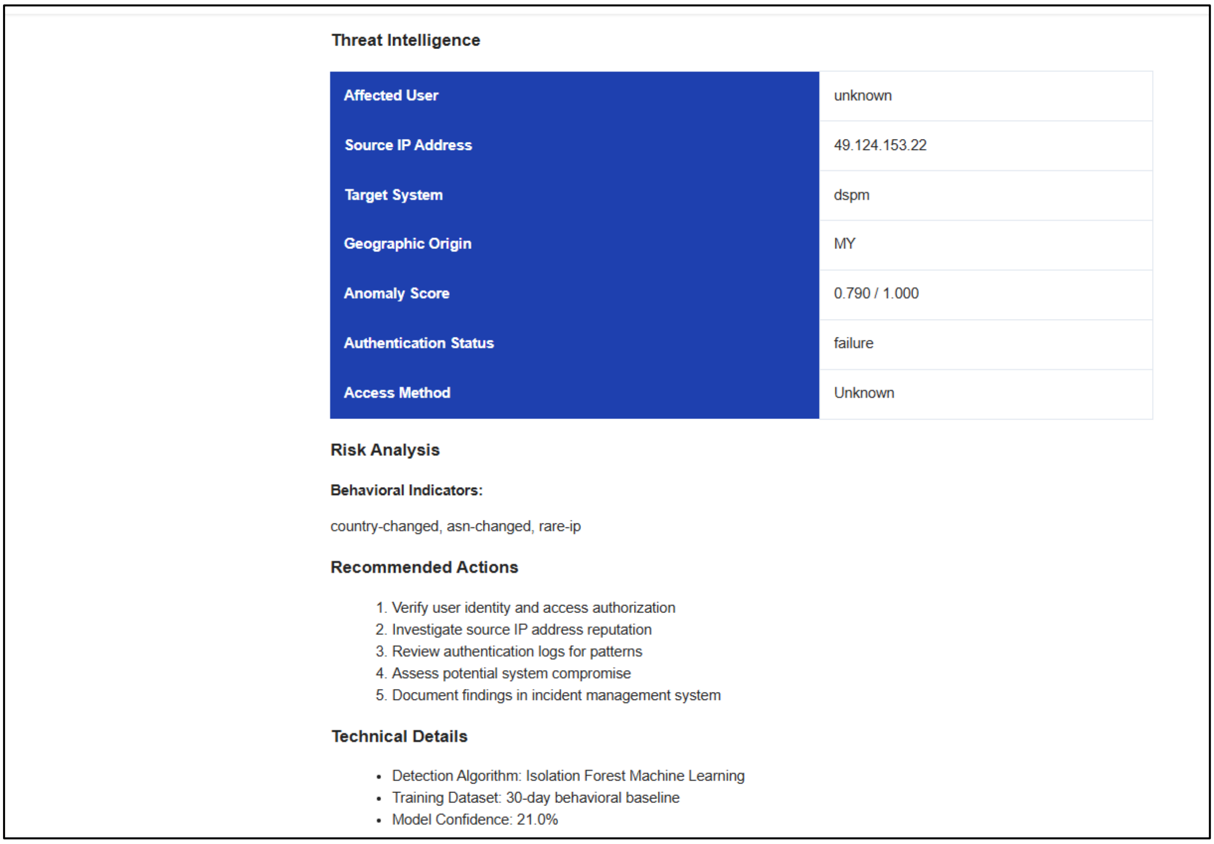
Automated Threat Detection Alert

Enterprise Security Operations Division

THREAT CLASSIFICATION: HIGH PRIORITY

Incident Summary

Incident ID	UEBA-20250929110916-19B53761
Detection Time	2025-09-29 11:09:16 UTC
Classification	HIGH Priority Security Event
Detection System	UEBA Machine Learning Platform



Threat Intelligence

Affected User	unknown
Source IP Address	49.124.153.22
Target System	dspm
Geographic Origin	MY
Anomaly Score	0.790 / 1.000
Authentication Status	failure
Access Method	Unknown

Risk Analysis

Behavioral Indicators:

country-changed, asn-changed, rare-ip

Recommended Actions

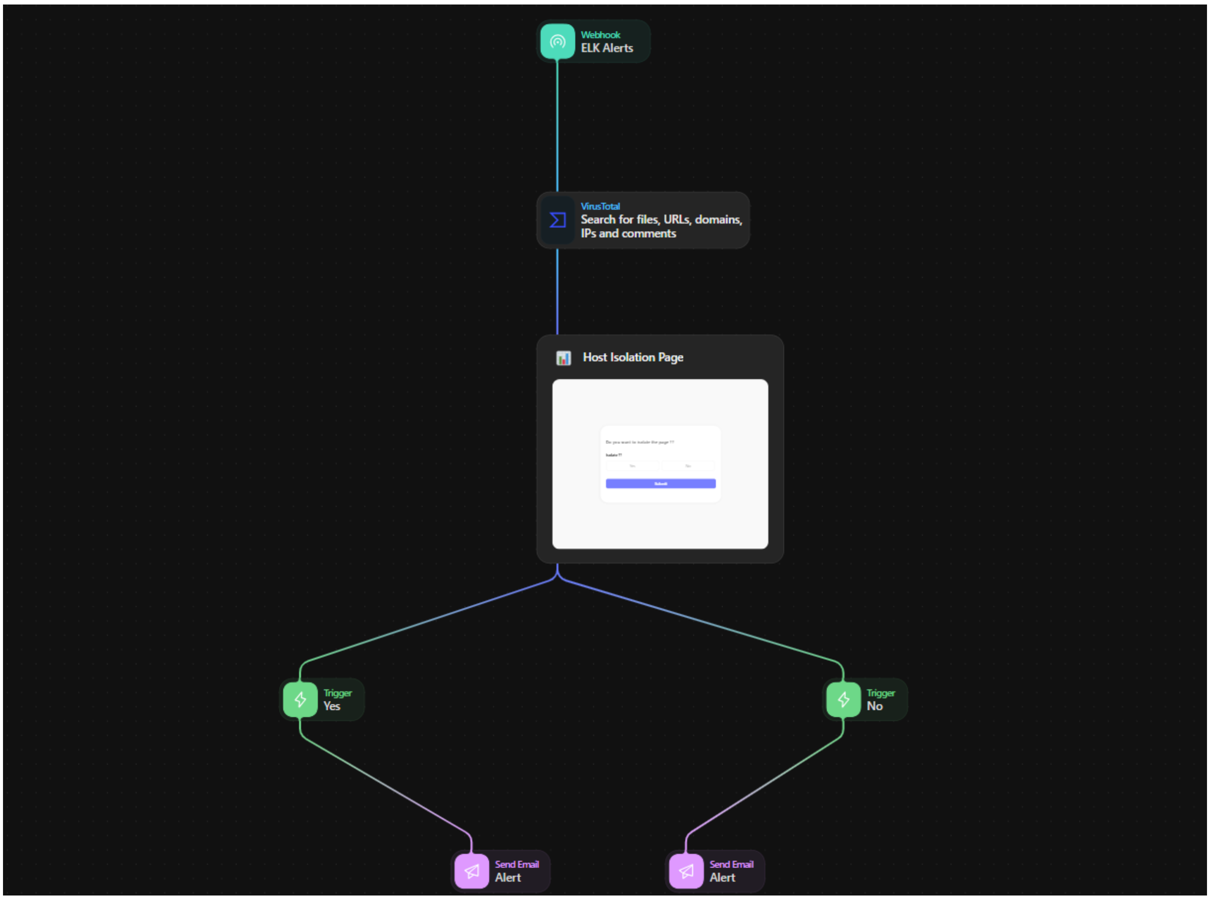
1. Verify user identity and access authorization
2. Investigate source IP address reputation
3. Review authentication logs for patterns
4. Assess potential system compromise
5. Document findings in incident management system

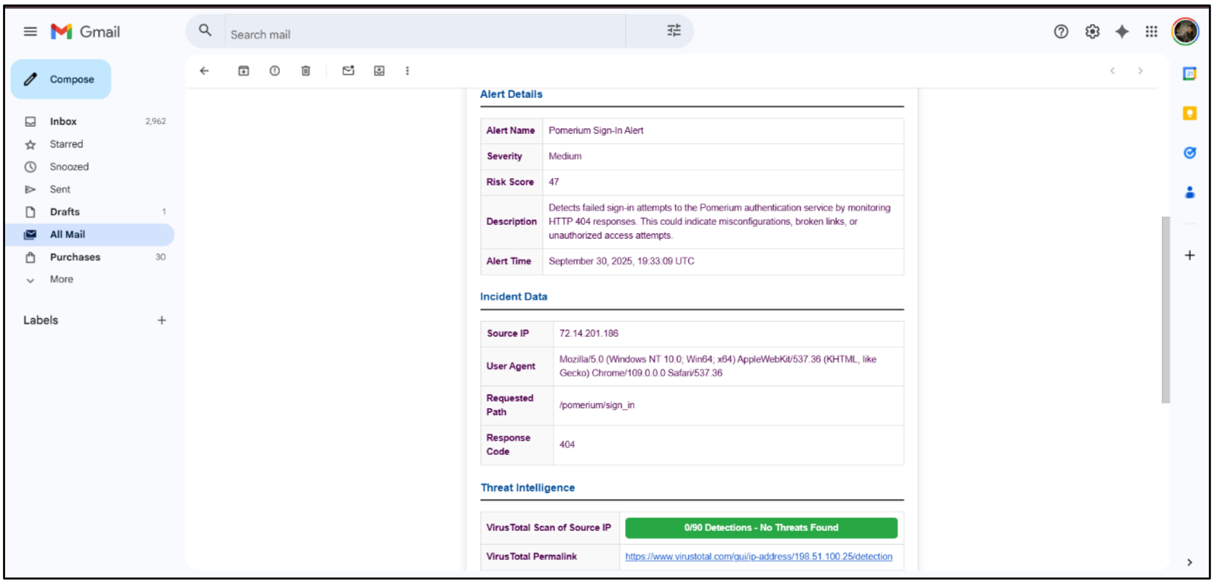
Technical Details

- Detection Algorithm: Isolation Forest Machine Learning
- Training Dataset: 30-day behavioral baseline
- Model Confidence: 21.0%

- **Host Isolation Simulation:**

  A critical severity alert was simulated to trigger a containment workflow. Tines initiated a predefined host isolation action, confirmed via log output.





Alert Details

Alert Name	Pomerium Sign-In Alert
Severity	Medium
Risk Score	47
Description	Detects failed sign-in attempts to the Pomerium authentication service by monitoring HTTP 404 responses. This could indicate misconfigurations, broken links, or unauthorized access attempts.
Alert Time	September 30, 2025, 19:33:09 UTC

Incident Data

Source IP	72.14.201.186
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
Requested Path	/pomerium/sign_in
Response Code	404

Threat Intelligence

VirusTotal Scan of Source IP	0/90 Detections - No Threats Found
VirusTotal Permalink	https://www.virustotal.com/gui/ip-address/198.51.100.25/detection

Summary of Validation

The combined evidence confirms that:

- All telemetry sources were successfully ingested, parsed, and visualized.
- Detection rules triggered reliably for simulated attack scenarios.
- The UEBA subsystem effectively detected and explained anomalous SSH behavior.
- Dashboards provided real-time insights with strong performance guarantees.
- Automation workflows enriched alerts and executed response actions as intended.

This demonstrates that the **XDR / Insider Risk solution is fully operational, technically sound, and detection-ready** for both known and insider threat scenarios.

8. Requirement ↔ Evidence Mapping Table

The following table provides a structured mapping between **stated requirements** for the XDR / Insider Risk solution and the **evidence** collected during deployment and validation. This ensures traceability, accountability, and alignment between objectives and deliverables.

Requirement	Implemented Solution / Work Done	Evidence / Validation
Centralized log aggregation from diverse telemetry sources	Deployed ELK Stack with Elastic Agents and syslog to collect logs from ZTNA (Pomerium, pfSense), DSPM (Presidio, Custodian), CDP(Churn model), CNAPP (Chekhov, Kyverno), Suricata IDS, and system authentication logs.	Kibana index pattern overviews showing structured ingestion for all sources; sample log search queries; ingestion validation screenshots.
Real-time detection and alerting for key security scenarios	Configured Kibana detection rules for failed/suspicious logins, DLP violations, IDS signatures, IaC misconfigurations, and Kubernetes policy violations.	Detection rules triggered during simulations (e.g., failed login, Nmap scan, DLP upload, IaC misconfigurations); alert panels in Kibana showing correct classifications.
Behavioral analytics for insider risk detection	Implemented UEBA subsystem using Isolation Forest for SSH anomaly detection with per-user	Streamlit dashboard anomaly visualizations; simulated SSH anomalies scored High/Critical;

	baselines and enrichment (GeoIP, ASN, VirusTotal).	explainability outputs showing behavioral factors; alert emails.
Actionable dashboards for SOC analysts and stakeholders	Built Kibana dashboards for each telemetry source with SOC-focused KPIs; Streamlit dashboards for UEBA with Analyst and Stakeholder views.	Screenshots of Kibana dashboards (ZTNA, DSPM, IDS, CNAPP) and Streamlit dashboards (KPI tiles, geo-visualizations, anomaly distributions).
Automated enrichment and response	Integrated Tines for IP reputation enrichment (VirusTotal), HTML email alerts, and host isolation playbooks for critical alerts.	Captured Tines workflow execution logs; enriched alert payloads; received HTML alerts for anomalies; host isolation simulation logs.
Performance and reliability in telemetry processing	Configured JSON parsing, ECS normalization, index routing, logrotate, and alert rate-limiting. Benchmarked dashboard performance and ensured field coverage.	Dashboard load time <2s (95th percentile); ≥90% field availability verified; logrotate and rate-limit configurations applied; performance test screenshots.
Scalability and modularity for future integrations	Designed the architecture with modular ingestion pipelines and dedicated indices, supporting future onboarding of new telemetry sources and expanded UEBA coverage.	Architecture & Data Flow Diagram; modular pipeline configuration files; documented ingestion and detection workflows for additional sources.

Summary

The evidence clearly demonstrates that each requirement has been addressed through targeted implementation steps and validated through hands-on testing. The system provides **comprehensive telemetry visibility**, **effective detection and response**, and **behavioral analytics for insider threat detection**, while maintaining a modular and extensible architecture for future scalability.

9. Conclusion

Achievements

The XDR / Insider Risk implementation successfully demonstrated a **fully integrated, open-source detection and response ecosystem** capable of ingesting diverse telemetry, applying both rule-based and behavioral detections, and automating critical response actions. Key achievements include:

- **Comprehensive Telemetry Integration**
  Successfully centralized logs from ZTNA, DSPM, CNAPP, network IDS, Kubernetes, and endpoint authentication sources into the ELK Stack with proper parsing, ECS normalization, and index segmentation.
- **Effective Detection Engineering**
  Deployed robust Kibana rules to detect failed and suspicious logins, DLP violations, network scanning and exploit activity, IaC misconfigurations, and Kubernetes policy breaches. All rules were validated through controlled attack simulations.
- **Behavioral Analytics for Insider Threats**
  Developed a UEBA subsystem that leverages Isolation Forest models for SSH anomaly detection using per-user baselines, geo/IP rarity, ASN shifts, and behavioral context. High-fidelity anomalies were enriched with threat intel and explained with top contributing factors for analyst triage.
- **Operational Dashboards**
  Built interactive Kibana and Streamlit dashboards tailored for SOC analysts and stakeholders. These dashboards provide real-time KPIs, anomaly trends, and investigative drill-downs, with strong performance guarantees (load times <2 s and ≥90 % field availability).
- **Security Automation**
  Integrated Tines to automate enrichment (VirusTotal), alerting (HTML notifications), and containment (host isolation) workflows, reducing manual response time and ensuring consistency.
- **Alignment with Zero Trust Principles**
  The solution provides identity-aware telemetry, context-driven detections, and layered

visibility, supporting strategic move toward a Zero Trust, behavior-aware security posture.

Gaps Identified

While the prototype fulfills its intended objectives, several **gaps remain to be addressed** for production-scale deployment:

- **Scalability**
  The ELK Stack and UEBA engine are deployed on single nodes without clustering, limiting horizontal scale and high availability.
- **Data Retention and Compliance**
  Log storage uses short retention policies suitable for testing but insufficient for compliance frameworks that require long-term archival and forensic replay.
- **Cross-Source Correlation**
  Detection rules are primarily source-specific; advanced correlation (e.g., linking authentication anomalies with network IDS alerts or DLP triggers) is not yet implemented.
- **Identity & Context Enrichment**
  UEBA is currently limited to SSH telemetry; it lacks federation with enterprise identity providers, SaaS usage data, and HR/asset context for richer behavioral baselining.
- **Automated Source Onboarding**
  Log ingestion pipelines require manual setup for each source. Self-service onboarding or templated ingestion workflows are not yet present.
- **Security Hardening**
  Basic authentication is used for dashboards; granular RBAC, MFA, encrypted transport, and key rotation policies are not yet in place.

These gaps were intentionally scoped out during the prototype phase to focus on functional correctness and detection capability.

Roadmap

To evolve this prototype into a **production-grade XDR and Insider Risk platform**, the following roadmap is recommended:

Short-Term

- Implement Elasticsearch clustering and index lifecycle management for improved scalability and retention.
- Harden authentication, enable TLS for all log transport, and implement role-based dashboard access.
- Expand detection content with additional insider threat rules (e.g., privilege escalation, lateral movement correlations).
- Optimize enrichment pipelines for speed and reliability.

Mid-Term

- Develop advanced cross-source correlation rules and entity risk scoring.
- Extend UEBA coverage beyond SSH to include web access, cloud authentication logs, and privileged actions.
- Automate ingestion onboarding with standardized templates and configuration management.
- Integrate additional threat intelligence feeds for broader enrichment coverage.

Long-Term

- Federate UEBA models with enterprise IdPs, asset inventories, and HR systems for richer behavioral context.
- Introduce SOAR-style orchestrations for complex multi-stage response workflows.
- Align the platform with regulatory frameworks (e.g., ISO 27001, NIST 800-53) and establish audit/compliance pipelines.
- Conduct red-team vs blue-team exercises to fine-tune detections and validate operational maturity.

Final Remarks

This solution establishes a **technically sound, modular, and extensible XDR foundation** that unifies telemetry, analytics, and response for both external and insider threat scenarios. Through strategic enhancements in scalability, correlation, identity integration, and security hardening, this platform can mature into a **full-scale enterprise XDR and insider risk defense capability**.

The success of this prototype also highlights the **viability of open-source technologies** for advanced detection engineering when combined with thoughtful architecture and operational discipline.