Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

The Rise of Cloud-Based Security Analytics and Operations Technologies

Jon Oltsik,
Senior Principal Analyst and ESG Fellow

October 2019

Contents

Back to Contents

Research Objectives

Security analytics and operations can be complex, requiring highly skilled professionals and detailed processes. To overcome these issues, security teams tend to deploy an array of security analytics tools and technologies to collect, process, analyze, and act upon growing volumes of security telemetry. Despite this investment, however, many organizations continue to find it difficult to manage cyber risk or detect and respond to cyber incidents.

How can CISOs address these issues and develop effective security analytics and operations processes? In order to get more insight into these trends, ESG surveyed 406 IT and cybersecurity professionals at organizations in North America (U.S. and Canada) involved with the planning, implementation, and/or operations of their organization's information security policies, processes (including purchase decisions), or technical safeguards and familiar with their organization's collection and/or analysis of security data in support of information security management strategy. This study sought to:

Determine current strategies used for security analytics and operations.

Identify how security analytics and operations challenges are affecting organizations' ability to monitor cyber risks and detect/respond to cyber-attacks

Understand the impact of using public cloud resources for processing and storing data on security analytics and operations technology decisions.

Uncover future enterprise security analytics and operations strategies and plans.

Back to Contents

Executive Summary

External changes and internal inefficiencies make security analytics and operations difficult.
Security professionals find it challenging to keep up with the cyber-threat landscape and the growing IT attack surface driven by initiatives like cloud computing, digital transformation, and IoT. At the same time, security operations centers (SOCs) struggle with disconnected point tools, manual processes, and a global cybersecurity skills shortage.

The security data pipeline continues to grow in volume and complexity.
Nearly one-third of organizations collect substantially more data to support cybersecurity analytics and operations today than they did 2 years ago, while more than half are retaining data online for longer periods of time than in the past.

Evolving from SIEM to SOAPA.
Seventy percent of organizations have a security event and information management (SIEM) system in place, and use SIEM for monitoring the security of cloud-based workloads, detecting known cyber-attacks, and producing reports for regulatory compliance.

Staffing and skills shortages lead inevitably to managed services.
Three-quarters of respondents agree that the cybersecurity skills shortage has impacted their organization's security analytics and operations effectiveness and 70% say it is difficult to recruit and hire additional SOC staff.

SOCs will have a "cloudy" future.
Many organizations are moving on from on-premises security analytics and operations technologies, as more than half now prefer cloud-based security analytics/operations solutions or would consider cloud-based security analytics/operations solutions on a case-by-case basis. Some will "lift and shift" on-premises tools to the cloud, some will replace on-premises tools with cloud-based alternatives, and some will supplement on-premises SOC technologies with additional cloud-based tools.

Organizations are incorporating machine learning and automation/orchestration into their technology plans.
More than half of organizations are adopting technologies featuring security analytics machine learning algorithms while nearly two-thirds are utilizing new technologies for process automation/orchestration.

Back to Contents

External changes and internal inefficiencies make security analytics and operations difficult.

ORGANIZATION'S PRIMARY CHALLENGES REGARDING SECURITY ANALYTICS AND OPERATIONS

27%
Monitoring security across a growing attack surface

23%
Keeping up with the volume of security alerts

22%
The cybersecurity team at my organization spends most of its time addressing high priority/emergency issues and not enough time on strategy and process improvement

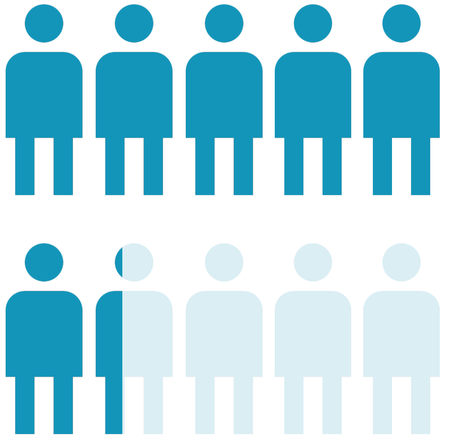
22%
Detecting/responding to security incidents

The security operations landscape is growing in complexity.

Unfortunately, meeting these objectives is challenging, as 63% of respondents claim that security analytics/operations is more difficult today than two years ago. Why? Because security analytics and operations are fraught with numerous challenges like monitoring the growing attack surface, keeping up with the volume of security alerts, addressing emergencies, and detecting/responding to security incidents.

Given these issues, many organizations cannot mitigate risk, defend critical assets, or remediate problems at an appropriate level.

LEVEL OF COMPLEXITY FOR SECURITY ANALYTICS & OPERATIONS COMPARED TO 2 YEARS AGO



More difficult compared to 2 years ago,

63%

Back to Contents

“These objectives are **essential** to counteract a dynamic threat landscape…”

There is plenty of room to improve security analytics and operations.

Organizations want to make security operations progress in areas like operationalization of threat intelligence, data enrichment, and improvement of the data pipeline for real-time security analytics. These objectives are essential to counteract a dynamic threat landscape and address the growing volume of data collected, processed, analyzed, and acted upon as part of SecOps.

ORGANIZATION’S PRIMARY OBJECTIVES REGARDING SECURITY ANALYTICS AND OPERATIONS

40%

Improve our ability to discover, prioritize, and remediate software vulnerabilities

38%

Improve the operationalization of external threat intelligence

38%

Improve the management of our data pipeline to provide more real-time data for security analysis

37%

Improve our ability to combine and enrich multiple security data sources to provide more context around security events

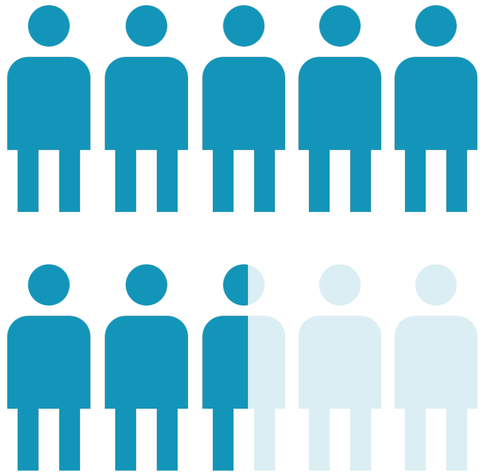
36%

Improve cyber-risk identification and communications with business and executive management

Back to Contents

Organizations are collecting more security data, and retaining it for longer.

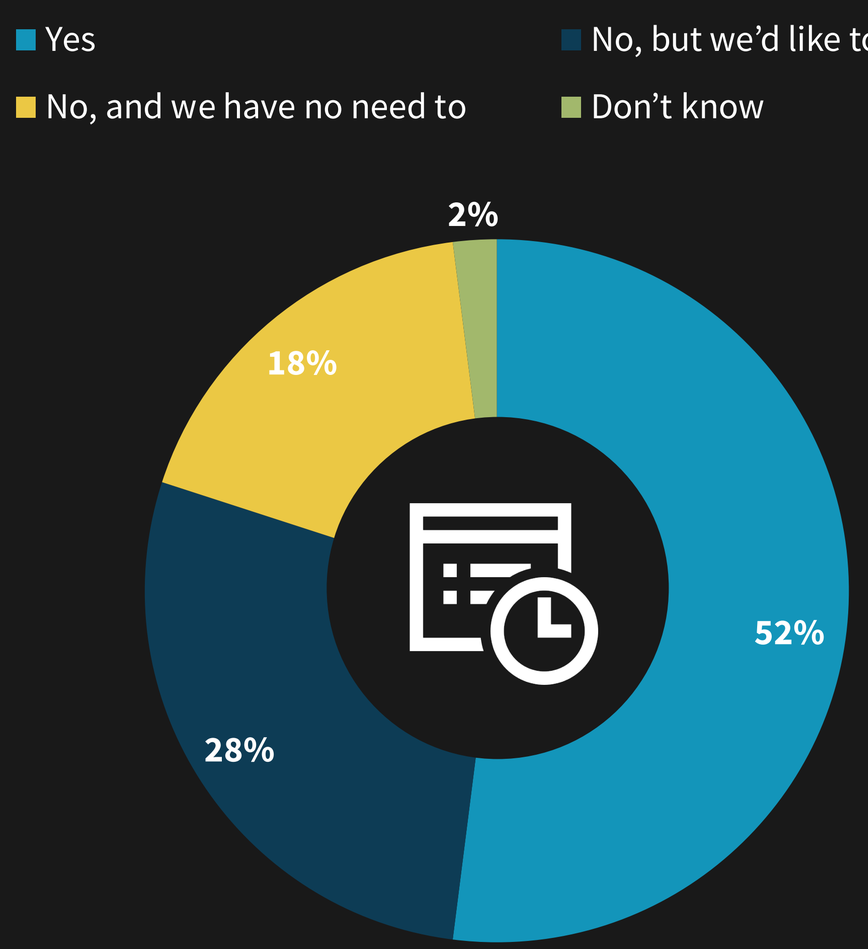
Security analytics and operations depend upon collecting, processing, analyzing, and acting upon growing volumes of diverse security data sources. In fact, nearly one-third (32%) of organizations collect substantially more data to support cybersecurity analytics and operations than 2 years ago, while another 44% collect somewhat more data. Additionally, 52% of organizations retain security data for longer periods of time than they did in the past.



We collect more security data than we did 2 years ago,

76%

ARE ORGANIZATIONS RETAINING SECURITY DATA FOR LONGER PERIODS OF TIME?



Back to Contents

MOST IMPORTANT DATA TYPES USED FOR SECURITY ANALYTICS/OPERATIONS

33%
Security data from endpoints

31%
Web security data

28%
Threat intelligence feeds

26%
Email security data

25%
Log data from security devices

"Based upon ESG research, it appears that the **focus is on incident detection.**"

Wide range of important security telemetry.

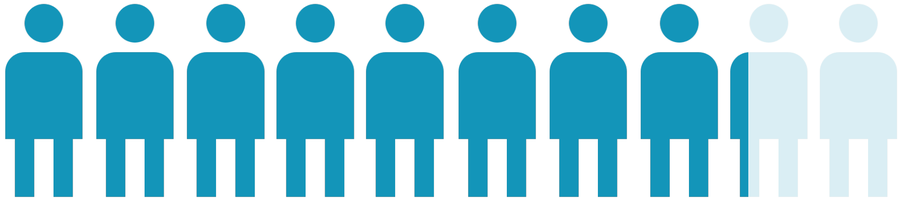
Which data sources are most important for security analytics/operations? Based upon ESG research, it appears that the focus is on incident detection. Survey respondents pointed toward security from endpoints (i.e., compromised systems), web and email security data (i.e., common threat vectors), threat intelligence feeds (i.e., to compare internal alerts with security data "in the wild"), and log data from security devices (i.e., network perimeter firewalls, IDS/IPS, proxies, etc.). Other data like DNS, identity, and directory logs are likely used as part of investigations.

Back to Contents

Evolving from SIEM to SOAPA.

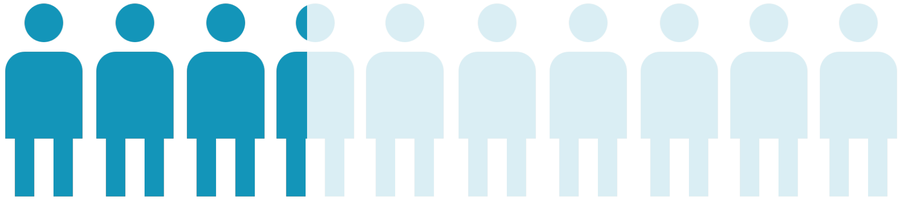
SIEM is on a collision course with cloud services.

Eighty-two percent of organizations are committed to moving large volumes of workloads and applications to the public cloud. This increases the attack surface and introduces new oversight and skills requirements in the SOC. Clearly, this is why 33% of respondents claim that SIEM systems are now used for security monitoring, reporting, and analysis of workloads running in the public cloud.



82%

of organizations are committed to moving large volumes of workloads and applications to the public cloud.



33%

of respondents claim that SIEM systems are now used for security monitoring, reporting, and analysis of workloads running in the public cloud.

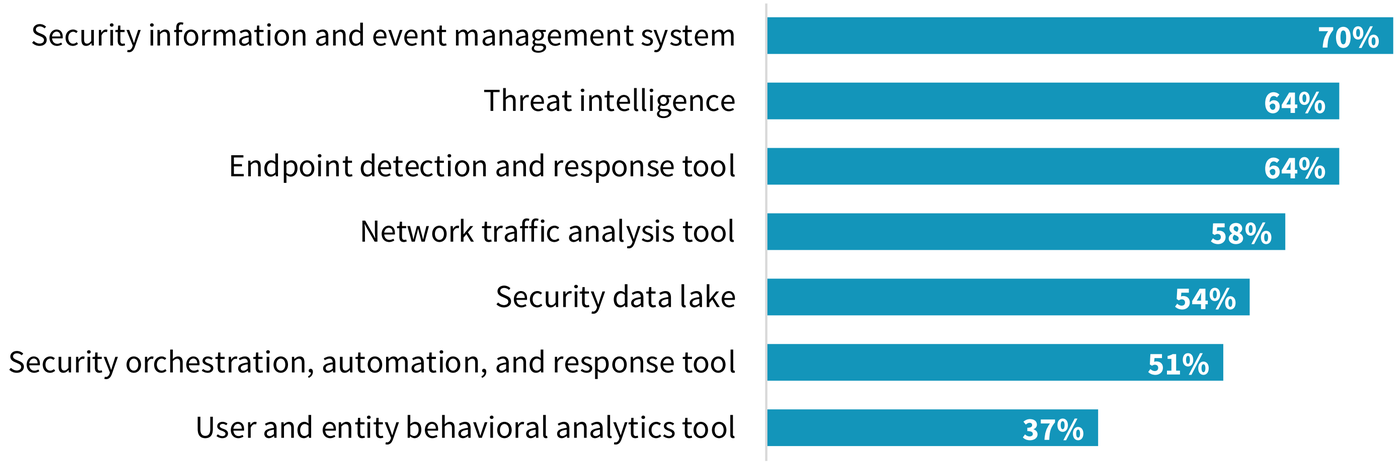
Back to Contents

SIEM leads a disparate collection of security analytics tools, but there is an appetite for integration.

Seventy-percent of organizations use SIEM today as well as an assortment of other security technologies like threat intelligence feeds/analytics, EDR, and network traffic analysis tools. While each tool provides valuable data analysis, it is difficult for the SOC team to piece together a holistic view of enterprise security across an assortment of disconnected point tools.

To overcome this limitation, 36% of organizations are very active regarding integrating security tools into a common security analytics and operations platform architecture (SOAPA), while 48% are somewhat active in this area. CISOs want unified SOAPA to help them improve SOC efficacy and efficiency.

SECURITY ANALYTICS AND OPERATIONS TOOLS DEPLOYED



EFFORTS TO INTEGRATE DISPARATE SECURITY ANALYTICS AND OPERATIONS TOOLS

36%

Very active, this is one of our highest priorities

48%

Somewhat active, this is important but not one of our highest priorities

Back to Contents

“SIEM is often seen as a **Swiss Army knife for a variety of use cases.**”

SIEM value and challenges.

SIEM can be a valuable security operations asset but it does have its limitations. For example, SIEM is especially useful for detecting certain types of known incidents using correlation rules, and is often seen as a Swiss Army knife for a variety of use cases, including security and regulatory compliance reporting.

TOP 5 MOST VALUABLE ATTRIBUTES OF SIEM

28%
SIEM can be used to detect specific types of security incidents

28%
SIEM can be used for security analytics and regulatory compliance reporting

24%
SIEM can be used for different security analytics and operations use cases

23%
The SIEM can scale to provide visibility into all the event data across our organization

22%
SIEM acts as an integration platform for other security applications

TOP 5 MOST CHALLENGING ATTRIBUTES OF SIEM

23%
SIEM requires lots of personnel training and experience to attain maximum value

22%
SIEM is good for detecting known threats but not as effective for detecting unknown threats

21%
Junior people tend to struggle doing anything more than looking at basic dashboards

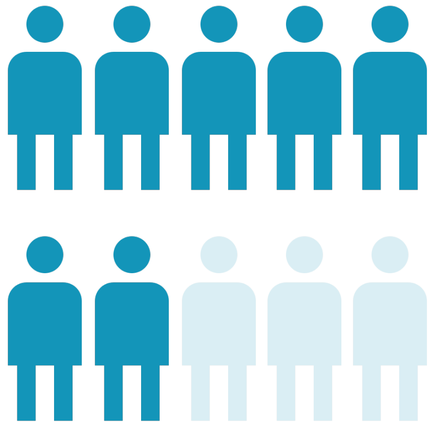
21%
SIEM is not well suited for certain use cases

21%
SIEM requires constant rule creation and tuning

Back to Contents

Profound impact of the cybersecurity skills shortage drives increased use of managed services in the SOC.

Three-quarters of organizations claim that the global cybersecurity skills shortage has impacted their security analytics and operations performance. So, why not just hire additional SOC staff? It's not that easy—70% of security organizations say that it is extremely or somewhat difficult to recruit and hire SOC personnel in this climate.



70%

of security organizations say that it is extremely or somewhat difficult to recruit and hire SOC personnel.

To bridge the personnel gap, most organizations are turning to managed security services—74% of organizations already use managed services for security analytics and operations in some capacity. Managed security services also have a strong future, as 91% of organizations will increase their use of managed security analytics and operations services in the next 12 to 18 months.

ORGANIZATION'S USE OF MANAGED SECURITY SERVICES

74%

already use managed services for security analytics and operations in some capacity.

91%

will increase their use of managed security analytics and operations services in the next 12 to 18 months.

Smart CISOs will include SOC technologies and managed services as part of a cohesive and comprehensive SOC strategy.

Back to Contents

While it hasn't yet attained preferred status, many organizations are using cloud-based analytics…

In the past, many security professionals eschewed cloud-based security analytics and operations tools, opting instead for the oversight and control associated with on-premises tools. Slowly but steadily, this behavior is shifting. Forty-one percent of survey respondents claim that their organization prefers cloud-based security analytics/operations technology today while another 17% are willing to consider cloud-based options on a case-by-case basis.

Why the changing preference for cloud-based security? Cloud-based security analytics/operations technologies offer massive processing/storage scale and attractive pricing models while eliminating the cost and operational overhead associated with on-premises solutions.

41%
of survey respondents claim that their organization prefers cloud-based security.

17%
are willing to consider cloud-based options on a case-by-case basis.

Security professionals are actively moving security analytics and operations technologies to the public cloud—38% are already using public cloud-based security analytics and operations technologies, 44% are willing to do so in a hybrid environment, and 12% would consider using cloud-based security analytics and operations technologies in the future.

38%
are already using public cloud-based security analytics and operations technologies.

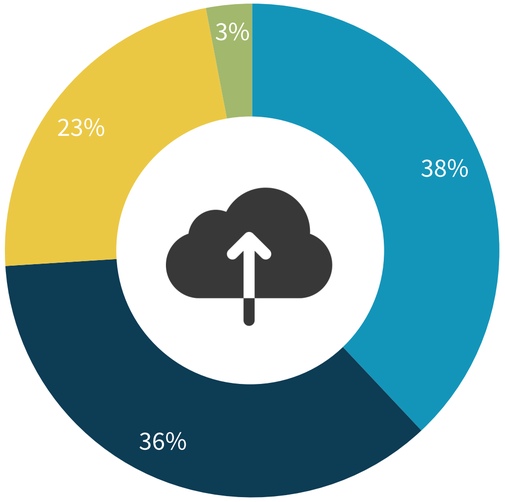
44%
are willing to do so in a hybrid environment.

Back to Contents

…and this usage is expected to increase.

Cloud-based security analytics technology strategies follow diverse paths. Thirty-eight percent of organizations will move some or all existing security analytics technology infrastructure to the cloud in a "lift and shift" approach toward SOC strategy. Alternatively, 36% plan to replace on-premises security analytics technologies with native cloud-based alternatives, while 23% will supplement on-premises analytics technologies with additional cloud-based capabilities.

All roads seem to lead to cloud-based security analytics in the near future. Organizations must inventory current SOC technologies, map their strengths and weaknesses with emerging requirements, and craft an intelligent migration that includes cloud-based security analytics technologies and supporting managed security services.



- Move some or all its existing security analytics technology infrastructure to the cloud
- Replace its on-premises security analytics technology with a cloud-based alternative
- Supplement an existing security analytics technology with additional capabilities delivered by a cloud-based security analytics provider
- Don't know

TOP 5 USE CASES ORGANIZATION'S ARE USING – OR WOULD CONSIDER USING – FOR CLOUD-BASED SECURITY ANALYTICS

42%
Real-time threat detection and response

42%
Cyber risk management monitoring and analysis

35%
Threat intelligence platform

35%
A dedicated security data lake

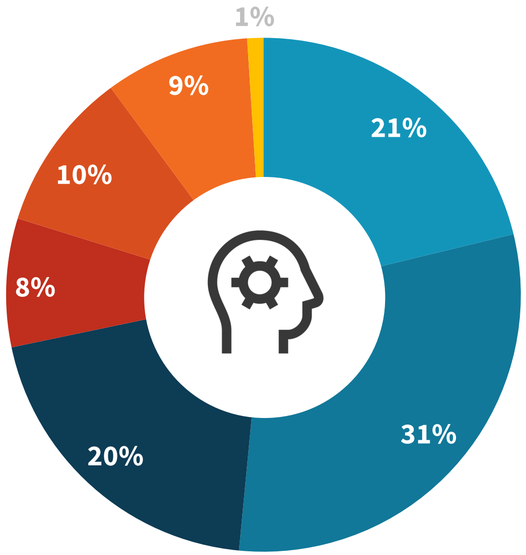
34%
A dedicated security analytics/operations system for workloads running in the public cloud

Back to Contents


Organizations are incorporating machine learning and automation/ orchestration into their technology plans.

Machine learning expected to help with threat hunting and security investigations.

Aside from managed services, security professionals want their security analytics and operations technology to help address their growing workload. More than half (51%) of organizations are already using machine learning technologies today while another 38% are piloting machine learning technology, planning a machine learning project, or interested in deploying machine learning technology in the future.



- Yes, my organization is already doing this extensively
- Yes, my organization is already doing this on a limited basis
- Yes, my organization is currently piloting a project to deploy machine learning technology for security analytics and operations
- Yes, my organization is planning a project to deploy machine learning technology for security analytics and operations
- No, but my organization is interested in deploying machine learning technology for security analytics and operations
- No, and my organization is not planning a project or interested in deploying machine learning technology for security analytics and operations
- Don't know

The top use cases for machine learning technology include improving advanced threat detection, accelerating security investigations, and identifying cyber-risks.

Many organizations remain cautious of machine learning technologies and they will likely supplement rather than replace existing layers of defense. Nevertheless, machine learning will gain incremental traction within the SOC. Rather than blind faith in algorithms, CISOs must develop the expertise necessary to deploy, operate, and fine-tune machine learning technologies to achieve a "force multiplier" effect on security operations.

TOP 3 REASONS FOR USAGE OF OR INTEREST IN MACHINE LEARNING TO SUPPORT ANALYTICS AND OPERATIONS

37%
Improve detection of advanced threats

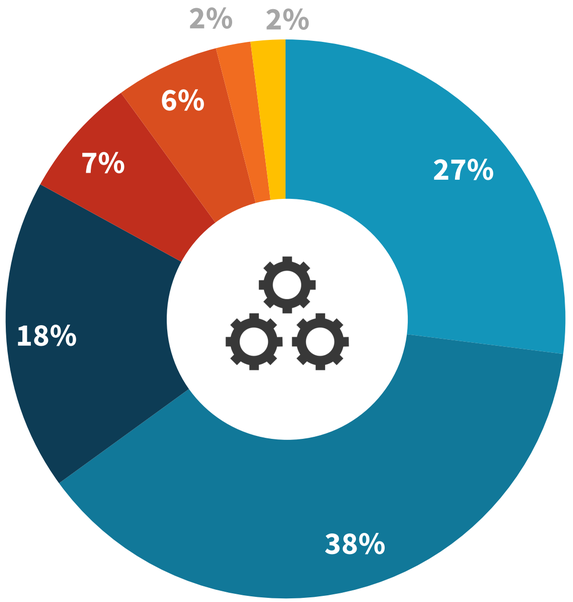
34%
To accelerate security investigations

34%
To help identify cyber-risks overall

Back to Contents

The Trend toward security operations process automation.

Similar to machine learning, many organizations need help with security operations process automation and orchestration. To address this requirement, 27% of organizations have deployed technologies for security analytics/operations automation and orchestration extensively while 38% have done so on a limited basis. Another 31% are piloting security operations automation/orchestration technology, planning a project, or interested in doing so.



- Yes, my organization is already doing this extensively
- Yes, my organization is already doing this on a limited basis
- Yes, my organization is currently piloting a project to automate/orchestrate security analytics and operations
- Yes, my organization is planning a project to automate/orchestrate security analytics and operations
- No, but my organization is interested in automating/orchestrating security analytics and operations sometime in the future
- No, and my organization is not planning a project or interested in doing so in the future
- Don't know

The top use cases for machine learning technology include integrating security and IT operations technologies, improving collaboration between security and IT operations, automating remediation tasks, and tracking security event lifecycles.

Security operations process automation should start with process assessment and an evaluation of all tasks associated with a workflow. CISOs should establish best practices by streamlining and optimizing manual processes and then (and only then) apply technologies for process automation.

TASKS THAT ARE OR WOULD BE THE TOP PRIORITIES FOR SECURITY OPERATIONS AUTOMATION/ORCHESTRATION

35%
Integrate security tools with IT operations systems

34%
Improving collaboration between security and IT operations staff

29%
Automate remediation tasks without involving IT operations

Back to Contents

chronicle

Chronicle, now part of Google Cloud, offers Backstory, a global security telemetry platform for investigation and threat hunting within your enterprise network. Backstory makes security analytics instant, easy, and cost-effective. Backstory is a specialized, cloud-native security analytics system, built on the core infrastructure that powers Google itself.

Learn more at https://chronicle.security

LEARN MORE

About ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.