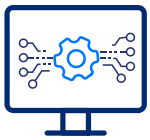
SOLUTIONS BRIEF

The Role of Security Analytics in Powering a Security Operations Platform

ANOMALI

The current state of the cybersecurity market

The cybersecurity industry is arguably the most dynamic, visible, and critical component of the technology sector on a global scale. Multiple, often overlapping challenges hit every sector at every level, and extend from corporate to end-user scenarios. While the potential number of security issues is virtually limitless, the primary concerns revolve around:



DATA OVERLOAD

The volume of security data overwhelms analysts. A large-scale enterprise firewall can generate millions of IOCs (indicators of compromise) per minute, and this number will continue to grow with the acceleration of increasingly sophisticated technology in the wrong hands. In this example, the application of AI-driven analytics would help detect anomalies and surface the highest-priority threats, do it in seconds, and at scale.

ALERT FATIGUE

Working as a security analyst has often been described as a tough, thankless job. The volume of IOCs and IOAs (Indicators of Attack) is staggering, the downside is huge, and most analysts are not experienced enough to filter out random noise from the SIEM to find the signals indicating the problem. The application of AI to drive smart alert grouping and correlation based on risk reduces noise and makes massive data sets manageable to T1 analysts.

SLOW RESPONSE

Most security operations teams are still dependent on manual processes for threat investigation and remediation. The problem is compounded by complex workflows, slow investigations, and a genuine sense of urgency to manage the containment of threats before they begin moving laterally. The creation of automated playbooks can not only accelerate an effective remediation response, it offers stressed-out analysts a huge jump in productivity and effectiveness.

UNKNOWN THREATS

New attack techniques designed to evade rule-based detection are surfacing on a regular cadence at high speed. The application of AI-driven UEBA can uncover novel attack patterns and tactics, particularly when errant user behavior is a risk catalyst.

SKILLS SHORTAGE

Lack of cybersecurity talent makes it hard to monitor environments 24/7. AI augmentation allows small teams to operate at a much greater scale. The use of natural language queries that automatically convert spoken language to Anomali Query Language (or converts from other query languages as well) can let your T1s punch well above their weight and reduce workload stress at the same time.

LIMITED VISIBILITY

Siloed tools offer depth but are not designed for breadth, and understanding cross-functional risk as threats move laterally across your organization can help address the limits created by partial visibility associated with legacy systems. Unified analytics and data aggregation supported by intuitive dashboarding provide complete, contextual monitoring.

COMPLIANCE RISKS

Regulatory and compliance mandates are complex, intentionally opaque, subject to change, and often enforced retroactively. The inability to prove diligence across security data against standards like PCI DSS leads to fines, while short turn-around requirements like SEC Form 8K can put even well-intentioned enterprises at risk. Detailed reporting evidence that can be AI-generated in minutes helps achieve compliance.

TOOL SPRAWL

Security tools are often onboarded in response to a specific threat or to achieve specific goals (compliance mandates, etc.). This often leads to a collection of disjointed security tools that may be very effective at what they do individually but do not play well with other tools, resulting in gaps in coverage, functional redundancies, and high overhead.

COLLABORATION DIFFICULTIES

A lack of a consistent perspective (e.g. tool sprawl) can lead to poor coordination across network, endpoint, and application teams, causing delays, often while the organization is under attack. This is another instance where an intuitive dashboarding capability that correlates across different data sources can take your SecOps game to the
next level.

SKILLSET GAPS

The majority of analysts are relatively fresh out of school and lack the experience and expertise across tools and domains to hunt threats and interpret alerts. AI-enabled query support can address this requirement dead-center, and uplevel the performance of all your analysts while saving you significant time and investment.

COMMUNICATION CHALLENGES

Having your boss's boss ask for detailed information in five minutes (that you know will take hours to find and correlate) can be a stress inducer for anyone. This is another area where AI enablement can summarize a dense, forty-page technical document into an exec-level one-pager, and do so in seconds. Everyone wants to look good in front of their boss, and this capability enables it.

Addressing these workforce, process, and technology issues is critical for improving the efficiency, effectiveness, and reporting of security operations in the face of continued skills scarcity and a complex, evolving threat landscape. So in this scheme, what is needed to help SecOps not only manage but stay comfortably ahead of threats?

Getting and Staying Ahead

NATURAL LANGUAGE SIEM SEARCH

Having analysts run search queries using natural expressions (in literally any language) removes the need to develop proficiency in complex and time-consuming query languages. This is not only a productivity/ease-of-use accelerator, this capability enables T1 analysts to perform at the level of a T3, and sends T3 performance off the charts.

Additional advantages include:

- Flexibility
  Natural language queries allow the flexibility to ask questions and explore data in freeform ways not tightly constrained by predefined rules. This supports and accelerates threat-hunting activities through a more intuitive engagement with system resources.
- Speed
  Natural language and conversational interfaces enable getting query results and findings faster through voice commands or typing compared to using GUI menus and forms. Your analyst is often looking for a needle in a haystack while the barn is on fire. Speed matters.
- Pattern recognition
  Keep in mind you're querying against a massive data set, where critical information can be hidden in patterns too subtle for a human to notice. Natural language processing capabilities can identify query intents, map entities, and suggest similar queries to guide the investigation process.
- Knowledge retention
  Queries expressed conversationally can catalog investigation steps, capture analyst knowledge, and share query logic using transparent natural speech. Building a curated data set based on prior interactions benefits everyone.

INTEGRATED SOAR CAPABILITY

Integrating Threat Intelligence with Security Orchestration, Automation, and Response (SOAR) can significantly amplify the effectiveness of threat detection and response efforts. Ideally, you're looking for a solution that has been not bolted on but instead meticulously built from the ground up, bringing unparalleled automation and efficiency to security operations. This model should be designed to scale with any organization's automation and response needs, allowing the creation and execution of playbook actions via query language syntaxes/natural language, and enabling highly customizable responses to security incidents. Faster and more informed decision-making can be supported by the seamless enrichment of threat data through an integrated TIP/CTI platform and other enrichment actions like VT/Shodan/AbusIPDB. Incident response can be improved by automating ticketing processes, which reduces manual overhead, and ensures tickets are tracked and resolved promptly. Additional benefits should include:

- Prioritized focus
  Playbooks automatically trigger responses for the highest priority threats based on risk ratings from your threat intel. When time is a factor, this ensures operator time is focused on where it matters most.
- Consistent 24/7 response
  Threat intel-enriched playbooks provide a consistent, round-the-clock automated response without relying on analyst availability, driving significant gains in productivity.
- Compliance benefits
  Orchestrated playbooks provide detailed documentation of security response processes for compliance auditors, accelerating response for time-driven mandates like SEC Form 8K requirements.
- Reduced training
  Security analysts can leverage playbooks built by senior staff rather than learn manual response workflows for each toolset.
- Accelerated containment
  Automated isolation of infected hosts via playbooks significantly reduces dwell time for adversaries and accelerates remediation.
- Institutional memory
  Playbooks codify and preserve optimal responses rather than relying on individual analyst knowledge, helping you build a curated corpus.

UI/DASHBOARDING FUNCTION

Through the use of fully customizable dashboards powered by AQL/Natural language, customers can gain a holistic view of their security landscape through dynamic visualization that highlights key metrics and trends. This allows the transformation of raw data into meaningful insights that can immediately identify threats and security vulnerabilities while monitoring compliance. This also fosters improvement in communication and decision-making by allowing the sharing of these customized dashboards among team members and stakeholders. Additional capabilities include:

- Executive reporting
  Dashboards quickly highlight security KPIs, trends, and risks to executives through data visualization.
- Unified visibility
  Disparate security data is seamlessly integrated into dashboards spanning networks, endpoints, clouds, and users, letting you see the entirety of your threat landscape and remediation efforts.
- Continuous monitoring
  Live-updated dashboards provide continuous visibility rather than one-off reporting, keeping you constantly alert to potential incidents.
- Reduced manual effort
  Automated dashboard creation and scheduled distribution can easily replace manual efforts and accelerate productivity.
- Enhanced situational awareness
  Interactive visual analytics augment raw data with human intuition during incidents.

ENDPOINT ANALYTICS

This function provides continuous real-time threat detection through the monitoring of endpoint telemetry for immediate visibility and action on anomalies, reduced dwell time, improved accuracy to minimize false positives and negatives, comprehensive analysis to uncover hidden patterns, and enhanced forensics to aid in post-attack analysis. Next-gen endpoint analytics should also be powered by Machine Learning to assess file hash risks for proactive threat detection while delivering detailed insights into the threat nature and severity beyond binary classification (malicious/not malicious) for incident prioritization. Overall, endpoint analytics enables customers to improve the accuracy of endpoint detections to minimize false positives and perform a comprehensive analysis to uncover hidden patterns within data. Additional capabilities should include:

- Behavioral sandboxing
  Analyze file behavior patterns in isolated sandbox environments to uncover evasive threats missed by static detection.
- Track terabytes of malware signatures to detect nuances that EDR cannot, upleveling existing investments in EDR technology.
- Prioritized alerts
  Machine learning-derived risk scoring to highlight the most critical threats for immediate response.
- Automated containment
  Instantly isolate compromised endpoints to prevent lateral spread and send alerts to other potential at-risk systems.
- Dwell time reduction
  Real-time detection and response can cut average dwell time by over 50% compared to periodic scanning tools.
- Unified views
  Combined endpoint and network analytics can provide correlated insights into attacks as they progress through the kill chain.
- Compliance benefits
  Detailed endpoint activity audit trails can satisfy regulatory compliance requirements, and can do so in a matter of minutes.
- Cloud scale
  The solution should scale seamlessly across tens of thousands of endpoints without performance impact.

NETWORK ANALYTICS

Continuously analyzes flow data to deliver comprehensive insights into network traffic patterns, monitoring and alerting on threats as they happen. The solution should take an "Inside out" approach, rather than focusing solely on external threats. Network analytics also scrutinizes internal traffic to look for hidden threats/lateral movement/zero-day exploits across all network telemetry. Additional capabilities can include:

- Early C2 detection
  Identify initial command and control callouts that precede data exfiltration to avoid malicious activities at the early stages of an attack while significantly reducing dwell time.
- Insider threat detection
  Analyze internal communications to uncover insider policy violations or threats early in the potential threat cycle. This can also enhance protection against social engineering attacks and accidental insider threats.
- Continuous scanning of the Internet for threats to identify bad actors, based on TIP/CTI, allows matching to internal telemetry to indicate which specific actor was involved in the threat or attack.
- Micro-segmentation
  Provide visibility for defining and monitoring micro-segment zones.
- Asset discovery
  Automatically fingerprint OS, devices, and applications across the network.
- Anomaly prioritization
  Rank anomalies based on severity determined by AI algorithms.
- Historical baselining
  Detect changes in traffic patterns compared to established baselines.
- Intuitive visualization
  Interactive network topology maps make it easy to investigate threats.

Applying Artificial Intelligence to Security Operations

Generative AI is in an ideal position to help organizations immediately and comprehensively extend their visibility into cyber threats. These solutions use cybersecurity-specific large language models to understand anomalous activities, with orders of magnitude improvements in speed and accuracy. Working with data from TIP/CTI platforms, an AI solution can train on vast, curated datasets that provide a comprehensive, immediate, and integrated perspective on threat activity, while delivering results with a business-level interpretation of the data for executive and C-Level review.

This type of solution enables immediate prioritized security responses based on detected threats, enhancing the speed and efficiency of incident response from cybersecurity analysts. Incorporating generative AI into a security operations platform significantly accelerates performance across all systems resources. For example, this enables users to search petabytes of data in seconds, as opposed to the current legacy standard of hours or days to run a search - assuming the search doesn't time out.

Generative AI can also be used in event search using query language for generation, ingestion, and summarization. This can include a real-time chat interface with intel-backed responses, a semantic search for related content, and suggestions for next steps. The SOC analyst effectively has sophisticated help available from an AI analyst who is always available. This technology helps analysts save time with summarization capabilities across the platform, supported by real-time chat about intelligence specific to the analyst's organization. Data should be securely stored and transmitted, and should never be used to train AI datasets.

Summary

The cybersecurity ecosystem is arguably the most dynamic within the technology sector and affects nearly every company at every level. The potential downside to a breach or attack is at a minimum inconvenient, or worse expensive, embarrassing, and potentially life-threatening. The range of capabilities available from a next-gen Security Operations Platform, coupled with the speed and scalability delivered by AI enablement makes this a genuine game changer.