# SOC MONITORING DASHBOARD

## DOCUMENTATIONS & STRUCTURE


QUERYTEL | CANADA | FEBRUARY 09 2026

# INTRODUCTION

Security Operations Centers operate in environments where visibility, speed, and accuracy are critical. As organizations grow in scale and complexity, security monitoring must evolve from isolated alerting tools into unified operational systems that support continuous oversight and informed decision-making.

This document describes the structure and behavior of the SOC Monitoring Dashboard developed by QueryTel Inc. The purpose of this documentation is to explain how the system supports security operations through real-time monitoring, operational awareness, and workflow alignment, without relying on manual interpretation of raw security data.

The dashboard is designed to serve as a centralized operational interface for security teams. It provides a consistent view of organizational security posture while supporting day-to-day monitoring, incident handling, and long-term analysis. The focus of this document is not on visual layout or user interface elements, but on the underlying system behaviors, workflows, and security practices that enable the dashboard to function as an effective SOC control surface.

# SOC OVERVIEW PAGE – OPERATIONAL BEHAVIOR

The SOC platform operates in a continuous monitoring state that serves as the default runtime mode for security operations. In this state, live telemetry from network security devices, identity systems, application controls, and infrastructure components is ingested in real time and maintained as an always-current representation of the operational environment. The system is designed to support persistent situational awareness rather than ad-hoc investigation.

Incoming data flows through a real-time ingestion and normalization pipeline that converts heterogeneous sources into a unified event model. Events are classified immediately upon arrival, allowing security-relevant activity to be evaluated through centralized detection and correlation logic while normal operational behavior is retained to establish behavioral baselines. This approach reflects standard SOC practices for noise reduction and sustained observability.

Event correlation is performed continuously across time, source, and identity domains. By maintaining temporal context, the platform can distinguish isolated anomalies from emerging threat patterns such as repeated authentication failures, abnormal outbound communication, or coordinated network probing. This detection model aligns with modern SOC workflows that prioritize behavioral analysis and risk progression over single-event alerting.

From the correlated event state, higher-level operational signals are derived, including detection and response latency, overall risk posture, and identity-related risk indicators. These values are recalculated dynamically as conditions evolve, enabling early prioritization and triage without requiring manual correlation. This supports both Tier 1 monitoring and Tier 2 escalation workflows.

In parallel, the platform evaluates the health and load of its enforcement and observation infrastructure. Telemetry from edge nodes, firewalls, and inspection layers is assessed alongside security signals, ensuring that potential incidents are interpreted in proper operational context. This reflects best practices in resilient SOC design, where security visibility is tightly coupled with infrastructure awareness.

Outbound traffic behavior is evaluated as a first-class signal, independent of inbound threat detection. The system continuously analyzes egress destinations, geographic patterns, and traffic volumes to identify potential command-and-control activity or data exfiltration. This capability supports proactive threat hunting and aligns with modern SOC strategies that emphasize full traffic lifecycle visibility.

Overall, the platform provides a synthesized operational state that enables continuous monitoring, early triage, and posture validation. Analysts consume system-generated insight rather than raw telemetry, allowing human effort to focus on decision-making and response rather than data filtering. The SOC platform operates in a continuous monitoring state that serves as the default runtime mode for security operations. In this state, live telemetry from network security devices, identity systems, application controls, and infrastructure components is ingested in real time and maintained as an always-current representation of the operational environment. The system is designed to support persistent situational awareness rather than ad-hoc investigation.

Incoming data flows through a real-time ingestion and normalization pipeline that converts heterogeneous sources into a unified event model. Events are classified immediately upon arrival, allowing security-relevant activity to be evaluated through centralized detection and correlation logic while normal operational behavior is retained to establish behavioral baselines. This approach reflects standard SOC practices for noise reduction and sustained observability.

Event correlation is performed continuously across time, source, and identity domains. By maintaining temporal context, the platform can distinguish isolated anomalies from emerging threat patterns such as repeated authentication failures, abnormal outbound communication, or coordinated network probing. This detection model aligns with modern SOC workflows that prioritize behavioral analysis and risk progression over single-event alerting.

From the correlated event state, higher-level operational signals are derived, including detection and response latency, overall risk posture, and identity-related risk indicators. These values are recalculated dynamically as conditions evolve, enabling early prioritization and triage without requiring manual correlation. This supports both Tier 1 monitoring and Tier 2 escalation workflows.

In parallel, the platform evaluates the health and load of its enforcement and observation infrastructure. Telemetry from edge nodes, firewalls, and inspection layers is assessed alongside security signals, ensuring that potential incidents are interpreted in proper operational context. This reflects best practices in resilient SOC design, where security visibility is tightly coupled with infrastructure awareness.

Outbound traffic behavior is evaluated as a first-class signal, independent of inbound threat detection. The system continuously analyzes egress destinations, geographic patterns, and traffic volumes to identify potential command-and-control activity or data exfiltration. This capability supports proactive threat hunting and aligns with modern SOC strategies that emphasize full traffic lifecycle visibility.


Overall, the platform provides a synthesized operational state that enables continuous monitoring, early triage, and posture validation. Analysts consume system-generated insight rather than raw telemetry, allowing human effort to focus on decision-making and response rather than data filtering. The SOC platform operates in a continuous monitoring state that serves as the default runtime mode for security operations. In this state, live telemetry from network security devices, identity systems, application controls, and infrastructure components is ingested in real time and maintained as an always-current representation of the operational environment. The system is designed to support persistent situational awareness rather than ad-hoc investigation.

Incoming data flows through a real-time ingestion and normalization pipeline that converts heterogeneous sources into a unified event model. Events are classified immediately upon arrival, allowing security-relevant activity to be evaluated through centralized detection and correlation logic while normal operational behavior is retained to establish behavioral baselines. This approach reflects standard SOC practices for noise reduction and sustained observability.

Event correlation is performed continuously across time, source, and identity domains. By maintaining temporal context, the platform can distinguish isolated anomalies from emerging threat patterns such as repeated authentication failures, abnormal outbound communication, or coordinated network probing. This detection model aligns with modern SOC workflows that prioritize behavioral analysis and risk progression over single-event alerting.

From the correlated event state, higher-level operational signals are derived, including detection and response latency, overall risk posture, and identity-related risk indicators. These values are recalculated dynamically as conditions evolve, enabling early prioritization and triage without requiring manual correlation. This supports both Tier 1 monitoring and Tier 2 escalation workflows.

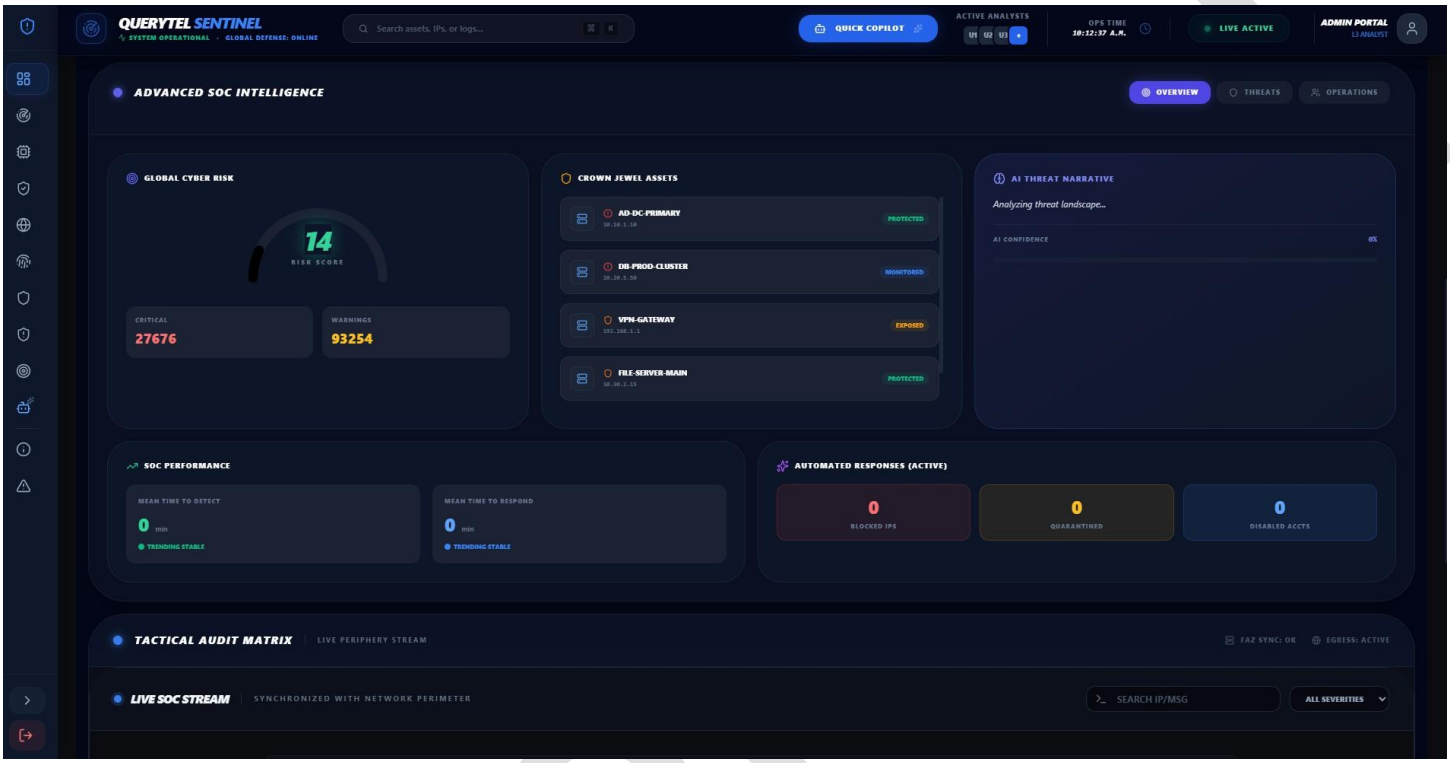
In parallel, the platform evaluates the health and load of its enforcement and observation infrastructure. Telemetry from edge nodes, firewalls, and inspection layers is assessed alongside security signals, ensuring that potential incidents are interpreted in proper operational context. This reflects best practices in resilient SOC design, where security visibility is tightly coupled with infrastructure awareness.

Outbound traffic behavior is evaluated as a first-class signal, independent of inbound threat detection. The system continuously analyzes egress destinations, geographic patterns, and traffic volumes to identify potential command-and-control activity or data exfiltration. This capability supports proactive threat hunting and aligns with modern SOC strategies that emphasize full traffic lifecycle visibility.

Overall, the platform provides a synthesized operational state that enables continuous monitoring, early triage, and posture validation. Analysts consume system-generated insight rather than raw telemetry, allowing human effort to focus on decision-making and response rather than data filtering.

# ADVANCED SOC INTELLIGENCE – RISK AND PRIORITIZATION WORKFLOWS

This module represents the transition from general situational awareness to prioritized security intelligence. While the platform continues to ingest and correlate telemetry in real time, emphasis shifts toward interpreting cumulative risk, asset criticality, and response readiness. Security signals are no longer viewed uniformly; they are evaluated in relation to business impact, exposure level, and current threat conditions.




At the system level, global risk scoring is derived from aggregated event severity, confidence, and distribution across monitored domains. Critical and warning-class signals contribute to a continuously recalculated risk posture rather than discrete alert counts. This allows the platform to express security state as a normalized risk signal, supporting leadership-level visibility without discarding underlying technical fidelity.

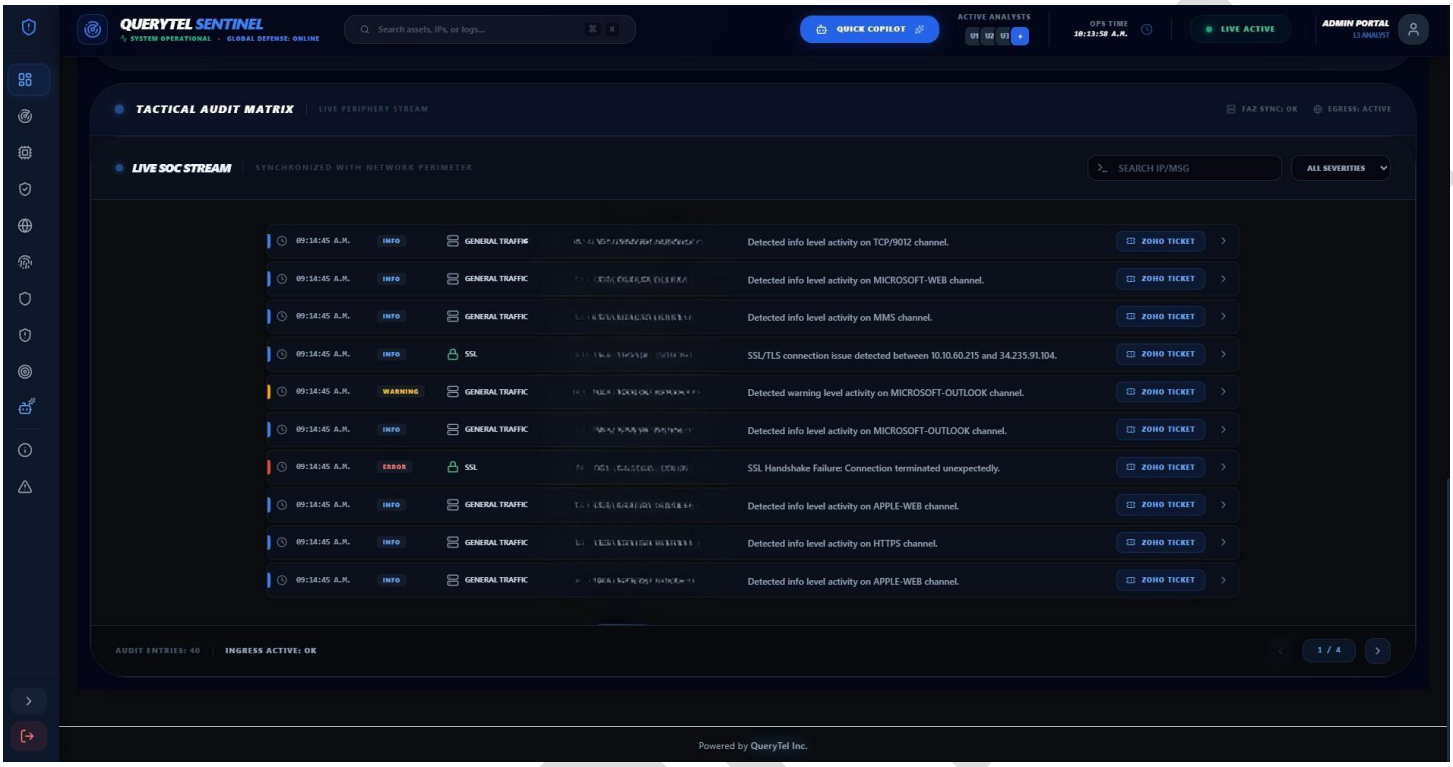
Crown jewel assets introduce asset-centric prioritization into the detection workflow. Designated high-value systems are continuously evaluated against their exposure, protection state, and observed activity. Changes in status reflect real-time correlation between asset importance and incoming security signals, ensuring that threats involving critical infrastructure receive immediate attention. This aligns with standard SOC practices that prioritize impact-driven response over equal treatment of all assets.

The intelligence layer also incorporates narrative-driven threat interpretation and response readiness indicators. Automated response actions are tracked alongside detection metrics, providing visibility into whether containment controls are actively engaged and effective. Mean time to detect and respond are treated as live operational indicators rather than retrospective KPIs, reinforcing a feedback loop between detection logic and response execution.

Overall, this module supports Tier 2 and SOC leadership workflows focused on prioritization, escalation readiness, and operational effectiveness. It reflects modern SOC practices that combine risk-based scoring, asset criticality modeling, and response automation awareness to ensure security effort is applied where it matters most.

# TACTICAL AUDIT MATRIX – REAL-TIME EVENT TRACEABILITY

This module represents the system's real-time audit and traceability layer, where correlated security and operational events are exposed as a live, ordered event stream. While upstream logic continues to classify, score, and correlate activity, this layer preserves event-level fidelity to support verification, compliance, and investigative workflows. Entries shown here are already normalized and severity-tagged, reflecting post-processing rather than raw log ingestion.



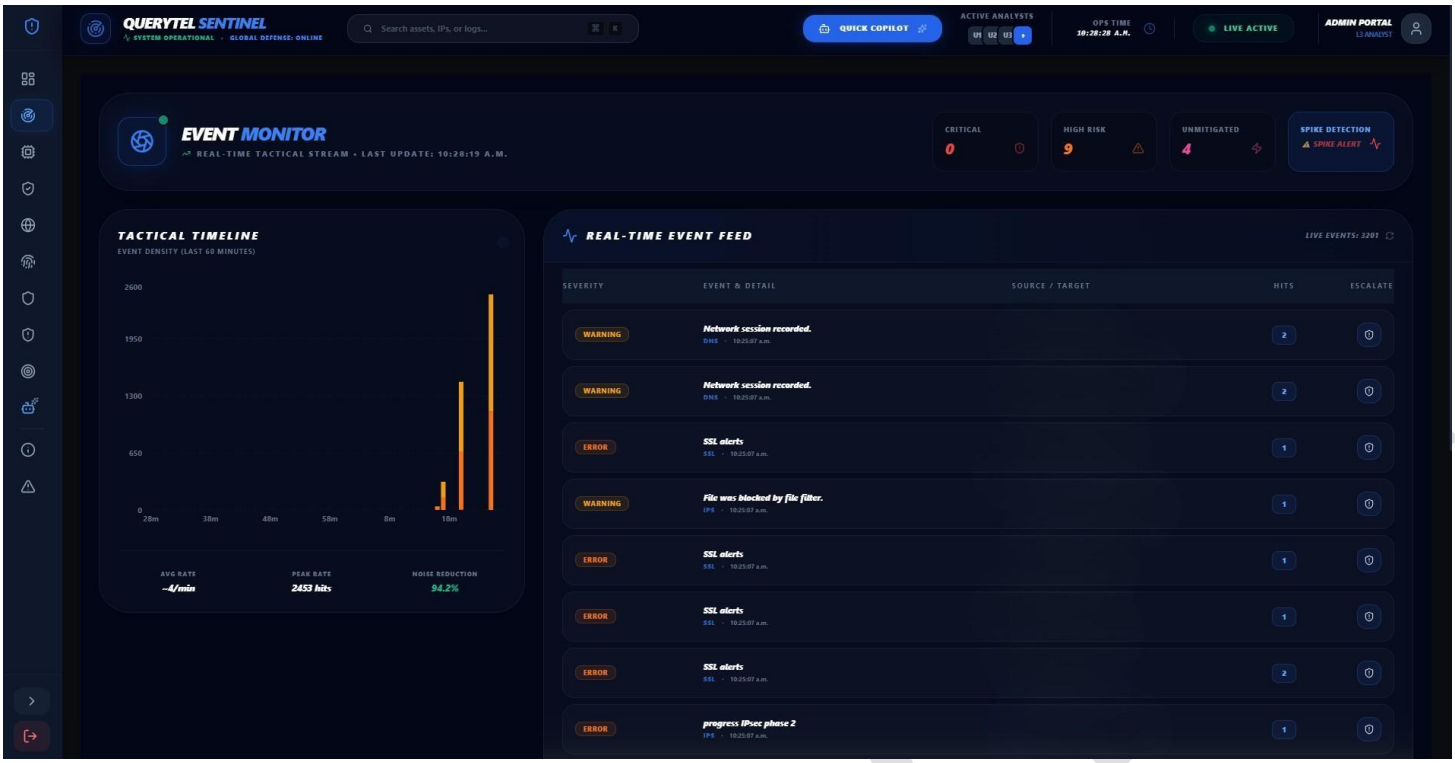

Operationally, this view supports Tier 1 and Tier 2 analyst workflows focused on validation and escalation. Analysts use the live stream to confirm detection accuracy, assess contextual details such as protocol behavior or connection failures, and determine whether an observed condition warrants escalation or ticket creation. The presence of structured handoff into incident management systems reflects a controlled transition from monitoring to response without bypassing auditability.

From a systems perspective, this layer enforces traceability between detection logic and human action. Each event remains timestamped, severity-scoped, and linked to its source context, ensuring that automated classification can be reviewed and that analyst decisions are defensible. This aligns with standard SOC and compliance practices that require verifiable evidence chains for investigations, audits, and post-incident analysis.

Overall, this module bridges continuous monitoring and formal incident response by providing a synchronized, real-time audit surface that preserves transparency while maintaining operational velocity.

# EVENT MONITOR – REAL-TIME DETECTION AND TRIAGE FLOW

This module represents the platform's real-time detection and triage layer, where security-relevant activity is observed as it emerges rather than after correlation cycles complete. While upstream systems continue normalization and risk evaluation, this layer focuses on immediacy, exposing live event density, severity distribution, and short-term behavioral spikes within a rolling time window. The system continuously recalculates event rates and suppresses baseline noise to ensure only meaningful deviations surface.

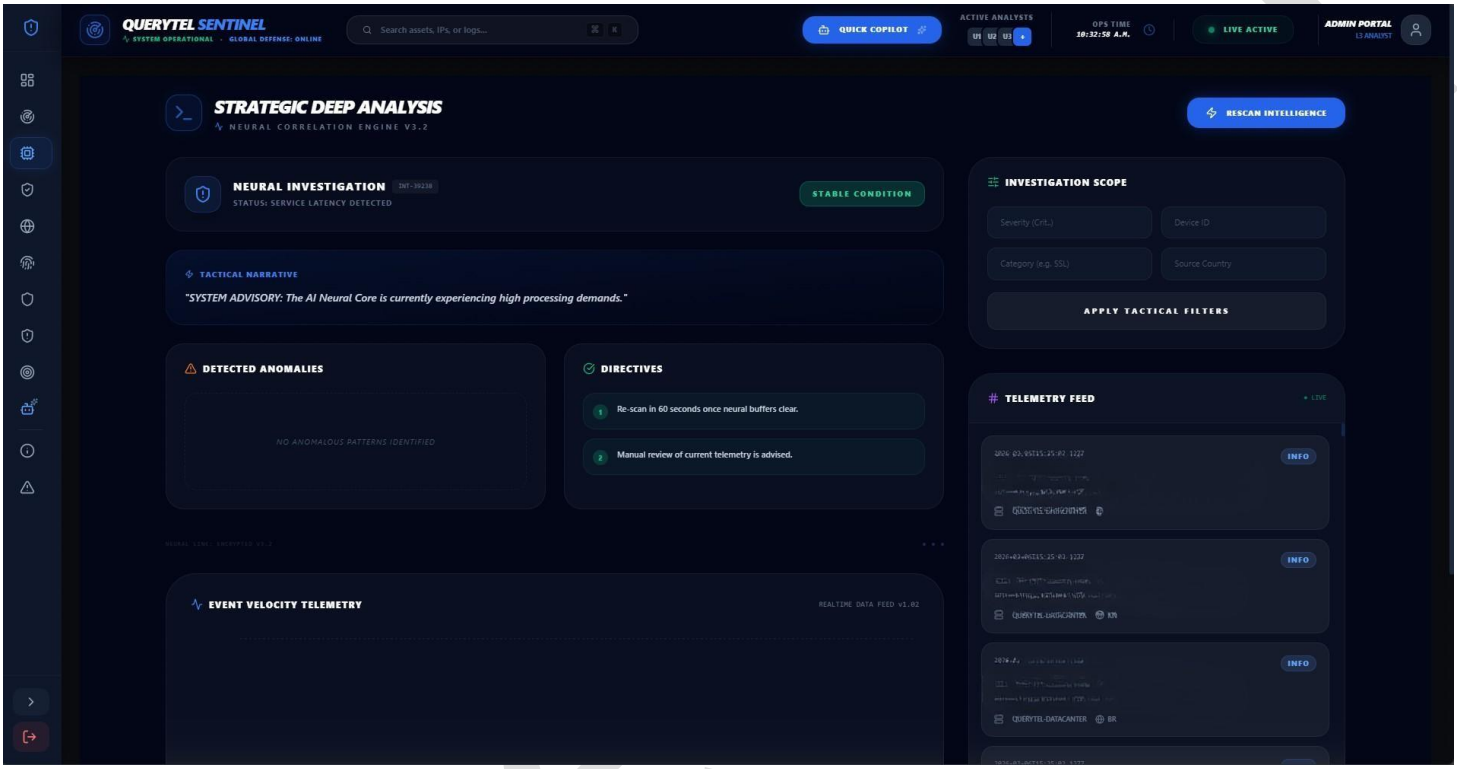



Operationally, this view supports Tier 1 analyst workflows centered on rapid assessment and early intervention. Analysts monitor temporal spikes, severity clustering, and repeated event hits to determine whether activity represents transient noise or the onset of an incident requiring escalation. Built-in spike detection reflects automated thresholding and anomaly awareness, reducing reliance on manual pattern recognition during high-volume periods.

From a practice standpoint, this module aligns with modern SOC designs that separate real-time signal observation from deeper correlation and investigation. By providing a high-fidelity, time-ordered event feed with severity context, the system enables fast human judgment while preserving traceability and controlled escalation paths, ensuring response speed without sacrificing consistency or auditability.

# STRATEGIC DEEP ANALYSIS – CORRELATION AND INVESTIGATION WORKFLOW

This module represents the platform's strategic investigation layer, activated when security conditions require deeper correlation beyond real-time monitoring and tactical triage. The system transitions into an analysis-driven mode where previously ingested and normalized telemetry is re-evaluated using expanded correlation windows, higher contextual sensitivity, and adaptive filtering. This layer does not introduce new data sources; it increases analytical depth over existing signals.



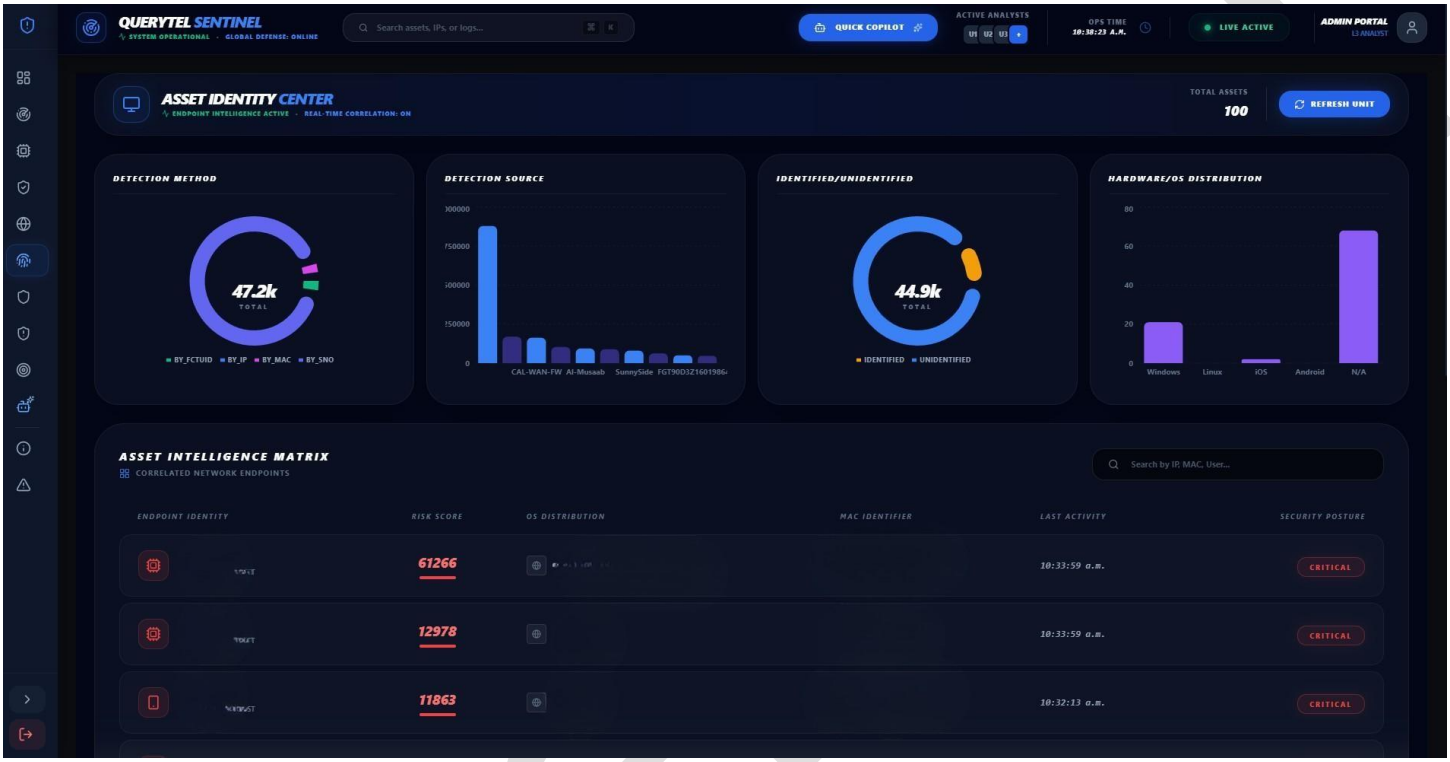

Operationally, this workflow supports Tier 2 and Tier 3 analyst activity focused on validation, hypothesis testing, and incident qualification. Analysts scope investigations by severity, category, device, or origin, allowing targeted reprocessing of telemetry without disrupting live monitoring workflows. Detected anomalies and advisory narratives are system-generated, providing guidance while preserving human authority over conclusions and response actions.

From a systems perspective, this layer emphasizes controlled reasoning and traceability. Correlation outcomes, investigative directives, and analyst interactions are preserved alongside supporting telemetry, ensuring that decisions are reproducible and defensible. This reflects standard SOC practices for advanced investigation, where analytical depth, auditability, and deliberate escalation take precedence over speed.

Overall, this module enables structured deep analysis without collapsing back into raw log inspection. It allows the SOC to transition smoothly from detection to understanding, ensuring that complex conditions are examined thoroughly before response actions are finalized.

# ASSET IDENTITY CENTER – ENDPOINT CONTEXT AND RISK ATTRIBUTION

This module represents the platform's asset and endpoint intelligence layer, where security telemetry is anchored to concrete identities rather than abstract events. The system continuously correlates network activity, detection signals, and behavioral observations to unique endpoints using multiple identification methods, allowing assets to be tracked even when attributes such as IP addresses or network locations change over time.



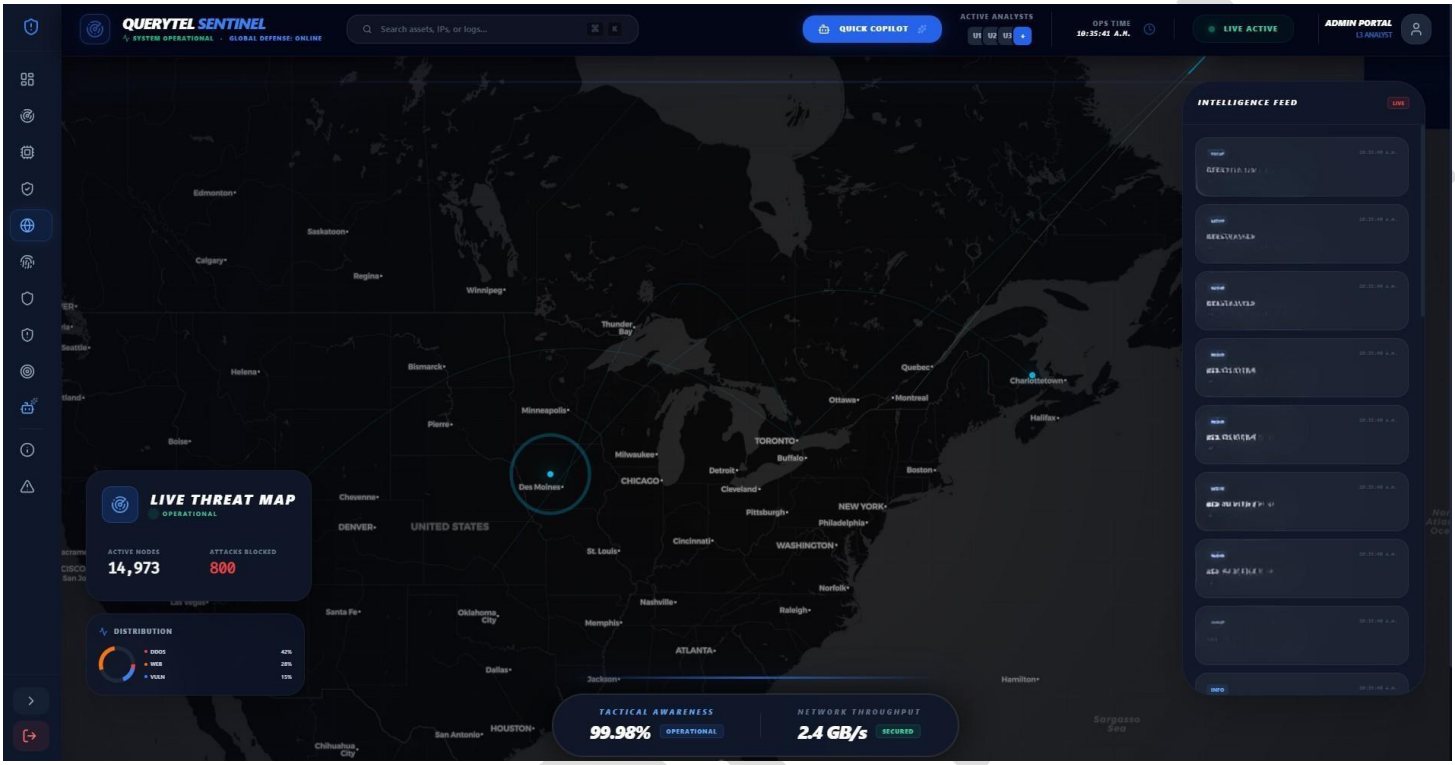

At a system level, endpoint identity is resolved through correlation across detection sources and identifiers, enabling the platform to distinguish identified assets from unknown or transient entities. Asset characteristics such as operating system, hardware class, and last observed activity are maintained as part of a continuously updated asset profile. This ensures that security signals are interpreted in the context of what the asset is, not just what it did.

Operationally, this layer supports Tier 1 through Tier 3 workflows focused on attribution and prioritization. Analysts can quickly assess which endpoints represent elevated risk based on accumulated behavior, exposure, and posture, rather than reacting to individual alerts in isolation. Risk scoring at the asset level enables consistent escalation decisions and prevents repeated investigation of the same underlying system across multiple events.

From a standards perspective, this approach aligns with modern SOC and zero-trust practices that treat asset identity as a foundational control. By maintaining persistent endpoint context and linking activity back to known or unknown assets, the platform enables stronger accountability, more accurate threat assessment, and more effective response planning.

# LIVE THREAT MAP – GEOSPATIAL SITUATIONAL AWARENESS

This module provides geospatial awareness by projecting correlated security activity onto a live geographic context. While detection and correlation continue upstream, the system translates network and threat telemetry into location-aware signals, allowing operators to understand where activity is originating, traversing, or being mitigated in real time. This layer does not introduce new detection logic; it contextualizes existing intelligence spatially.



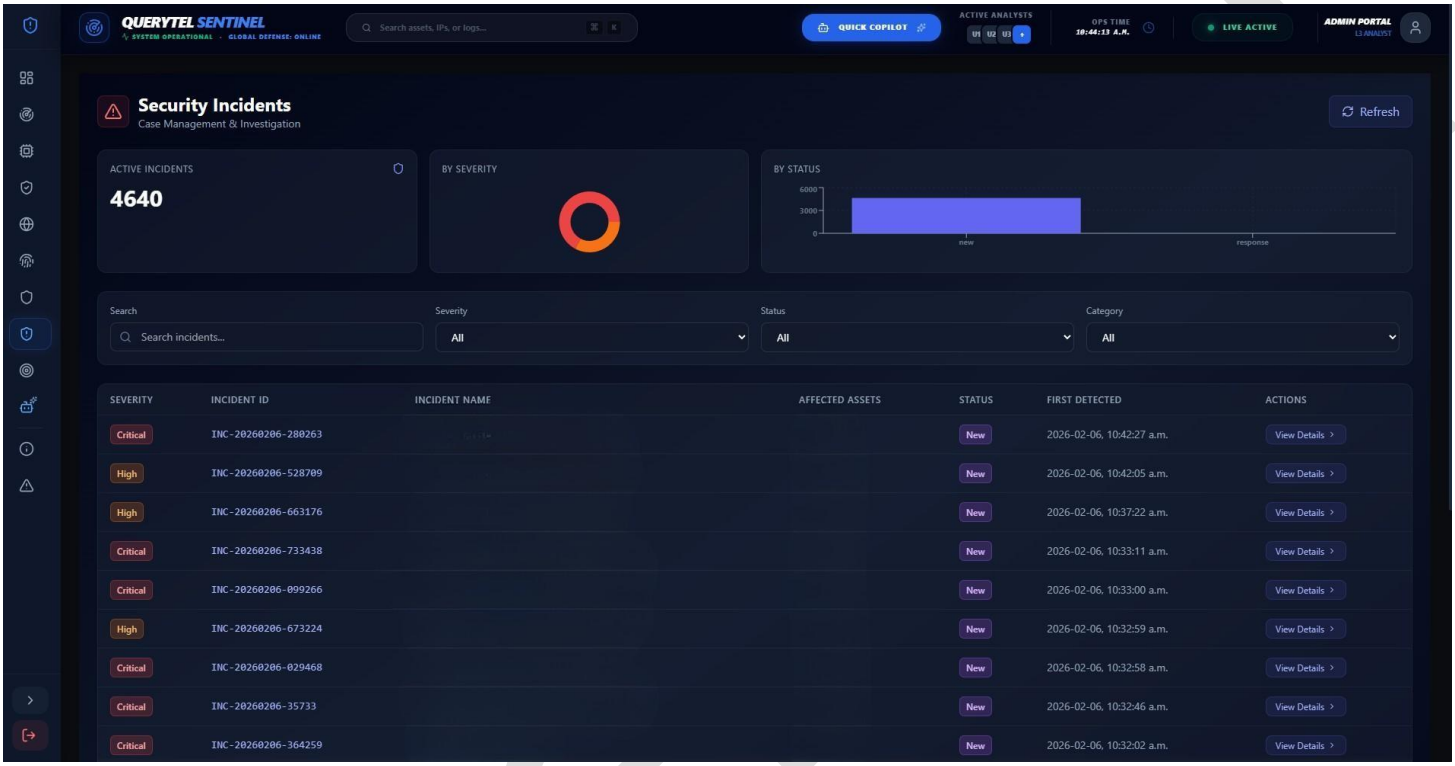

Operationally, this view supports SOC-wide situational awareness and rapid posture assessment. Analysts and SOC leads use geographic clustering, flow visualization, and active node distribution to quickly determine whether observed activity reflects localized anomalies, regional concentration, or distributed behavior. Blocked attack counts and throughput indicators provide immediate feedback on defensive effectiveness without requiring deeper investigation.

From a practice standpoint, this module aligns with standard SOC visualization patterns used for real-time awareness rather than decision-making. It enables fast comprehension during active conditions, supports executive-level briefings, and enhances coordination during incidents without replacing analytical or investigative workflows.

Overall, this layer serves as a shared operational reference point, ensuring that complex, high-volume activity can be understood at a glance without sacrificing the integrity of upstream analysis.

# SECURITY INCIDENTS – CASE MANAGEMENT AND RESPONSE WORKFLOW

This module represents the platform's formal incident management layer, where correlated security conditions are elevated into tracked, actionable cases. At this stage, detection and analysis have already occurred; the system transitions from signal interpretation to structured response coordination. Incidents are instantiated as discrete entities with defined severity, scope, affected assets, and lifecycle state.



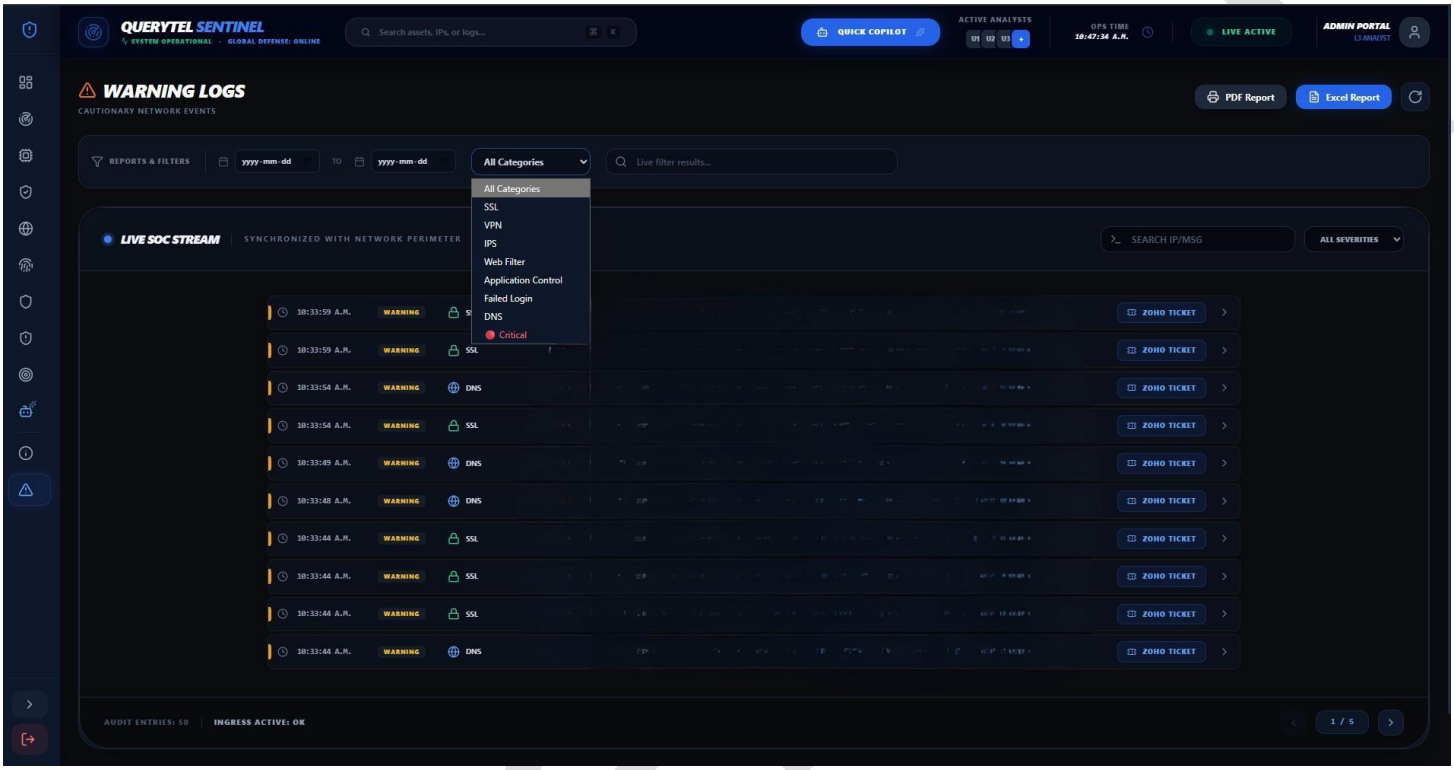

Operationally, this workflow supports Tier 2 and Tier 3 response activities. Analysts assess incident context, confirm impact, and manage progression through defined response states without re-evaluating raw telemetry. Incident identifiers, timestamps, and severity classifications ensure consistent handling, prioritization, and accountability across the SOC, while filtering and categorization support workload management during high-volume conditions.

From a systems and standards perspective, this layer enforces governance, traceability, and repeatability. Each incident maintains an auditable history linking detection, investigation, and response actions, aligning with established SOC, incident response, and compliance frameworks. This separation between detection logic and case management ensures that response actions are deliberate, reviewable, and defensible.

Overall, this module provides the authoritative record of security events requiring action, closing the operational loop between monitoring, analysis, and response execution.

# WARNING LOGS – PRE-INCIDENT OBSERVATION AND CONTROLLED ESCALATION

This module represents the platform's pre-incident observation layer, where cautionary security signals are retained, monitored, and evaluated without immediately triggering incident workflows. Events surfaced here have exceeded baseline behavior thresholds but have not yet met the criteria for formal incident creation. The system continues real-time ingestion and correlation while isolating these signals for closer scrutiny.




Operationally, this workflow supports Tier 1 monitoring and early intervention. Analysts review warning-level activity by category, protocol, or time range to determine whether patterns are stabilizing, degrading, or progressing toward higher risk. Integrated filtering and reporting allow focused analysis without interrupting continuous monitoring, while controlled handoff into ticketing systems ensures escalation remains intentional rather than reactive.

From a standards perspective, this layer reflects mature SOC practices around alert fatigue management and graduated response. By explicitly separating warnings from critical incidents, the platform enforces proportional response, preserves investigative context, and maintains an auditable trail of decisions leading up to escalation. This approach supports both operational efficiency and compliance requirements where justification for response actions must be demonstrable.

Overall, this module acts as a pressure-release mechanism within the SOC workflow, ensuring that potential issues are neither ignored nor prematurely escalated, and that response actions are driven by observed progression rather than isolated signals.