SPONSORED CONTENT

CSO
FROM IDG

single point of contact

CLOSING THE CYBER SECURITY GAP

3 KEYS TO ANALYTICS-DRIVEN SECURITY

splunk>

Listen to your data.®

IDG Communications, Inc.

AS TECHNOLOGIES MORPH AND GROW MORE CAPABLE,

the threat landscape evolves and increases in size. Cyber thieves are constantly trying new techniques and methods for exploiting humans and devices. Their goal: identify vulnerabilities that provide access to mission-critical data and systems. Potential targets include credit card data, healthcare records, employee data and more that can be sold on the dark web, encrypted and held for ransom, or used to disable critical systems.

Detecting and responding to these threats consumes an increasing number of resources for CSOs and security professionals. According to the 2018 Security Priorities study from IDG, 28% of IT professionals and leaders say that external cyber threats force them to redirect time and focus away from more strategic tasks. External threats rank second only to compliance, as reported by 32% of respondents.

Although the study showed that insider threats represent less of a concern overall (16% of respondents named it as a major concern), security professionals ought to still address it, as indicated by recent research.

The 2018 Global State of Information Security Survey (GSISS), conducted by PwC, CIO and CSO, shows that sources of security incidents are spread across mobile devices, consumer technology in the workplace and operational systems such as industrial controls or plant-floor equipment. And employees and business partners are just as likely to cause these incidents as are unknown hackers or nation states.

What's more, organizations with offices in dispersed locations, including different countries, face additional challenges in making sense of incident data spread across operations centers, regions or time zones.

The Talent Gap

With such a rapidly evolving security landscape, every business needs a security team that can leverage statistical, visual, behavioral and exploratory analytics to drive insights, decisions and actions.

But there's a problem: the ongoing security talent gap.

A quick look at the state of the nation tells the story: the average number of open positions at organizations across major industries is 3.4, according to IDG's 2018 Security Priorities study. And the need only continues to grow. More than a third (37%) of organizations will add full-time employees for security functions in the next 12 months. And more than a quarter (26%) will bring in outsourced or contract employees in an effort to fill the gap.

Overall, 3.5 million cybersecurity positions will be unfilled by 2021, predicts Cybersecurity Ventures.

Even organizations that do manage to fill open security positions will likely have to contend with entry-level talent trying to step into the bigger shoes of more senior-level professionals. In other words, there aren't enough seasoned security experts to go around.

Even now, small security teams all too often face an avalanche of alerts from an array of tools without the resources to sift through the noise. Is that alert about a predawn login the result of a hacker attempting to gain entry to a corporate network, or just an employee getting an early start to the work day? What alerts, among thousands or even millions of such notifications, constitute legitimate threats? Teams searching for these needles in haystacks are increasingly hard-pressed to keep up.

3.5
MILLION
CYBERSECURITY POSITIONS WILL BE UNFILLED BY 2021, PREDICTS CYBERSECURITY VENTURES.

What's needed is a way for organizations to stay ahead of security issues by detecting threats, then quickly identifying and investigating malicious activities to execute responses — all with limited resources. Three keys to success point the way forward.

1: Centralize Data

Step one on the path to closing the security gap involves mapping what's there and what's happening across an organization's IT landscape. That means taking inventory of every source of data across the enterprise stack.

AT FIRST GLANCE UNSTRUCTURED DATA MIGHT NOT SEEM RELEVANT TO SECURITY, BUT, JUST AS WITH ANY OTHER TYPE OF DATA, IT MAY ILLUMINATE A POTENTIAL ENTRY POINT FOR HACKERS AND AUTOMATED SYSTEMS DESIGNED TO COMPROMISE NETWORKS.

It's a common complaint: data in silos — data in disparate databases and on different systems, both on premises and in the cloud, challenges visibility.

Ingesting data from all devices and systems across the enterprise in a centralized data platform, on the other hand, can foster situational awareness and lay the groundwork for taking the next step. That's because access to all data and data sources provides the most context for quickly discovering and stopping threats.

This involves not just structured data in conventionally machine-readable form and found in monitoring systems, for example. It also includes unstructured data such as customer feedback and textual comments from employees, found in emails, PDFs or other documents. At first glance, unstructured data might not seem relevant to security, but, just as with any other type of data, it may illuminate a potential entry point for hackers and automated systems designed to compromise networks. For that reason, all data remains relevant to the overall security mission.

Security information and event management (SIEM) solutions can provide the necessary access to insights from data across disparate systems; thanks to customizable dashboards, visualizations and alerts, this data is presented in an easy-to-read form. Best-in-class SIEM solutions can understand any data source, and, more importantly, filter it and make it available to security teams to derive valuable insights.

In a broadly recognized best practice, more than two-thirds (68%) of organizations have deployed or plan to roll out SIEM technology in the year ahead, according to the GSISS.

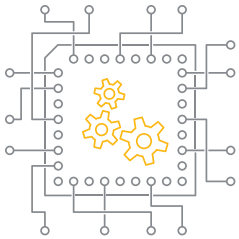
With a centralized view of data, security teams can next take action based on responding appropriately to alerts from across the enterprise IT stack. For this step, automation provides the leverage IT teams need to stay on top of alerts while also remaining responsive to emerging threats.

2: Automate and Orchestrate

The challenge here is making sense of an avalanche of data. It's not enough simply to visualize it; organizations also need to know what it means.

However, given the mountain of data that must be sorted to identify potential threats, it's not feasible to rely on human analysts alone. Investigating a single alert might take a team member 45 minutes or more to pursue and prioritize.

Automation allows teams to deploy repeatable processes that would otherwise require a larger staff to perform manually. Machine learning (ML) capabilities in particular can turbo-charge the ability to detect previously unknown threats or make sense of anomalies by discovering patterns across volumes of data that are too large for human analysts to tackle by themselves.



AUTOMATION BECOMES A VIRTUAL ANALYST, PROVIDING DEEP VISIBILITY WHILE FREEING UP KNOWLEDGE SECURITY WORKERS TO FOCUS ON HIGHER-LEVEL TASKS.

Automation can automatically identify which of hundreds of anomalies across multiple entities, including users, accounts, devices and applications, constitute legitimate threats requiring faster action.

These data-driven tools provide a variety of benefits, from improving security teams' understanding of external and internal threats to offering better visibility into anomalous network activity. They can also reduce that 45-minute investigation time to as little as thirty seconds.

The idea is not to replace an already limited number of IT staff members, but to augment their abilities by presenting them with a more intelligent and easier to visualize set of alerts that evolve in response to incidents.

Orchestration — tying together data, processes, and disparate systems to streamline the security workflow from detection all the way through remediation — also helps augment the abilities of IT teams. Orchestration tools help leverage repeatable processes to connect other tools to each other and keep data and processes in sync. By freeing security professionals up from having to make and maintain those connections themselves, orchestration allows teams to focus on more critical tasks.

In a nutshell, automation hardens defenses by reducing the number of unattended security alerts. In effect, automation becomes a virtual analyst, providing deep visibility while freeing up knowledge security workers to focus on higher-level tasks.

3: Integrate and Optimize

Optimizing IT security means coordinating the efforts of day-to-day IT operations and development with security. Three-quarters (75%) of respondents to IDG's 2018 Security Priorities study report that their organizations manage IT and security together, fostering tighter coordination and enabling IT to operate with an appropriate level of security awareness.

More than half of IT organizations (54%) say that tightly integrated IT security represents an integral part of their overall IT strategy. That's up from 37% just two years ago, according to the Security Priorities study. What's more, 82% of IT leaders expect their organizations' IT and security strategies to be tightly integrated within three years, according to the State of the CIO 2018 survey from IDG.

Key to achieving the kind of high-level integration between IT and security? Optimizing security processes.

This means operationalizing the results of security analysis to update systems and share learnings internally or externally. Security automation tools can aid this effort by allowing teams to incorporate insights from incidents and responses into repeatable processes that run in response to future incidents. This ensures immediate action the next time a similar incident occurs.

These tools also help surface relevant alerts, and suggest, rather than perform, potentially sensitive actions such as deleting files or blocking users and access points. This capability further aids IT teams by helping more junior members perform at a higher level. Team members can execute actions suggested by the tools (after verifying their appropriateness).

Taking the 3-Step Approach for Real Bottom-Line Impact

A major financial services company leveraged centralization, automation and optimization to help a small security staff get on top of data from billions of credit card transactions across multiple systems.

Corralling data from across the enterprise, staff members saw, for the first time, that their separate security systems blocked a total of 400,000 attempted port intrusions every four hours. They also saw that over a month's time, their systems prevented 16,000 pieces of malware from penetrating their networks.

Automation and optimization now allows the team to correlate data from across the IT stack to develop intelligence about incidents and coordinate the appropriate response. Data even identifies the geographical location of incoming exploits and malware, letting the team prioritize security events according to where or through what assets they originate.

In another example, one large city government centralized data from across 40 agencies with a combined workforce of 30,000 employees. Together, these agencies handle about a million incidents every single day. Left on their own, each agency would miss the significance of many of these incidents.

Thanks to automation and orchestration across their individual data sources, they have coordinated their incident detection and response systems and processes. That way, when one agency gets hit with an incident, the others can learn from it — in turn optimizing their defenses and blocking similar attacks on their own systems.

In other words, optimization lets organizations maximize their limited number of senior security staff members by augmenting the abilities of more junior-level team members. At the same time, those junior security pros, freed from repetitive tasks by automation, can concentrate on higher-level tasks that help them grow into more seasoned professionals.

Optimization is the final step in closing the security gap, providing new intelligence, spotlighting threats and catching more incidents.

Putting It All Together

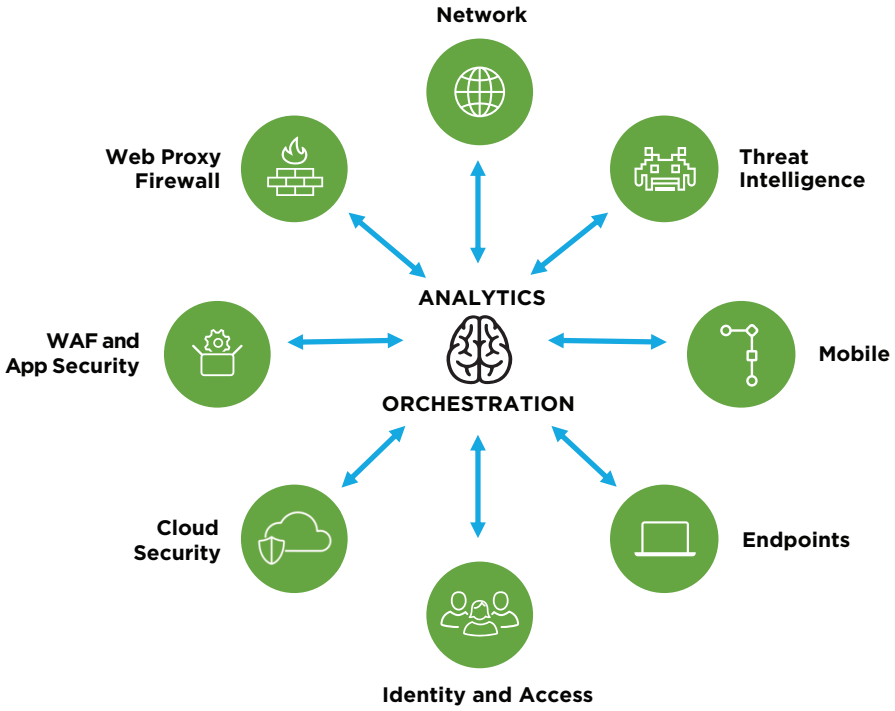
Armed with the 3-step process of 1) centralizing data, 2) automating and orchestrating, and 3) integrating and optimizing, organizations can continue running their IT departments and innovating for the future while at the same time handling the increasing workload around security operations.

Using analytics and machine learning to gain context for data across the enterprise allows resource-constrained IT security teams to augment their human knowledge and expertise. When adding automation and orchestration technologies to the mix, organizations can optimize security processes, enabling them to close the security gap and get on with the work of building better products and services for their customers.

Improve Your Security Posture With Splunk

Splunk as Your Security Nerve Center

Legacy approaches to IT operations' tasks and processes are slow, inefficient and often result in siloed data and insights, costing the business time and money. By marrying machine data with machine learning, Splunk delivers a modern approach to bring data-driven decisions easily to modern IT organizations. With Splunk, your teams are empowered to predict and prevent issues from arising and quickly resolve operational disruptions in real time. You can move seamlessly from business service reports to infrastructure and application layer investigation and remediation. The result? Overarching visibility into your services and the ability for your organization to operate with agility.



By using Splunk, you can turn your security data into insights and action, drastically improving your operational efficiency. Our solutions work together toward a common goal of reducing the time delta between identifying a threat and its remediation.

Benefits of Analytics-Driven Security

DETECT, INVESTIGATE AND RESPOND TO INCIDENTS FASTER

Splunk streamlines data aggregation, advanced threat detection, investigation, orchestration and response capabilities with best-of-breed technologies that optimize the entire security workflow. By ingesting, centralizing and understanding data from nearly any source, and applying advanced analytics and machine learning to it, Splunk casts the widest of nets to detect known and unknown threats faster and with superior precision. Automation then accelerates investigation and response workflows, by taking intelligent action against detected threats and incidents in seconds instead of hours.

MANAGE YOUR RISK

Every second a threat remains undetected or unattended increases your exposure to risk and widens your attack surface. This leaves your organization vulnerable to greater risk, compounding from any incident that left you vulnerable in the first place. Splunk helps you close this gap with advanced threat detection capabilities that give you greater visibility into risk, incidents and threats. And by leveraging programmed response playbooks, alerts are immediately investigated, triaged and acted on — allowing your security operations to run 24/7 and limiting risk across the enterprise.

AUGMENT YOUR SECURITY RESOURCES

Security teams are overwhelmed by the volume of alerts they need to investigate, the growing complexity of incidents and the advanced tactics deployed by today's hackers. Splunk helps security teams scale with proven technologies that operate with varying levels of autonomy, replacing tedious and repetitive tasks with intelligent workflows. From learning from your enterprise activity and drawing baselines to automatically detect anomalies that may indicate possible threats, to streamlining orchestrated responses across complex security stacks — security teams increase their productivity and augment their performance with Splunk's security solutions.