Listicle

5 Ways Analysts Can Simplify SecOps

splunk>

Let’s face it: Security *should* be simple. But more often than not, SecOps is disconnected and needlessly complex, involving a patchwork of security tools that are meant to solve only one or two problems. Eventually, analysts end up doing swivel-chair security, constantly toggling between multiple consoles in an attempt to get the job done.

Incidents based on narrowly defined detections can also lead to a high volume of alerts, quickly overwhelming anyone on the frontlines of a security operations center (SOC). As a result, threat detection, investigation, and response (TDIR) becomes much slower and prone to error, creating gaps in the organization’s defenses that attackers can easily exploit.

The good news? Gone are the days of manual response and false positives — security teams can now eliminate analyst grunt work, resolve high-value incidents, and lock down their security practice without breaking a sweat.

Below, we dive into five key ways security analysts can take their security practice to the next level (and their overtime hours down a peg):

1. **Gain comprehensive visibility into your organization’s cloud, hybrid, and on-prem environments.**
2. **Learn how to quickly prioritize and triage alerts.**
3. **Leverage relevant threat intelligence for escalation and remediation.**
4. **Stay ahead of the latest threats with out-of-the-box content.**
5. **Establish standardized operating procedures and have a response plan at the ready.**

1. Gain comprehensive visibility into your organization's cloud, hybrid, and on-prem environments.

In the age of remote work and dizzying, large-scale migrations, organizations are swiftly adopting cloud and multi-cloud solutions as part of their infrastructure.

As security teams sprint ahead with a flurry of digital initiatives, analysts need to pay close attention to security requirements and the technical complexities of cloud migration. The journey to cloud nativity (and the attack surface that comes with it) presents a big risk to the enterprise — especially when network controls, access management systems, or cloud configurations are woefully out-of-date.

Without full visibility across the entire enterprise — including cloud and hybrid environments — analysts are at risk of flying blind. Security teams may be unable to see the full breadth of an incident, making detecting and remediating existing threats even more challenging.

No data set is an island

With data dispersed across so many sources, analysts are unable to correlate or contextualize different pieces of information for more accurate threat detection. Organizations need a single platform to transform raw data from any source into actionable insight, so they can capture and analyze relevant log data — regardless of volume, variety, and velocity.

When tools and data are unified within a single work surface, security teams can see the big picture, assess risk, and provide context for the organization's security posture. Better yet, by monitoring multiple cloud deployments, security teams can achieve full visibility into cloud and multi-cloud services (including Amazon Web Services, Azure, and Google Cloud Platform) and all the actionable insights that come with them.

A SIEM by any other name

None of this would be possible without a modern security incident and event management (SIEM) solution, which allows analysts to ingest data from an infinite number of sources, across all types of environments, so they can better detect the where and why of security events.

Traditional SIEMs simply won't cut it. Analyst jobs will be a lot easier with a single security monitoring solution that bridges data across the enterprise — including all nodes, transactions, and users — as organizations transition to the cloud and continue to traverse hybrid environments. At the end of the day, full visibility is critical to the success of any security strategy — and, more aptly, any successful security analyst.

Cheat sheet for comprehensive visibility

Challenge(s): Cloud complexity; an expanding attack surface; siloed and fragmented data across disparate tools/environments; integration.

Need(s): A single, unified work surface; the ability to seamlessly search data no matter where it resides.

Solution(s): Data collection and normalization at scale; continuous monitoring of events from one centralized location across environments; integrated threat intelligence to provide timely context across the attack surface; high-level dashboards and visualizations.

Product(s): Splunk Enterprise Security

Feature(s): Mission Control unifies workflows and offers comprehensive visibility across detection, investigation, and response.

2. Learn how to quickly prioritize and triage alerts.

Security is a data problem

Security analysts are overwhelmed by zettabytes of data, constantly sifting through a wealth of information that can make it virtually impossible to correlate one event with another.

To expand or reduce the scope of their analysis (which is nothing if not vast), analysts need to apply filters to a sea of log data, then place events, actions, and annotations into a timeline to see everything that's going on. But this methodology can only get them so far when dealing with swathes of data and alerts. That's where risk scoring comes in.

You miss all the risk attributions you don't make

Targeted attack detection and risk scoring make it much easier for analysts to isolate and investigate an incident when dealing with a high volume of data. Threat intelligence, behavior profiling, and advanced analytics can improve detection success so that security teams don't have to sift through data to detect and alert on events.

Since security events have different levels of urgency attached to them, potential threats are identified and prioritized via dashboards, then assigned to analysts for review. By prioritizing threats according to their risk level, security teams can maximize their coverage and reliably detect advanced attacks by making sense of "weak" signals (in other words, alerts that would most likely be a false positive). Triaging notable events based on the fidelity of the threat makes the remediation process more reliable and equips analysts with contextual awareness to help determine next steps.

Risk attribution can also help optimize threat hunting while surfacing more sophisticated threats, like low and slow attacks that most correlation searches traditionally miss. With this type of profiling, teams and resources are freed up to focus on complex, high-fidelity threats while aligning operations to industry-standard cybersecurity frameworks (including MITRE ATT&CK, the NIST framework, and more).

A SIEMple solution

Analysts need a strong incident investigation and forensics strategy powered by a modern SIEM. Risk-based alerting (RBA) has become increasingly critical for highly-advanced services. Security teams can make better decisions and gather forensic evidence with the comprehensive collaboration and reporting capabilities integral to any investigation.

Bottom line: Freeing up your analysts to focus on high-value tasks means they're better positioned to respond quickly and efficiently in the event of a security breach — and who wouldn't want that?

Cheat sheet for alert triage

Challenge(s): Alert fatigue; SecOps and threat complexity; lack of orchestration; manual workflows; scalability.

Need(s): Follow and analyze complex attack chains to eliminate cumbersome manual investigation workflows; transform overwhelming numbers of alerts into high-fidelity notables prioritized by organizational risk.

Solution(s): Enhanced detection capabilities; automated threat analysis; completely integrated workflow; risk-based alerting.

Product(s): Splunk Enterprise Security, Splunk Attack Analyzer, Splunk SOAR

Feature(s):

- Risk-Based Alerting to reduce and prioritize the number of overall alerts.
- Pre-built and customizable playbooks for a multitude of use cases.

3. Leverage relevant threat intelligence for escalation and remediation.

Threat intelligence lends much-needed context to even the most nebulous of threats, playing a big part in understanding anomalous behavior before serious (or additional) damage is done.

There are a few different types of intelligence at play — including strategic, technical, and operational — which are collected from external and internal sources. Once the threat intelligence is aggregated into a single location, the data is evaluated to determine which pieces of data are important in the decision-making process.

A single source of truth

On any given day, analysts have to jump between a number of point products (e.g., endpoint protection, antivirus, firewall) in order to understand how different pieces of information are connected. Even with the help of threat intelligence feeds, there can be an overwhelming amount of indicators of compromise (IOCs) that are impossible to track down manually. With a myriad of disconnected tools — in addition to varying data structures and formats — leveraging the necessary intelligence can be tedious and time-consuming, especially when security teams are short on time.

Even with a security analytics solution on hand, one of the biggest challenges organizations will face is maintaining and evolving their security program's rules to better detect and respond to evolving threats. Today's organizations need and expect a SIEM that's not merely a handful of tools, but an integrated ecosystem with broad and deep capabilities to satisfy multiple security and business use cases in diverse environments.

Reduce time to investigate with integrated intelligence

Thanks to Threat Intelligence Management, security teams can integrate and automate intelligence into every stage of the incident response process. Intelligence management brings together a rapidly growing intelligence marketplace — featuring all types of open, commercial, and community intelligence sources — to users everywhere, so they can create complex pipelines without ever having to worry about writing or maintaining scripts.

This allows security teams to manage security events and threat intelligence feeds within one common work surface, synthesizing intelligence into a single, normalized view. This ensures actionable insight into a far-flung ecosystem of teams, tools, and partners — ultimately minimizing mean time to resolution (MTTR) and dwell times by surfacing events within a single console — empowering analysts to conduct a full investigation with a centralized, high-priority view into security events at just the right time.

Cheat sheet for threat intelligence

Challenge(s): Lack of context; data overload; correlating relevant security events

Need(s): Workflows that automatically aggregate findings based on predetermined rules against common security grouping techniques and calculations (including similar entities, cumulative risk score, MITRE ATT&CK thresholds, and more).

Solution(s): An aggregate view shows all related high-fidelity findings in one click — further simplifying the analyst experience to take action and respond to sophisticated threats

Product(s): Splunk Enterprise Security

Feature(s):

- Threat Intelligence Management for context and embedded intelligence.
- Risk-Based Alerting to surface high-fidelity intelligence for action.
- Mission Control simplifies security workflows with integrated, unified intelligence.

4. Stay ahead of the latest threats with out-of-the-box content.

Out-of-the-box (OOTB) security content helps security teams realize value right out of the gate with pre-built dashboards, reports, incident response workflows, correlation searches, and security indicators. This type of relevant, ready-to-use content helps analysts quickly understand and detect threats within their environment, execute best practices for investigations, and automate their response based on recommended guidance.

Rubber, meet road

Security teams often struggle to establish and expand security coverage while maintaining existing detections in the face of an ever-changing threat landscape. The average security manager is expected to configure dashboards, rules, and searches to detect IOCs threatening their environment. This takes a lot of time, effort, and expertise to do from scratch, and it takes analysts away from meaningful threat detection and response work — risking longer dwell times and a greater chance that threat actors can cause harm before they're discovered.

In contrast, out-of-the-box security content helps security teams spend less time developing security content, so analysts can spend more time investigating and responding to actual threats, monitor ongoing tactics, as well as techniques, and procedures (TTPs). Once these signs are detected, analysts can apply relevant searches or playbooks to determine whether to investigate further or how to respond. Periodic, automated updates to OOTB security content also takes this approach one step further, with a dedicated threat research team testing and improving detections on the SIEM's backend, ultimately protecting users against the latest and greatest attacks.

Analyze this

Nowadays, analysts have a host of resources like the Splunk Use Case Library — a handy tool for discovering new use cases based on data ingested, which can be used within your environment — or analytic stories — a collection of searches grouped together around a common theme that includes narrative background, correlation searches, behavior models, and automated playbooks. Out-of-the-box cloud security monitoring content can also make it easier to detect and respond to threats across hybrid, cloud and multi-cloud environments, thanks to sophisticated detection rules.

Together, these powerful components help analysts detect, investigate, and respond to signs of threats in their environment before it's too late

Cheat sheet for out-of-the-box content

Challenge(s): Expanding security coverage; managing detections; manual work maintaining and tracking updates; out-of-date content

Need(s): Native, automatic version control; quantified risk and coverage

Solution(s): Real-time updates provide the latest security content; out-of-the-box detections built by industry experts

Product(s): Splunk Enterprise Security

Feature(s): Analytic Stories and Enterprise Security Content Updates for comprehensive threat detection and a layer of industry and product expertise.

5. Establish standardized operating procedures and have a response plan at the ready.

Standardized operating procedures are no longer a “nice-to-have” but a “must-have” for SOC analysts. Without documentation or a formalized process, inconsistencies are bound to occur, ranging from a misalignment in terminology to a lack of consensus around what alerts get prioritized and why. Team members may execute different actions at different levels of urgency, or even skip certain actions from the jump, negatively impacting an organization’s security posture. Additionally, the level of experience and familiarity with some SOC processes and procedures can differ considerably between a junior analyst versus a senior one, which is why performance measurement is so critical to the SOC.

The nirvana solution

Security teams looking to streamline processes and increase productivity can lay the groundwork with standard operating procedures (SOPs). An SOP is a process that can be operationalized and optimized for repetition, with the end goal to help team members work faster and more efficiently by avoiding the duplication and tedium of manual and repetitive processes and tasks. These processes help security teams reduce dwell time while ensuring consistent quality control and compliance across the board. SOPs can also establish baseline performance and service-level agreements for carrying out certain protocols.

With a clear list of steps to follow and playbooks to implement, it becomes that much easier for an analyst to thwart an attack, no matter how advanced. Response plans also allow analysts to templatize and execute on the SOPs in question, as well as collaborate across incident response workflows for common security use cases. These templates look at each stage of an incident response plan, assign key stakeholders to specific phases, and apply simple automation playbooks in order to expedite the entire process and improve the workflow.

Data from response templates allows analysts to measure everything top-to-bottom in the incident response workflow, and helps with SOC management and guidance on where to apply automation. Pre-built templates can also be used for security use cases and help teams to achieve repeatable and reliable security operations.

Cheat sheet for standard operating procedures

Challenge(s): Inefficient, manual playbooks for specific customers and use cases; misalignment in terminology between different components of the security ecosystem

Need(s): Automate repetitive tasks and implement automated response actions; orchestrate complex workflows across tools/automate security operations; streamline and standardize workflows; alignment to OCSF and other frameworks

Solution(s): Increase productivity and operational efficiencies for overwhelmed and understaffed security teams with automation and orchestration.

Product(s): Splunk Enterprise Security, Splunk SOAR

Feature(s):

- Pre-built and customizable playbooks for a multitude of use cases.
- Apps to help orchestrate and integrate all of the security tools in your stack.
- Case management tools to help ensure a cohesive and collaborative investigation.
- Event management options to help consolidate large volumes of security events.

Got questions?
We’ve got answers!

Contact us

splunk>

24.CMP.Listicle.5-ways-analysts-can-simplify-secops_v5