elastic

Get more operational value from your SIEM

elastic.co →

Table of Contents

Introduction

As organizations embrace digital transformation initiatives to adapt to market changes, many have been forced to re-evaluate their security approach. New web products and services, mobile apps, and the need to support a remote workforce are making inroads for new types of cyber attacks. **Addressing these attacks requires security teams to evolve quickly to keep up**.

A core challenge to keeping up is avoiding inefficiencies that can threaten the business despite security teams' best efforts. The explosion of SaaS adoption, ongoing privacy mandates, and directives to consolidate security functions only add operational complexity.

The key to staying in control while maintaining operational efficiency starts with the data you have readily available within your security information and event management (SIEM) platform. The volume and variety of data that security teams need are exploding — cloud, Internet of Things (IoT), mobile sources, and observability data, to name a few. The result is a massive increase in event activity critical to uncovering insights needed to protect the business.

This explosion in data often introduces operational challenges due to SIEM limitations. **It may be time to review your approach to SIEM** to ensure you are ready for these new challenges.

175 ZB

IDC predicts that by 2025, worldwide data will grow to 175 zettabytes

41.6 B

By 2025, 41.6 billion connected devices will generate 79.4 zettabyes of data

42 B

Respondents to PwC's Global Economic Crime and Fraud Survey 2020 reported $42 billion in total fraud losses

Security requirements are evolving

As organizations adopt a more cloud-centric business model, security teams are tasked with more responsibility to ensure their businesses' most valuable assets — users, applications, endpoints, and data — are protected. Consider the following trends that are making it difficult for security teams to meet their KPIs and metrics.

People

Staying ahead of new and more sophisticated attack methodologies is essential.

- Security skills are in short supply
- Burdened security teams are striving to work better together, faster, and more efficiently

Process

Pressure is increasing to maintain operational efficiency and speed as cloud initiatives explode.

- Massive amounts of data are moving to the cloud
- Remote workers and partners need support for more cloud solutions

Technology

Support for high-volume data sources is vital to provide visibility into evasive activity and details needed to contextualize a threat.

- It's difficult to perform responsive queries and analysis across premises and cloud"
- In many systems, accessing high-volume data sources may be cost prohibitive

Security teams are painfully aware that digital transformation adds more attack surface — each new connected device or cloud service can introduce a new potential vector for an adversary to exploit, and could result in severe security threats or exposed assets that add to business risk. **The most fundamental requirement is to have the right context at the right time in order to make better and faster decisions**.

Rethink your security strategy using data as your framework

Maintaining visibility of a dynamic, growing attack surface is often impractical. Per-ingest or per-event licensing models and/or architectures that do not meet cloud scale requirements can force tradeoffs. Teams often spend time and resources deciding which data to include and exclude from day-to-day operations, leaving the organization with limited visibility in their SIEM, resulting in operational silos — data silos, team silos, and process silos.

Instead of working through tradeoffs and one-off approaches to preserving data that is difficult to include in SIEM — such as high-volume data sources or historical data — security teams are increasingly taking a different approach centered on data needs. The foundation of the modern SIEM must accommodate any and all data, thereby allowing security teams to break down silos. **The modern SIEM enables security teams to search at scale** across massive amounts of any kind of data — whether it be traditional, non-traditional, or high-volume data sources — across a multilayered ecosystem with speed and accuracy. Once that foundation is in place, security teams can gain massive benefits for **operationalizing any security use case at scale** — monitoring and compliance, threat detection and prevention, hunting and incident response — while also addressing fraud, privacy breaches, and other priority issues that can put the business at risk. The key lies in the ability of security operations teams to **collect, analyze, visualize, and act on security insights in a unified manner**.

How your SOC benefits from a unified approach

A unified approach presents security teams with a number of advantages. A single data store, with powerful data security, data processing, and data visualization capabilities, provides the necessary context across distributed environments to extract valuable security insights from all your data. With the right security analytics — high-fidelity detections, validated machine learning jobs, and other out-of-the-box methods spanning on-premises and cloud — security teams can improve security posture, detect knowns and unknowns, and quickly respond to avoid damage and prevent future incidents. Strategically, **as dynamic changes occur, security teams can evolve quickly**. Practitioners can take on broader skillsets as they:

Leverage more context to better manipulate data and analyze tradecraft

Collaborate to uncover new research or implement new detections

Develop new visualizations and operating procedures

Profile threat actors and emulate adversarial behavior

More teams can take on hunt responsibilities. Strong platform-level integration capabilities can enable highly efficient procedures that simplify adapting to new classes of threats and emerging regulatory mandates.

With a unified approach, your SOC can solve complex security problems for a multitude of security functions, including threat hunting, SIEM, threat research, compliance, security monitoring and investigation, digital forensics and incident response, endpoint protection, antifraud, and more.

Holistic visibility

Collect security insights and include any data sources needed to drive to business-aligned outcomes.

Cloud scalability

Obtain necessary context from across the organization to verify threats, including years of historical context.

High SOC efficiency

Find the highest priority issues quickly and easily integrate with other tools and technologies for faster investigation and response.

Value for the entire security team

Security Engineer and Admin

- Centrally analyze logs, flows, and contextual data from across your environment — no matter how disparate your data sources
- Fast, federated search to quickly access and search across a complex, distributed environment
- Index and easily access high-volume data sources without exorbitant cost

Security Analyst

- Accuracy to detect complex threats faster
- Speed to accelerate response and efficiency
- Perform automated threat detection and minimize MTTD

SOC Manager

- Maintain a high level of awareness across the environment to improve security posture
- Avoid recurrences of known issues while identifying unknown issues
- Meet security KPIs without incurring high costs

elastic

Is your SIEM holding you back?

Today, security-relevant data can come from cloud services, network and user activity, endpoints, applications, connected devices, and many other sources. Many SIEM solutions trying to access all these data sources result in slow “coffee-break” analysis times or cost-prohibitive deployments.

Some SIEMs are built on separate data stores for different types of security analytics — one for machine learning, one for event-based correlations — leaving teams to archive data in yet another separate data store for threat hunting context or forensic evidence, and so on. As mentioned above, these silos cause inefficiencies in how teams share context, collaborate, manage cases, and respond to threats.

SIEM should help your SOC evolve faster, but many SIEM products do not provide the scale or flexibility to help security teams break down data silos or task silos, which result in investigative workflows that are limited by those silos. The result is operational silos that prevent security teams from moving faster, smarter, and more efficiently.

elastic

Common challenges in operational efficiency with traditional SIEM solutions include:

- Security data sources are not consolidated and reside in disparate data stores across the enterprise, making it challenging to have holistic visibility.
- Retention times are too short, forcing compromise for detections, investigative context, and threat hunting. Scoping breaches on attacks with longer dwell times is difficult.
- Security analysts lack adequate data sources needed to gain context about activity that may not indicate an advanced persistent threat, but is still very much a real threat to the business.
- SOC teams are not able to leverage machine learning tools unless they have in-house data scientists to develop models and skilled threat hunters to interpret context.
- Security engineers must make huge investments in data normalization projects and/or continually rearchitect their SIEM's underlying data fabric when they need to add new context-rich data sources (such as high-volume data). They must already "know" their data.
- Research teams spend inordinate amounts of time developing SIEM rules that are brittle and are not resilient to evasive techniques, and lack high-fidelity context from the right data.
- Tier 1-2 analysts spend too much time chasing down alerts that result in dead ends or require retrieving additional context from other data stores, causing delays and inefficiencies.
- Developers spend most of their time troubleshooting integrations or trying to stay abreast of vendor updates.

Get better protection using a modern SIEM

A modern SIEM can access all security data — regardless of size, scale, or location. With visibility into the entire environment, security teams have access to rich context and historical lookback periods needed to better detect and respond to threats faster and with better accuracy to prioritize threats.

Access to any and all data

Real-time and historical insights

Achieve max SOC velocity

Gain operational efficiency with Elastic Security as your SIEM

Security teams are managing a growing amount of data and need to be able to search, analyze, and perform automated detection across all of it, quickly and accurately. Response to modern threats requires instant correlation for effective investigative work, hunting, threat profiling, and more across traditional security data, cloud infrastructure, application data, and years of historical data.

Security teams use Elastic Security to access consolidated data, contextualize findings with threat and business context, and use historical data to quickly find the best resolution path. Elastic Security solves for SIEM, endpoint security, threat hunting, cloud monitoring, fraud detection, and many other use cases so your SOC can leverage the power of search and visualization to protect the organization with a unified approach to threat detection, prevention, and response.

Work smarter with Elastic Security

Gain holistic visibility

Collect Elastic Common Schema-normalized data with Beats and index all security-relevant data to eliminate data silos across the organization. Interact with intuitive out-of-the-box dashboards and develop drag-and-drop custom visualizations that fit your needs with Kibana, Lens, and Canvas.

Get security insights, fast

Ingest data using both schema on write and schema on read formats, for optimal query performance and the flexibility to add or change fields after ingestion. Bring results into dashboards in seconds with the speed that the Elastic Stack is known for. Crush alert fatigue with prioritized correlations.

Include years of historical data

Leverage searchable snapshots to cost-effectively tap into as much security data as you need for inclusion in detections, investigative context, threat hunting, cloud monitoring, and more. Scope breaches with dwell times of months or even years.

Reduce dwell times

Automate detection with MITRE-mapped out-of-the-box detections, developed by Elastic's internal security research team, and custom detections that leverage the powerful and intuitive Event Query Language (EQL) to perform correlations that detect tools, tactics, and procedures of advanced threats.

Find malicious anomalous activities

Apply unsupervised machine learning jobs to any data source with a timestamp to identify standalone anomalies or associated anomalies that constitute a potential threat. Combine supervised and unsupervised machine learning to detect methods such as domain-generating algorithms (DGAs) with low false-positive rates.

Streamline SecOps workflows

Use Elastic Security's interactive workspace to detect and respond to threats, triage events, and gather evidence on an interactive, intuitive timeline. Leverage built-in case management and integration with major security orchestration, automation, and response (SOAR) and workflow vendors to accelerate response and resolution.

Implement the modern SOC

Elastic Security serves as the technology foundation of modern security teams everywhere. Elastic's open platform approach to security enables ease of integration, flexibility, and the power of leveraging community-driven contributions and collaborations to help SOC teams evolve quickly and make better, faster decisions.

Conclusion

As security teams protect their organizations against an ever-expanding security landscape, they must not lose sight of the need to stay operationally efficient. With access to all security-relevant data and cost-effective methods to access historical data, you can solve more use cases by deploying Elastic Security as your SIEM and increase the operational value of your SIEM deployment overall. Leading **security teams are choosing Elastic Security as their SIEM because they need a unified approach to detection, prevention, and response**.

Elastic provides holistic visibility across the entire environment with speed and efficiency to identify and resolve issues, offers cloud scalability across your entire hybrid environment, and enables your SOC to reach maximum efficiency regardless of how distributed teams are or how many silos they operate within today. Keep your business protected with a new approach to SIEM with Elastic Security.

Want to check out Elastic Security for yourself?

Try Elastic Security on Elastic Cloud (14 days free, no credit card required).
Or, deploy it on-prem, where it's always free.

Start Elastic Security free ⟶

Search. Observe. Protect.

Elastic makes data usable in real time and at scale for enterprise search, observability, and security. Elastic solutions are built on a single free and open technology stack that can be deployed anywhere to instantly find actionable insights from any type of data — from finding documents, to monitoring infrastructure, to hunting for threats. Thousands of organizations worldwide, including Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia, and Verizon, use Elastic to power mission-critical systems. Founded in 2012, Elastic is publicly traded on the NYSE under the symbol ESTC. Learn more at elastic.co.

AMERICAS HQ
800 West El Camino Real, Suite 350, Mountain View, California 94040
General +1 650 458 2620, Sales +1 650 458 2625

info@elastic.co