Technical Validation

Securonix Security Operations & Analytics Platform

Cloud-native Analytics-driven SIEM with Efficient Collection, Detection, and Response

By Jack Poller, Senior Analyst

November 2019

This ESG Technical Validation was commissioned by Securonix and is distributed under license from ESG.

Contents

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

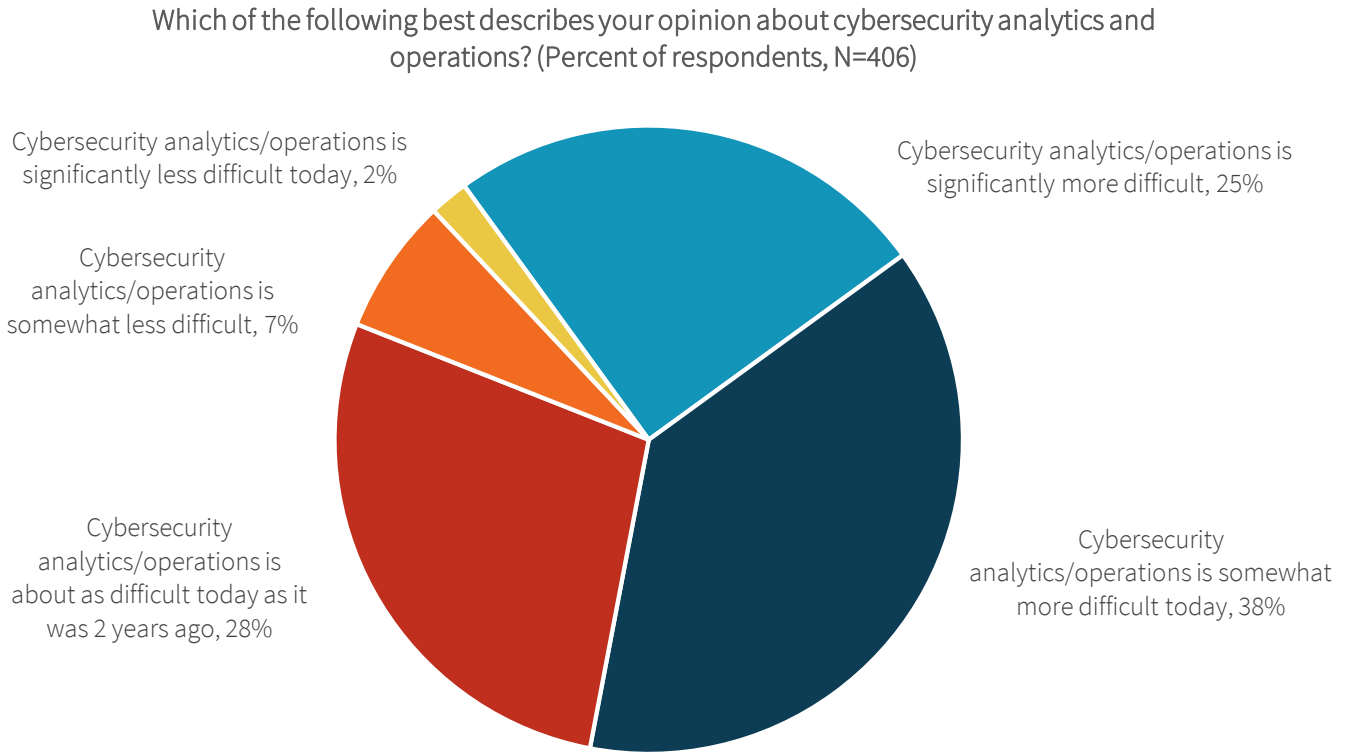
Introduction

This report examines Securonix Security Operations & Analytics Platform with a focus on how the platform efficiently and effectively provides next-gen security information and event management (SIEM); network traffic analysis (NTA); user and entity behavioral analytics (UEBA); security orchestration, automation, and response (SOAR); and security data lake (SDL) solutions. ESG also examined the economic value and benefits of the Securonix cloud-native SaaS solution.

Background

According to ESG research, almost two thirds (63%) of organizations say that cybersecurity analytics and operations is more difficult today than it was two years ago (see Figure 1).[1]

Figure 1. Level of Cybersecurity Analytics/Operations Difficulty



Source: Enterprise Strategy Group

Fundamental external changes and internal inefficiencies increase complexity and continue to make security analytics and operations difficult. Forty-one percent of organizations say that one of the top drivers of this increasing difficulty is the evolving and rapidly changing threat landscape, the most cited response, and 30% say that one of the drivers is that the attack surface has grown over the past two years.

In terms of internal drivers, 35% of organizations say that the fact that they collect and process more security data is one of the primary drivers of the additional complexity of security analytics and operations, and 34% say that the volume of security alerts has increased over the past two years is also a driver.

More than three-quarters (77%) of organizations use ten or more security analytics and operations tools, with SIEM, threat intelligence, and EDR being the most commonly deployed. Organizations are collecting and analyzing data from a wide

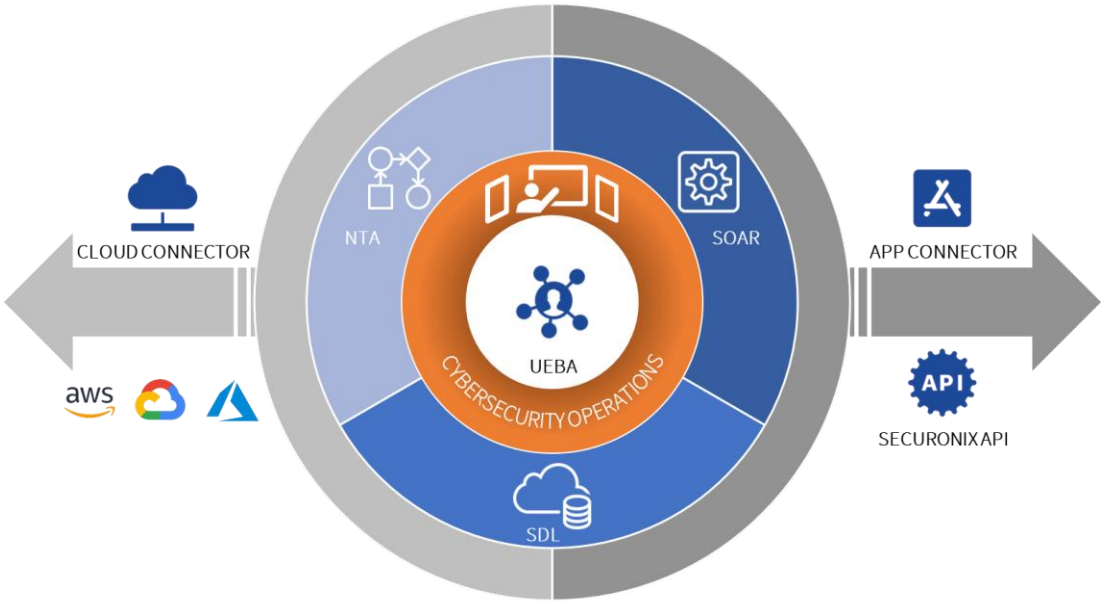
[1] Source: ESG Research, *The Rise of Cloud-based Security Analytics and Operations Technologies*, August 2019. All ESG research references and charts in this technical validation have been taken from this research report.

range of telemetry including endpoint security, web and network systems, email security, network and security system logs, threat intelligence, vulnerability management systems, and more. Thus, these organizations say that two of their top challenges are monitoring security across a growing attack surface (27%) and keeping up with the volume of security alerts (23%).

Securonix

The Securonix Security Operations & Analytics Platform provides data collection, behavior analytics and machine-learning-based advanced threat detection, and automated incident response. The SaaS platform leverages cloud-native, big data, and AI tools and methodology to deliver an effective and efficient solution with unlimited scalability.

Figure 2. The Securonix Security Operations & Analytics Platform Architecture



Source: Enterprise Strategy Group

Securonix designed the platform to ingest cybersecurity telemetry into a security data lake (SDL)—a centralized, scalable repository for all structured and unstructured data. NTA, UEBA, and machine learning (ML) analytics identify threats and SOAR enables analysts to create and manage cases, respond, and remediate threats. Securonix's cloud-based platform is open: organizations can access the data in the SDL, and APIs and connectors can facilitate access and analyses.

Securonix Platform is a cloud-native SaaS solution. Securonix provides fully managed 24x7 operations with 99.5% availability and continuous upgrades and feature enhancements. The platform is SOC 2 Type 2 certified and encrypts data in transit (and optionally, data at rest). Granular role-based access controls can limit access and apply least-privileged access policies. The multi-tenant architecture maintains complete tenant data segregation, and detailed logging provides a full audit trail of all activities. Securonix is an AWS Security Competency partner with certified subject matter experts that manage and maintain the SaaS platform.

Securonix uses identity-based pricing decoupled from data volume and velocity. This provides organizations with predictable costs and encourages the collection and analysis of all telemetry—the more data that is collected and analyzed over longer timeframes, the greater the probability of identifying long-lived threats from temporally disconnected indicators of attack and compromise (IOA/IOC).

Securonix provides next-generation SIEM capabilities—unlimited scalability, UEBA, threat hunting, and SOAR. Using big data technology, Securonix can ingest and store as much telemetry data as needed without impacting functionality. Data is

stored in an open data format and can be used by other applications. The SIEM includes built-in connectors to ingest telemetry from cloud applications and infrastructure, enterprise applications, identity and HR data, and non-technical data feeds. Data is enriched in real time with identity, asset, geolocation, threat intelligence, and other data.

Analytics and machine learning algorithms are applied to event data in real time to detect advanced cyber and insider threats. Analysis includes IOC/IOAs and threat chains aligned to the 12 stage MITRE ATT&CK kill chain and the individual TTPs within each stage. Thus, Securonix automates the MITRE kill chain to both detect existing "slow-and-low" attacks and predict future slow-and-low attacks based on leading IOCs and behavioral patterns. Additional built-in UEBA and threat chain analyses include insider threats, cyber threats, fraud, cloud security, and business applications.

The Securonix Platform accelerates threat hunting using natural language search. Security analysts can search for threat actors or IOCs. Visual pivoting enables rapid exploration and development of threat context, and visualized data can be saved as dashboards or exported.

Securonix integrates SOAR and case management capabilities and can also interoperate with third-party solutions including Demisto, Remedy, and ServiceNow. The Securonix platform includes an AI-based incident remediation recommendation engine based on previous behavior patterns of incident responders. Built-in incident response playbooks include configurable automated actions. The incident management system and workflow allow multiple analysts and teams to collaborate on investigation and remediation.

ESG Technical Validation

ESG's evaluation and testing of Securonix involved using a demo environment to collect cybersecurity telemetry, discover threats, and investigate and remediate a threat chain. Leveraging ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation, we evaluated the economic benefits of Securonix.

Data Collection and Attack Detection

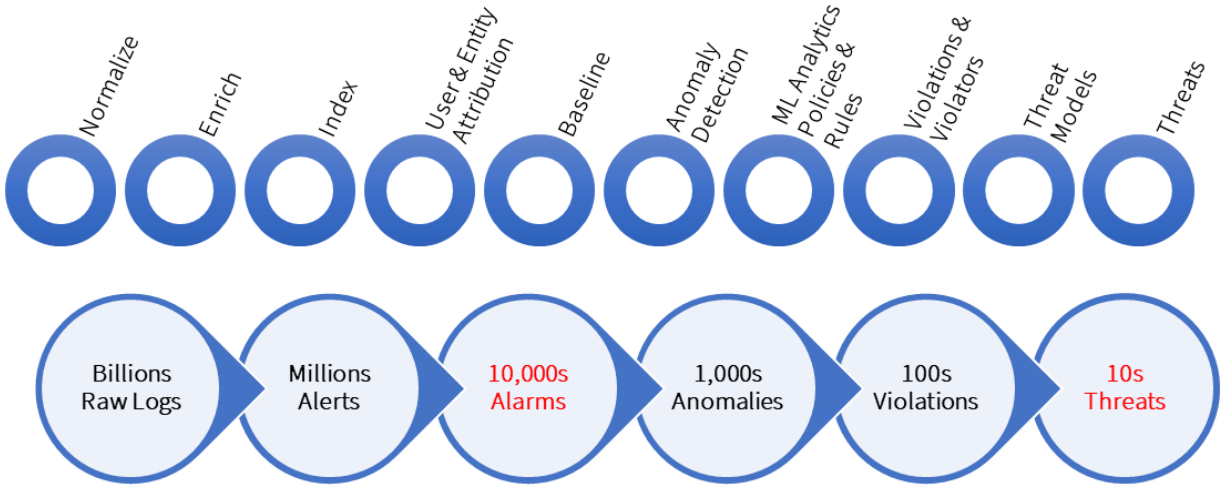
ESG started with a preconfigured demo deployment of Securonix managed through a standard web browser interface. The demo environment mimicked a typical enterprise IT infrastructure with a variety of endpoint, network, and cloud cybersecurity control systems from disparate vendors. All telemetry was collected into Securonix cloud security data lake.

As shown in Figure 3, Securonix has developed an analytics-driven pipeline to process telemetry. First, Securonix normalizes and enriches the data. The enrichment process identifies, correlates, and tags key types of information including point-in-time information such as IP address assignment to a specific device and geographic location, as well as other data types such as user data (ID, email, group, division, etc.), account information, device information, software and version information, and more. Indexing and storing enriched data in the SDL enables rapid searches and provides the ability to run analytics across all data sources.

Next, Securonix analyzes the data using a variety of algorithms and machine learning models to detect and identify anomalies and IOA/IOCs. Securonix uses threat chains such as the MITRE ATT&CK framework, which models ten stages of adversarial tactics and techniques in a typical attack. Using threat chains, Securonix correlates a set of threats over time into a single specific attack.

A typical enterprise environment may generate billions of raw log entries daily. Traditional SIEMs can process these log files, identifying millions of potential issues and generating tens of thousands of alarms. Securonix's analytics-driven pipeline further reduces the alarms into thousands of behavior-based anomalies, hundreds of violations tied at the entity level, and finally down into tens of threat chains to be investigated. Securonix only generates alarms for the threat chains, reducing the security analyst workload and minimizing alert fatigue.

Figure 3. Next-gen Cybersecurity Analytics-driven Pipeline

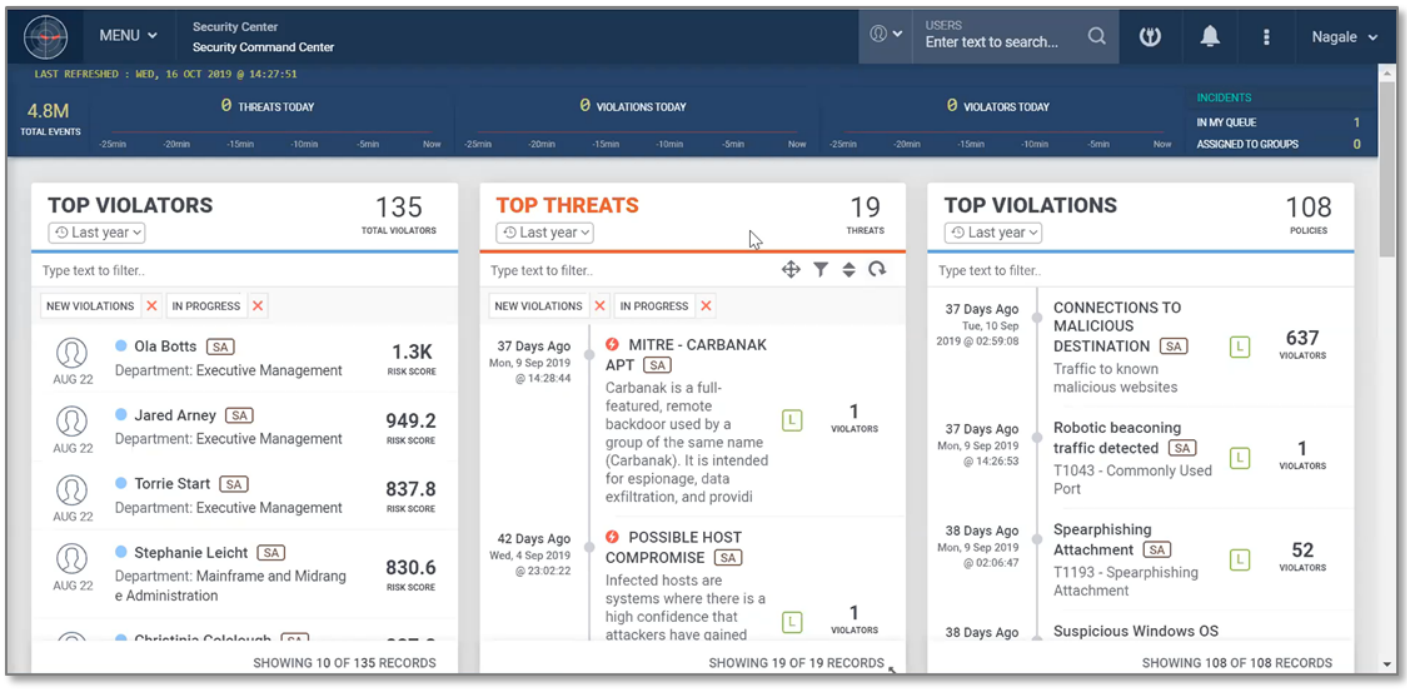


Source: Enterprise Strategy Group

ESG first reviewed the Securonix dashboard. As shown in Figure 4, the top of the dashboard provides summary data including the number of threats, violations, and violators for the day, along with a graph for each metric of events for the last 30 minutes. Also shown is the total number of events, the number of incidents being managed, and the number in the queue for the analyst.

The main portion of the dashboard is divided into three customizable panels providing at-a-glance summaries of the top violators, top threats, and top violations. The left panel, top violators, ranks users by a risk score, computed from the risk represented by each threat chain including that user. The center panel, top threats, lists the most recently identified threat chains. The right panel lists the most recently identified violations—an IOC/IOA. Each of the entries in the lists are live links—clicking on the links drills down to provide more details.

Figure 4. Securonix Dashboard



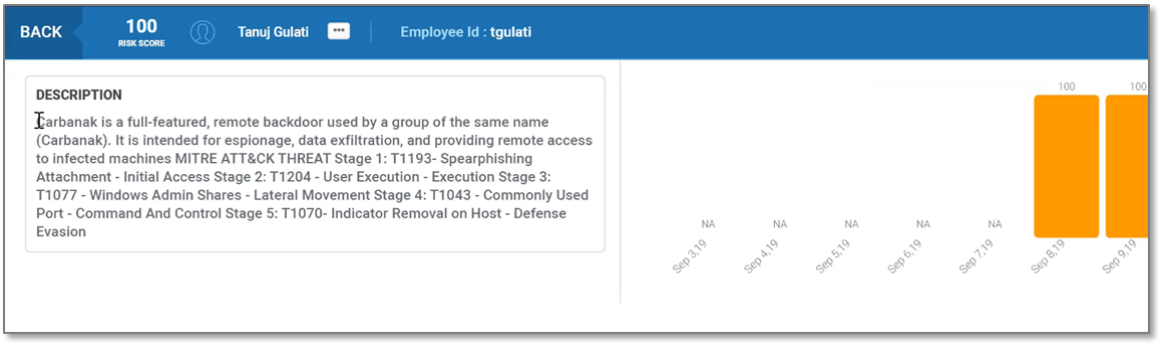
Source: Enterprise Strategy Group

ESG followed the typical workflow of an analyst observing the current state of the IT environment, focusing on the top threats, which represent the attacks in progress. To start an investigation of a current attack, we clicked on ***MITRE - CARBANAK APT***, the first item in the list of top threats.

As shown in Figure 5, Securonix displayed a summary of the attack, identifying the risk score of the affected user. Risk scores (0-100) are computed based on the MITRE ATT&CK stages—attacks that progress further through the stages represent higher risk to the organization.

Below the summary is the attack description. As with risk scores, the attack description considers the attack progress—each MITRE ATT&CK stage observed in this instance of the attack is identified in the description. Alongside the description is a graph showing the risk over time from this attack.

Figure 5. Attack Investigation: MITRE – CARBANAK APT



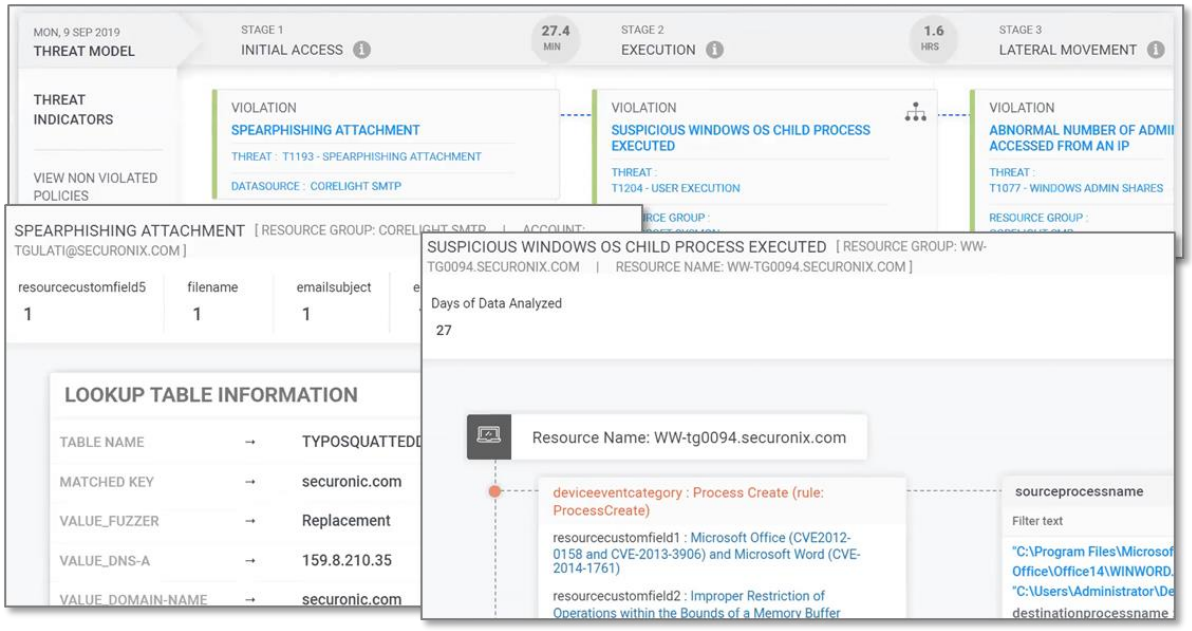
Source: Enterprise Strategy Group

Below the description is a scrollable flowchart providing summary info on each stage of the attack, as shown in Figure 6. Securonix's analytics identified this attack threat chain by correlating individual events over time, and the top portion of the flowchart displayed a map with the stage names and the elapsed time between stages. The bottom portion of the flowchart displayed critical details for the stage including the data source. In this Carbanak APT attack, user tgulati was sent a spear phishing attachment, identified with telemetry from Corelight SMTP. Twenty-seven minutes later, the user clicked on the attachment, launching a suspicious executable, identified with telemetry from Microsoft Sysmon. One hour and 36 minutes later, using Corelight telemetry, Securonix identified that an abnormal number of administrative shares were accessed, indicating lateral movement of the attack.

ESG clicked on the spear phishing attachment box and Securonix displayed details about the event. Enriched data, such as the typosquatted domain name, the most like match, and IP address, were displayed, enabling the security analyst to quickly understand how the user may have been fooled into opening a malicious attachment.

Continuing the investigation, ESG clicked on the lateral movement box on the attack flowchart and Securonix displayed details. Enriched data included *Improper Restriction of Operations with the Bounds of a Memory Buffer,* which indicates that Microsoft Sysmon had identified a buffer overflow event.

Figure 6. CARBANAK APT Attack Investigation: Spear Phishing and Execution Stages



Source: Enterprise Strategy Group

ESG continued the investigation of the Carbanak APT attack, reviewing the lateral movement, command and control, and defensive evasion stages. For each stage, Securonix provided relevant details, enabling the administrator to understand the event and why the event had been identified as a stage in this attack.

For lateral movement, identified by machine learning as an anomalous number of accesses to administrative shares, Securonix provided a graph of accesses over time, along with counts for valid accesses, noisy (indeterminate) accesses, and anomalous accesses. For command and control access, Securonix identified and displayed robotic beaconing to a specific IP address.

Why This Matters

Seventy percent of organizations today use SIEM, which incorporates a variety of other security technologies like endpoint detection and response (EDR), network traffic analysis, UEBA, and threat intelligence feeds/analytics. 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.

ESG validated that Securonix has gone beyond wrapping a single user interface around multiple point tools. The integrated solution has been architected to maximize the productivity of the security practitioner with a seamless architecture and environment that supports surfacing threats, analyzing impact, remediation, and root cause. Securonix applies multiple analysis techniques to identify threats and attacks in near real time with the analysis-driven data processing pipeline. Securonix reduces security practitioner workload by correlating multiple IOC/IOAs into a threat chain representing an attack. Dynamic risk scoring helps the security team to prioritize their activities.

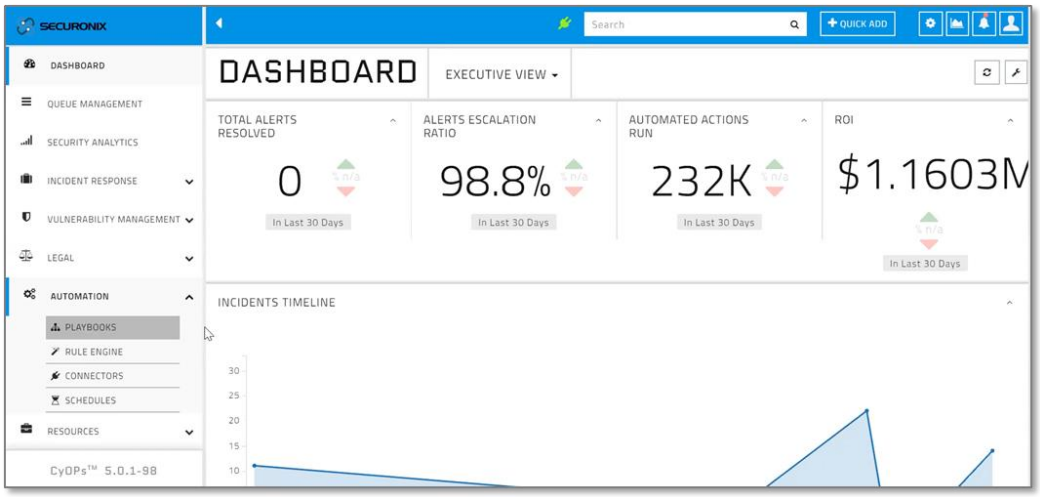
Securonix simplifies attack investigation, providing all relevant, enriched data aligned to the MITRE ATT&CK framework, organized in an intuitive interface, and displayed as a logical flowchart of events. This enables analysts to focus on investigating and responding to attacks rather than triaging many thousands of alerts for each individual IOC/IOA.

Attack Response and Threat Hunting

The Securonix Security Operations & Analytics Platform includes a complete security orchestration, automation, and response (SOAR) solution, including suggested remediation steps along with automatable playbooks.

ESG started with a review of the Securonix SOAR dashboard, shown in Figure 7. The top of the dashboard displays a 30-day summary of the state of incident response, including the number of resolved alerts, the alert escalation ratio, the number of automated actions executed, and the calculated ROI. Below the summary is the incident timeline, charting the number of incidents per day for the last 30 days.

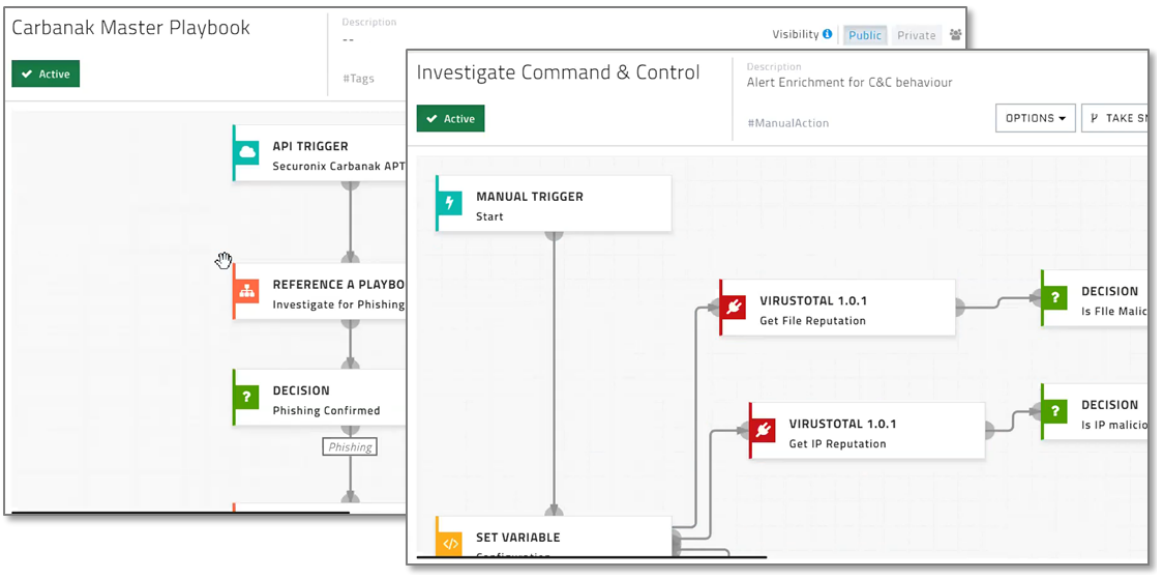
Figure 7. SOAR Dashboard



Source: Enterprise Strategy Group

Next, ESG reviewed the Carbanak master playbook by using the left side menu to navigate to Playbooks. As shown in Figure 8, Securonix Playbooks use an easy-to-understand flowchart to display the detection and remediation steps. We clicked on the ***Investigate Command and Control*** box to drill down into the process step, and Securonix displayed the flowchart for this stage of the investigation. Manipulating the flowchart and editing the playbook was intuitive.

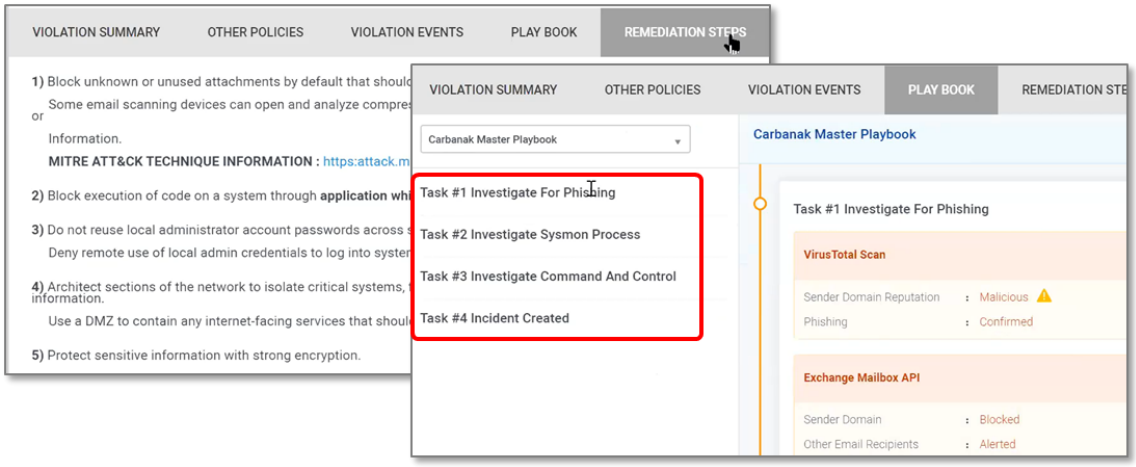
Figure 8. Playbooks



Source: Enterprise Strategy Group

Next, ESG continued the typical workflow of a security analyst, proceeding from the investigation stage to the remediation stage. From the CARBANAK APT attack details display (see Figure 5), ESG clicked on the ***Remediation Steps*** tab. Securonix displayed best practices for remediating the Carbanak attack, as shown in Figure 9. These in-context steps are derived from the MITRE ATT&CK framework and from Securonix crowdsourcing of best practices throughout the industry. Next, ESG clicked on the ***Playbook*** tab, and Securonix displayed the playbook, which included the automatic creation of a case to track the incident.

Figure 9. Carbanak APT Remediation Steps and Playbooks

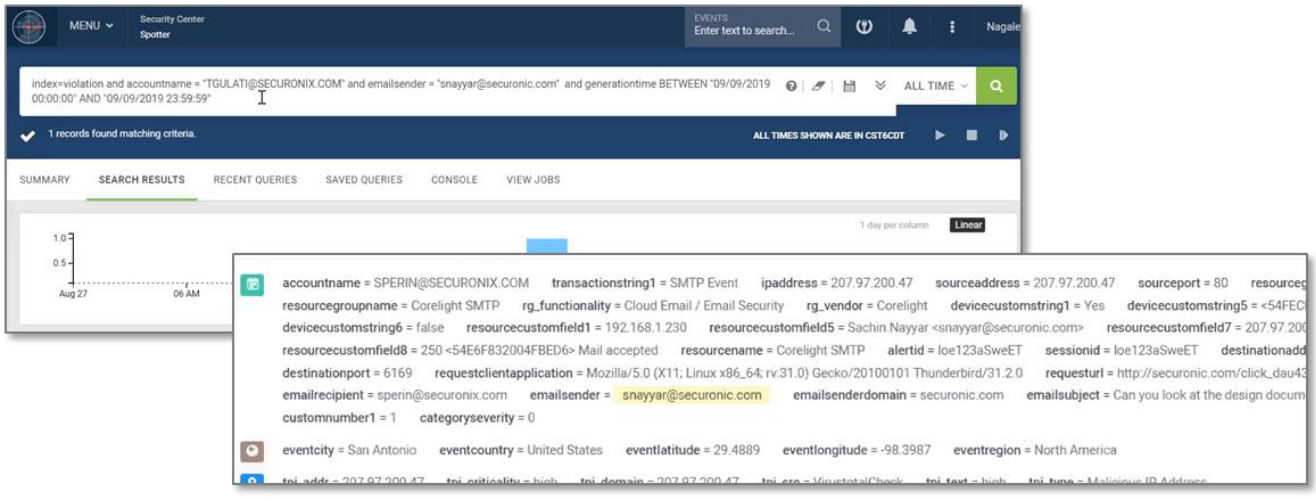


Source: Enterprise Strategy Group

Next, ESG continued with the typical workflow of a security analyst, pivoting to threat hunting. Having investigated and remediated the attack, the next step is to search the environment to identify if any other users may be susceptible to the same or similar attacks.

From the Carbanak attack stage flowchart, we clicked on the spear phishing box. The spear phishing details provided the email sender, which included the typosquatted domain. We right-clicked on the email sender and selected ***Launch Spotter*** to launch the text-based search engine. This provides simple access to the Securonix SDL (Security Data Lake). As shown in Figure 10, Securonix automatically built a search query specific to the incident, and the search results displayed the single record for this event. The results included a graph of the events over time, and the enriched data for the event.

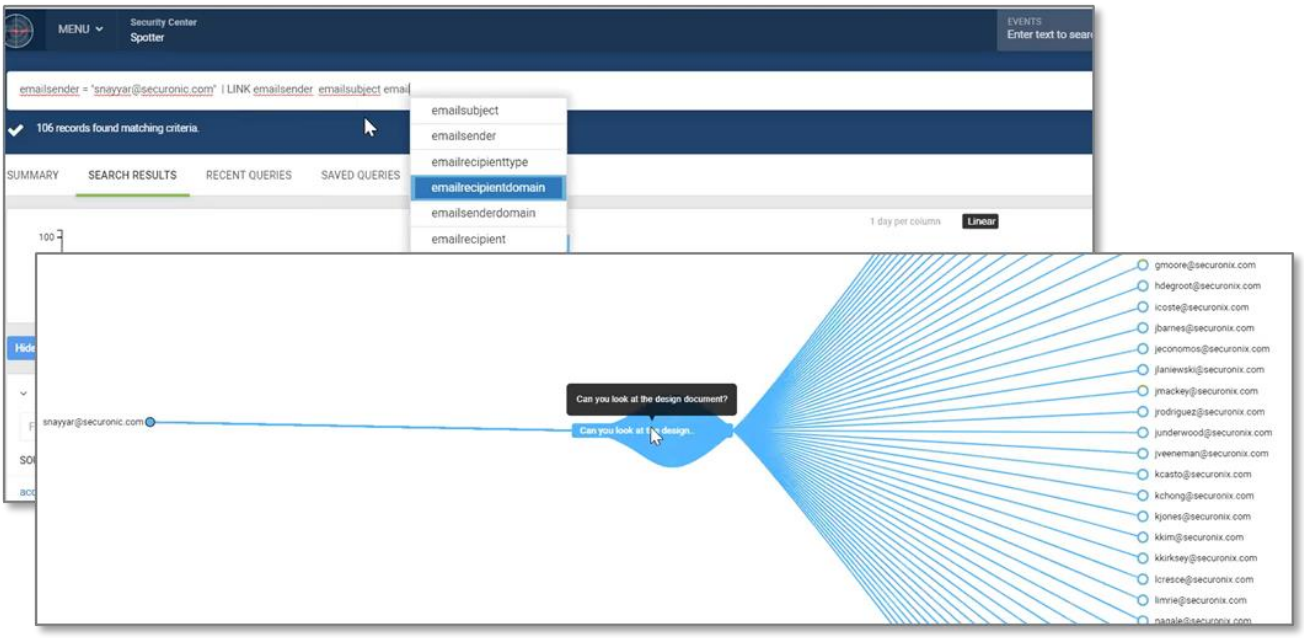
Figure 10. Pivoting to Threat Hunting



Source: Enterprise Strategy Group

To search for related threats, ESG quickly modified the search box, removing the ***ACCOUNTNAME*** and timeframe search parameters, leaving just a search for the email sender of the original spear phishing email. We added search parameters to link the email sender with the email subject and then email recipient, as shown in Figure 11. Securonix provided autocomplete suggestions for search times, and then returned search results within a second. The results were displayed on an interactive graph and hovering the mouse over the email subject box brought up a popup with the email subject text.

Figure 11. Interactive Threat Hunting: Linking Email Sender to Email Subject to Email Recipient

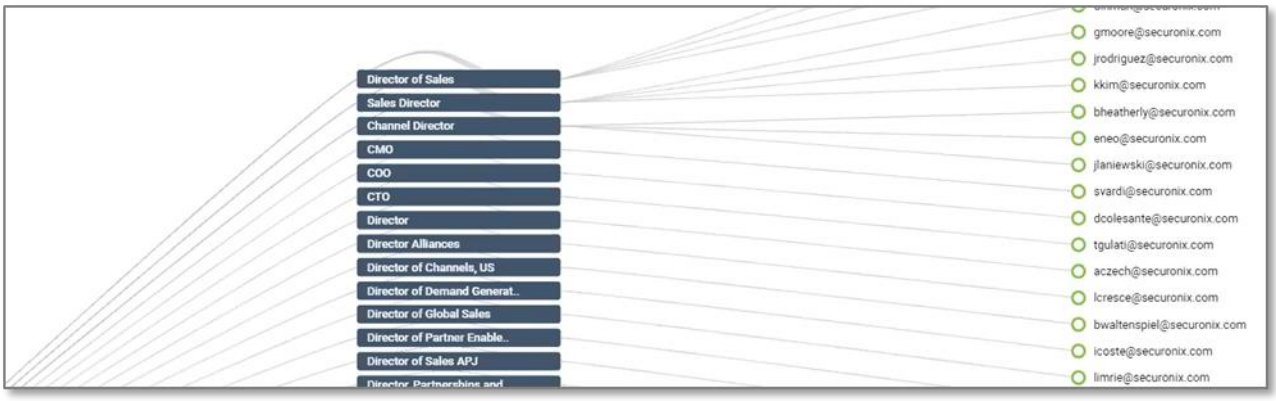


Source: Enterprise Strategy Group

The search results enabled us to quickly identify other potential victims of the spear phishing attempt, and we could take action to prevent infections such as emailing those users, or automatically blocking the sender.

To understand the attacker's methodology, we modified the search, changing the linking to first link to the recipient title. Because the data stored in the SDL is enriched, searching and linking is very fast, and results were returned within a second, as shown in Figure 12. We could use these results, which showed that the attacker was targeting the director and C-level staff of the organization, to develop defenses, such as increased security awareness and training for this group.

Figure 12. Interactive Threat Hunting: Pivoting Search, Linking Sender to Recipient Title



Source: Enterprise Strategy Group

Why This Matters

Security analytics and operations can be complex, requiring highly skilled professionals and detailed processes. This is especially true for incident responders and threat hunters using a SIEM. According to ESG research, 23% of organizations say that one of the most challenging attributes of SIEMs to their organizations is that they require lots of personnel training and experience to attain maximum value (the top response), and 21% complain that junior people tend to struggle doing anything more than looking at basic dashboards.

ESG found that Securonix provides a sophisticated, effective, and easy-to-use solution that accelerates incident response, providing context-specific remediation guides and automated playbooks. Securonix's extensive library covers the MITRE ATT&CK framework, and security teams can quickly create and edit playbooks using an intuitive flowcharting environment.

Securonix's intuitive natural language search system reduces the analyst learning curve and accelerates threat hunting. Searches are federated across all data sources, and with enriched data stored in the data lake, search results are returned in near real time. Threat hunters can quickly and easily pivot searches to find existing and potential threats and develop proactive defenses.

Economic Value

ESG evaluated the economic value of Securonix Security Operations & Analytics Platform, leveraging ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. Three pillars provide Securonix economic value, as shown in Figure 13.

Figure 13. Securonix Economic Value

Source: Enterprise Strategy Group

Cloud-native and Cloud-scale

Cloud-native is an approach to building and running applications that exploits cloud architectures. Cloud-native apps are architected to be elastic and run in a distributed environment. Agile and scalable app components are loosely coupled and deliver discrete and reusable features that are integrated in a well-described manner.

The benefits of Securonix cloud-native methodology and cloud-native platform include:

- Rapid product iteration—Securonix can quickly deliver bug fixes as well as new features and functionality using continuous integration and delivery (CI/CD). Organizations don't have to wait for major product release cycles or interrupt service to obtain needed features and fixes.
- Auto-provisioning—Securonix cloud-native environments use on-demand, self-service, programmatic provisioning and releasing of resources. This enables Securonix to make the most efficient use of resources, eliminating the cost and effort of manual overprovisioning for anticipated peak loads. Securonix passes the savings on to the user.
- Auto-scaling—Securonix leverages cloud-native auto-scaling to manage the complex up-down process needs as workload resource requirements change over time. Thus, Securonix can accommodate the needs of any sized organization without service interruptions.
- Auto-redundancy—cloud-native applications are inherently resilient, automatically moving processing from failed nodes. Thus, Securonix can deliver an exceptionally reliable platform, and customers should expect little downtime.

- Quick time-to-value—organizations can start a Securonix instance in the cloud without the time, cost, and effort necessary to acquire, install, and manage an infrastructure stack.

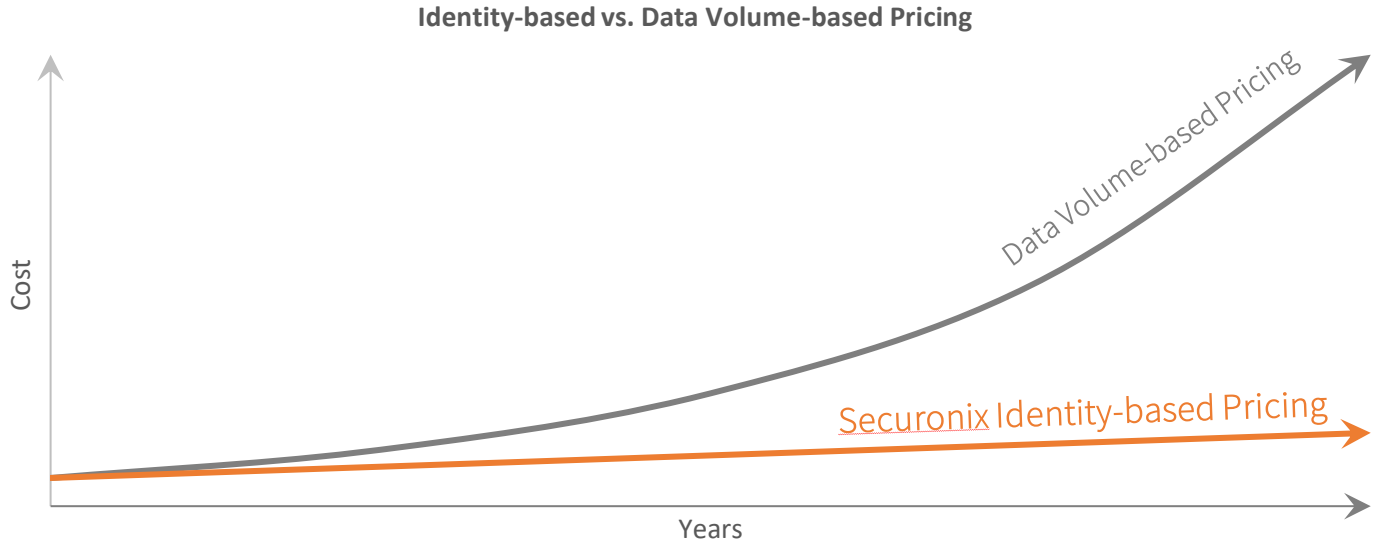
Cloud-scale infrastructures can be scaled without any technical limitations. Securonix leverages cloud-scale infrastructures from public cloud service providers (CSPs) including Amazon, Google, and Microsoft. The benefits include:

- Automated deployment and management—this alleviates much of the cost and effort of delivering a SaaS solution.
- On-demand infrastructure—public CSPs deliver infrastructure instantaneously on demand, eliminating the need for Securonix to invest in infrastructure.
- Cloud reliability and availability—public CSPs maintain 99.99% or better availability, enabling Securonix to deliver the same level of availability and reliability, without additional investment.
- Deployment flexibility—organizations can choose in which regions their data resides for compliance and data sovereignty, and government entities can leverage compliance-centric infrastructure such as Amazon Cloud for Government.
- Unlimited scalability—CSPs provide independent and infinite compute, storage, and network scalability, enabling Securonix to provide services to any sized enterprise.

Securonix leverages the resources, benefits, and economies of scale of public CSPs to provide a fixed and predictable pricing model for SIEM services. Traditional SIEM solutions use a data volume-based pricing model, and costs increase in direct relation to the ever-growing volume of security telemetry.

Securonix uses identity-based pricing—the cost of the service is dependent primarily on the number of users. Decoupling pricing from data volume and velocity provides organizations with predictable costs (see Figure 14) and encourages the collection and analysis of all telemetry. Collecting and analyzing more data over longer timeframes affords a greater probability of identifying long-lived threats from temporally separated IOA/IOC.

Figure 14. Identity-based Pricing



Source: Enterprise Strategy Group

Cybersecurity Data Lake

Securonix enriches, indexes, and stores all source data into a single security data lake. The SDL is accessed and managed using big data and high-performance computing tools and techniques. Benefits include:

- Any data—organizations can collect and store telemetry from new or unusual sources, enabling security analysts to search and correlate events from any and all sources. Securonix ML and UEBA algorithms can be updated to incorporate data from any source. This improves the fidelity and ability to discover unknown and long-lived APTs.
- All data—organizations can collect and store an unlimited amount of data. This enables algorithms and threat hunters to search for long-lived APTs, as well as provide data for compliance and forensics.
- Search, investigate, and report at scale—performance of analysis and searches is not affected by the size of the SDL, encouraging the collection of more telemetry over longer timeframes.
- Link analysis—Securonix supports real-time threat hunting and link analyses using stored enriched data. Performance is not impacted by the need to enrich data during search time, and search results are returned within a matter of seconds, enabling security analysts to rapidly discover existing and potential threats and attacks.
- Own, access, and share the data—Securonix implements an open non-proprietary SDL, and the data is "owned" by the organization, not by Securonix. Organizations can access and share the data in the SDL and can develop their own applications that use the data. This alleviates the cost and effort of storing the data in multiple locations.

Complete Security Operations Platform

Securonix Security Operations & Analytics Platform combines the features and functionality of next-gen SIEM, NTA, UEBA, SOAR, and SDL into a single platform. The benefits of an integrated solution include:

- Simplification—Securonix's integrated solution simplifies security operations, reducing the cost and effort of integrating tools from disparate vendors, training security analysts to use multiple tools, and managing multiple vendor relationships.
- Risk amplification and scoring—risk scoring based on progress through MITRE ATT&CK stages amplifies critical risks, enabling organizations to triage attacks and improve ROI when addressing threats.
- Advanced analytics—Securonix's analytics-driven pipeline uses advanced ML and UEBA analytics in real time as data is ingested into the system, providing quicker discovery of threats and attacks.
- Reduce MTTR—threat investigation, automated case management, remediation, and threat hunting are integrated, automated, and orchestrated, eliminating the time, effort, and expense of developing processes, tools, and scripts.
- Cost savings—the amounts of data duplication, processes, and personnel required to build and maintain infrastructure for separate point tools are reduced.

Why This Matters

Cybersecurity professionals have previously avoided cloud-based security analytics and operations tools. Slowly but steadily, cloud solutions are becoming acceptable. Forty-one percent of ESG research survey respondents indicate 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 solutions offer massive processing/storage scale and attractive pricing models without the need for on-premises infrastructure and operations overhead.

ESG found that the Securonix SaaS solution delivers the operational and economic benefits of cloud-native and cloud-scale technology and architecture. Securonix provides unlimited scalability, operational simplicity, rapid and automated deployment and management, reliability, and availability.

Securonix identity-based pricing decouples pricing from data volume and velocity. This ensures that organizations can predict their costs and encourages organizations to collect, store, and analyze any and all security telemetry—collecting more data over longer timeframes affords a greater probability of identifying long-lived threats.

Storing the cybersecurity data lake in the cloud provides unlimited storage and scaling. Organizations can store any and all security telemetry, providing greater fidelity for analyses, threat hunting, and remediation. Securonix provides access to the SDL, eliminating the need to retain data in a separate location for other analyses or forensic efforts.

Securonix's integrated solution eliminates investments in separate SIEM, NTA, UEBA, SOAR, and SDL solutions. Securonix incorporates data collection, analysis, automation, and case management into a single solution, simplifying practitioner workload and eliminating the cost and effort to develop processes and train personnel to use multiple point tools.

The Bigger Truth

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.

ESG validated that Securonix simplifies and accelerates cybersecurity data collection, threat detection, attack response and remediation, and threat hunting. Testing revealed:

- Securonix can identify threats and attacks in near real time with the analysis-driven data processing pipeline, reducing security practitioner workload, and accelerating triage with dynamic risk scoring.
- Securonix simplifies attack investigation, enabling analysts to focus on investigating and responding to attacks rather than triaging many thousands of alerts for each individual IOC/IOA.
- Securonix provides a sophisticated, effective, and easy-to-use solution that accelerates incident response, providing context-specific remediation guides and automated playbooks. Securonix's extensive library covers the MITRE ATT&CK framework, and security teams can quickly create and edit playbooks using an intuitive flowcharting environment.
- Securonix's intuitive natural language federated search engine reduces the analyst learning curve. Enriched data and big data processing return search results in near real time, accelerating threat hunting.
- The SaaS solution provides unlimited scalability, operational simplicity, rapid and automated deployment and management, reliability, and availability.
- Securonix's identity-based pricing decouples pricing from data volume and velocity, providing predictability and encouraging the collection and analysis of all security telemetry, increasing the ability to identify threats.
- Securonix incorporates data collection, analysis, automation, and case management into a single solution, simplifying practitioner workload and eliminating the cost and effort to develop processes and train personnel to use multiple point tools.

Organizations in need of next-generation cybersecurity data collection, threat detection, and response should thoroughly test the efficacy, functionality, and operational capabilities before purchasing or deploying any cybersecurity analytics and operations solution.

Securonix Security Operations & Analytics Platform is a SaaS solution integrating SIEM, NTA, UEBA, SOAR, and SDL features and functionality. Leveraging cloud-native, big data, and AI tools and methodology enables Securonix to deliver an effective and efficient solution with unlimited scalability. The Securonix analysis-driven data processing pipeline identifies attacks in near real time and provides rapid responses to searches across all data sources while identity-based pricing changes the economics of SIEM solutions, providing predictable costs and encouraging the collection of all relevant data. If your organization is looking to streamline cybersecurity analytics and operations, then ESG believes that you should seriously consider how Securonix can efficiently and effectively help mitigate risk, defend critical assets, and remediate problems.

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

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188