exabeam®

Ultimate Guide to Cloud-native SIEM

Transition SIEM to the cloud

eBook

Table of Contents

Table of Contents

Table of Contents

Introduction

Over the last 20 years, the workload of security information and event management (SIEM) solutions has evolved dramatically. While additional scope has made SIEM platforms more powerful, it has added complexity that is beyond the capabilities of many security operations teams who need to effectively detect, investigate, and respond to the threats.

Cloud-native SIEM dramatically simplifies deployment and management, and increases ease of use, speed, and detection accuracy. Cloud-native SIEM is also highly scalable, efficient, and cost effective. As organizations grow, merge, and evolve, cloud-native security solutions can offload the costs of hardware and maintenance from IT teams and simplify operations for security engineers and analysts, so they can focus on delivering the best possible threat detection, investigation, and response (TDIR).

Cloud-native SIEM, in conjunction with sophisticated market-leading behavioral analytics, finds threats missed by other tools. Cloud-native SIEM lets you easily bring in logs and feeds from anywhere on-premises or in the cloud — even from new third-party vendors. Full indexing at the point of log ingestion in the cloud means queries return results faster. This, in turn, increases analyst productivity and efficiency, because analysts aren't left waiting for information indicative of a potential data breach or attack.

Many companies today are evolving their infrastructures toward the cloud, adopting SaaS applications such as Office 365, Salesforce, Google Workforce, and many others. Keeping data from this new class of infrastructure in the cloud lessens the workload and data management expense, and simplifies the protection of data (cloud to cloud). In this context, using cloud-native SIEM as the foundation of your security operations is a business decision that will produce payback on multiple fronts.

This guide defines SIEM and cloud-native SIEM, outlines the benefits and potential disadvantages of each, reviews different hosting models, explores a number of use cases, and discusses how to migrate from an on-premises to cloud-native SIEM.

What does a SIEM solution do?

SIEM solutions use rules and statistical correlations to turn logs, events, feeds, and telemetry from security systems into actionable information. This information can help security teams detect threats in real time, manage incident response, perform forensic investigation on past security incidents, and prepare audits for compliance purposes.

SIEM plays a central role in security operations monitoring, alerting, threat detection, and managing compliance. As data volumes, exposure points, third-party alerts, and the cost of talent and storage have multiplied, the speed of SIEM innovation has not kept up. Every sensor, detection product, or feed required to enable security use cases in a SIEM drives the collection of more data, often into terabytes per day. As the amount of data increases and the window of opportunity to detect and investigate attacks decreases, defenders are left vulnerable if they don't know what to look for. Unfortunately, most traditional on-premises SIEM products offer limited analytics, speed, and scalability. Organizations today need a better approach.

What is cloud-native SIEM?

Cloud-native SIEM solutions unify security monitoring into a single cloud-based location. Cloud-native SIEM also exploits the cloud's speed and economies of scale to grow and take advantage of innovations with less disruption. Organizations can leverage cloud-native SIEM technology to gain better visibility into distributed workloads. Cloud-native SIEM can help monitor all assets, including servers, devices, infrastructure components, and users connected to the network — through a single cloud-based dashboard.

Why cloud-native SIEM is needed

Since their inception in 2005, SIEM solutions have evolved into expensive, monolithic enterprise infrastructures built on proprietary software and custom hardware provisioned to handle the large data volumes they ingest and analyze. But legacy SIEM solutions weren't built for today's data volumes or security challenges. Nor were they built to identify compromised credentials. This has resulted in a SIEM effectiveness gap:

- Attacks are becoming more sophisticated and harder to detect.
- Compromised credentials are the key access point, but investigating user behavior, such as lateral movement and privilege escalation, is resource intensive, delayed, and inconclusive.
- Most SIEM solutions leverage generic log management capabilities. Security context is not added to ingested data in motion and must be added to data at rest.
- Many SIEM products encourage collecting all the data — not just the right data. Not only is this expensive, but it results in SIEM analysts buried in alerts with limited context, and this impedes the effectiveness of most investigations.
- Most legacy SIEM products use specialized or proprietary query languages requiring advanced knowledge to operate. So, few users can fully realize the power of these complex products.
- Resources for security teams are limited and talent is specialized, hard to find, and expensive.

While no solution can prevent all attacks, some can detect intrusions and malicious activity better than others. Often, the effectiveness of a SIEM solution is limited due to a lack of specialized expertise, limited analytics, or the high cost to maintain and analyze all the data collected. Combating these challenges requires a system equipped with pre-built rules, behavioral detections, automated timelines, and suggested steps for a thorough security investigation.

Cloud-native SIEM solutions use a modern architecture that is more affordable, easier to implement, and helps security teams discover real security issues faster:

- **Modern data lake technology** — offering big data storage with unlimited scalability, low cost, and improved performance
- **Dynamic scalability and predictable costs** — SIEM administrators no longer need to meticulously calculate sizing and make architectural changes when data volumes grow. SIEM storage can now grow dynamically and predictably when volumes increase. Advanced reporting capabilities help cloud-native SIEM users better forecast their consumption or map their ingestion to use case coverage.
- **Enrich data with context** — This is essential to filter out false positives in the SIEM solution to analyze data and be able to effectively detect and respond to real threats.
- **New insights with user and entity behavior analytics (UEBA)** — Modern SIEM offerings today include advanced analytics components such as machine learning and behavioral profiling, which go beyond traditional correlations to discover new relationships and anomalies across huge data sets.
- **Powering incident response** — Modern SIEM solutions leverage security orchestration, automation, and response (SOAR) technology that helps identify and automatically respond to security incidents and supports incident investigation by security operations center (SOC) staff.
- **Rapid delivery of advanced detections** — Management of product and detection updates is seamless with cloud-native SIEM. Updates to detect the latest threats can easily be provisioned with little or no end user action.
- **New managed hosting and management options** — Managed security service providers (MSSPs) are helping organizations implement SIEM, by running part of the infrastructure (on-premises or in the cloud), and by providing expertise to manage security processes.

Cloud-native SIEM solutions provide real-time monitoring, security events analysis, and security data logging for compliance, auditing, and tracking, all delivered as a cloud-managed solution. Cloud-native or SIEM as a service are increasing in popularity as they offer the opportunity to simplify deployment and reduce the time to implement, manage, maintain, and scale SIEM solutions. It also reduces licensing complexity compared to on-premises solutions.

For most organizations, cloud-native SIEM solutions are the best option. Companies use SIEM solutions to identify potential security vulnerabilities and threats before they can disrupt business operations and for daily security and compliance management. Cloud-native SIEM solutions aggregate security data into a single pane of glass and provide a comprehensive view of the security state across your tool stack and protected resources. Cloud-native SIEM can surface user behavior anomalies, using machine learning and artificial intelligence to identify normal versus abnormal user or entity behavior to reduce business risks and help automate threat detection and incident response processes.

Cloud-native SIEM features and capabilities

Cloud-native SIEM can help organizations quickly and easily centralize and collect event data from multiple sources, including on-premises and cloud assets. This is especially beneficial for hybrid deployments, which need to combine information on activities and events occurring in multiple data centers.

Key features provided by cloud-based SIEM solutions

Monitoring — Cloud-native SIEM platforms centralize monitoring efforts into a single user interface that displays information about integrated systems, workloads, and applications. They can aggregate data from physical and virtual components located in all environments, including multiple clouds, cloud applications, and on-premises data centers.

Alerting — A cloud-native SIEM platform aggregates and analyzes security data, generating meaningful, real-time alerts that notify analysts about security incidents.

Managing — Cloud-native SIEM aligns with the shift to the cloud model, simplifies cloud data collection, and lets organizations own, manage, and upgrade less infrastructure.

Automating — Advanced cloud-native SIEM solutions offer automation capabilities, including automated analysis of security incidents based on AI algorithms, and automated incident response and security orchestration.

Attack timelines — A cloud-native SIEM platform provides the ability to automate powerful visualizations that highlight events in a histogram.

Cloud-native versus on-premises SIEM

When you implement SIEM, you can deploy the solution as a service running in the cloud or on-premises. A cloud SIEM provider will manage the provisioning and often help with initial configuration — or offer expert professional services to speed deployment, which allows you to start operations immediately. Assuming you have already sized and sourced the infrastructure components, an on-premises implementation requires in-house installation and configuration, so it will likely take longer. Some other advantages of cloud-native SIEM are effortless updates for upgrades and new detections, and fewer limits on storage (and thus lower long-term storage costs). The sum of these should lead to lower total cost of ownership (TCO).

- **IT resources** — In-house IT teams can be short on staff (two-thirds of companies have an IT skills shortage), so it is important to consider giving in-house teams fewer responsibilities. Cloud-native SIEM allows you to outsource expertise to maintain security.
- **Control** — An on-premises implementation can offer more localized control, which may be necessary for some restricted or regulated data. However, the maintenance burden is much higher and often unrealistic for many organizations.
- **Cost** — The overall cost of implementation can vary widely for cloud-native SIEM, as there are lower upfront costs, but ongoing subscription costs. Cloud-native SIEM enables scalability and performance but requires thoughtful usage, especially when running resource-hungry workloads. On-premises SIEM tends to have higher upfront costs, with the technical debt paid over time. However, upgrades and expansions can drive up cost and expense through managing and deploying additional hardware. On-premises deployments also include additional downtime associated with upgrades.
- **Migration and data-in-transit** — Organizations moving sensitive data offsite always face risks associated with data-in-transit security and may also be exposed to compliance risks. However, most cloud-native SIEM vendors provide security measures, such as data encryption and strong authentication, that can mitigate these risks.
- **Limited access to raw log data** — Even though data comes from the organization's endpoints and systems, some cloud-native SIEM vendors might limit access to this information if you have not paid for the storage space. In these instances, the vendor provides aggregated reports based on the collected data. It is critical to select a vendor that uses a data lake architecture, which allows your organization to maintain its raw log data, making it available for forensic analysis and audits.

Strategic benefits of cloud-native SIEM

Massive scale

In the past decade, networks have grown, and the number of connected devices has exploded. Digital transformation has led to a similar explosion in the volume of data. In addition, there is a growing need to have access to all historical data — not just a filtered, summarized version of the data — to enable deeper analysis.

On-premises SIEM solutions rely on storage deployed in the data center, making it difficult and expensive to store and manage large data volumes. A common result of this is that a subset of log data gets analyzed. Cloud-native SIEM leverages elastic compute and modern data storage that allows massive scale at a fraction of the cost. This makes it possible to retain and analyze more log data across even more platforms and systems. In addition, cloud-native SIEM allows organizations to better integrate event data from on-premises infrastructure and cloud-native assets. A combined view of activities and events is particularly important in hybrid cloud deployments.

Global companies may have data lakes distributed around the world and need to keep data local for privacy or legal governance. Cloud infrastructure and robust identity and login controls make it easy to determine what security metadata will be shared globally in a distributed environment — including data masking (where required) and role-based access controls to ensure compliance.

Fast deployment

With on-premises SIEM, the deployment process to fully functional systems is time consuming. On the other hand, cloud-native SIEM allows organizations to customize and deploy the solutions faster. Without any hardware to request, set up, or manually maintain and upgrade, the speed of deployment is increased substantially. Cloud-native SIEM provides security operations teams an advantage in automated TDIR. Pre-built connectivity and integration with the leading security and IT tools and cloud infrastructures eliminates the difficult chore of data ingestion. Rapid automated development of new data sources and parsers reduces human error while empowering analysts with greater visibility, broader use case coverage, and improved threat detection.

Faster value, lower barriers

Legacy SIEM solutions are rife with complexities that demand expensive, highly trained personnel and extensive professional services to design, deploy and update. Today's cloud-native SIEM solutions are designed to be simple to deploy and operate, delivering the simplicity and functionality lacking in most legacy platforms that suffer from years of scope creep, add-ons, and custom extensions. Using cloud-native SIEM, organizations can deploy more quickly and easily, and access up-to-date functionality by simply connecting to the internet and signing in. This instant, easy access saves time and effort, and eliminates the need for extensive use of professional services. Security operations teams can adopt a SIEM more quickly and recognize the value immediately. There is no need to employ multiple SIEM engineers for constant tinkering of indicators of compromise (IoCs) and events of interest. Tuning rules, and configuring log parsers and APIs all take time, and often days of negotiation with the SIEM vendor and third-party customer service teams.

Reduced TCO

On-premises solutions require a significant investment in hardware and software that, in some cases, may become obsolete. The transition from CAPEX to OPEX is well understood and allows for faster time to value. The speed at which you can connect disparate security logs, events, and metadata from other feeds defines how quickly you can get up and running for a comprehensive monitoring program. Adding to this is the cost of the number of people needed to maintain, operate, and evolve the system to reflect the changing needs of the security operations team. Setup and maintenance are just the start. SIEM TCO should take into consideration the mean time to detect and respond to incidents and to automate repeatable tasks such as triage, as well as other efficiencies gained by moving to the cloud.

Automated updates and improvements

On-premises SIEM requires significant management and upkeep; staying up to date with new technologies, log feed changes, product updates, and tuning rules all have adverse effects on your ability to quickly detect, investigate, and respond to threats. SIEM engineers are constantly looking at the latest releases and evaluating whether they can or should update, how fast, and when.

With cloud-native SIEM, the onus is on the vendor to keep things updated and push new features and detections. New updates and improvements are delivered continuously (remembering the last zero-day exploit drop). Rollouts are faster, automated, and consistent across every instance and tenant in the cloud. As new detections, playbooks, and incident response checklists become more turnkey in your organization, you can add new versions on the fly and tailor existing use cases to your needs.

The cloud also lets you keep pace with your threat intelligence feeds, allowing automatic updates of new known malicious IPs, domains, TOR endpoints, and other potential IoCs.

Near-real-time threat detection

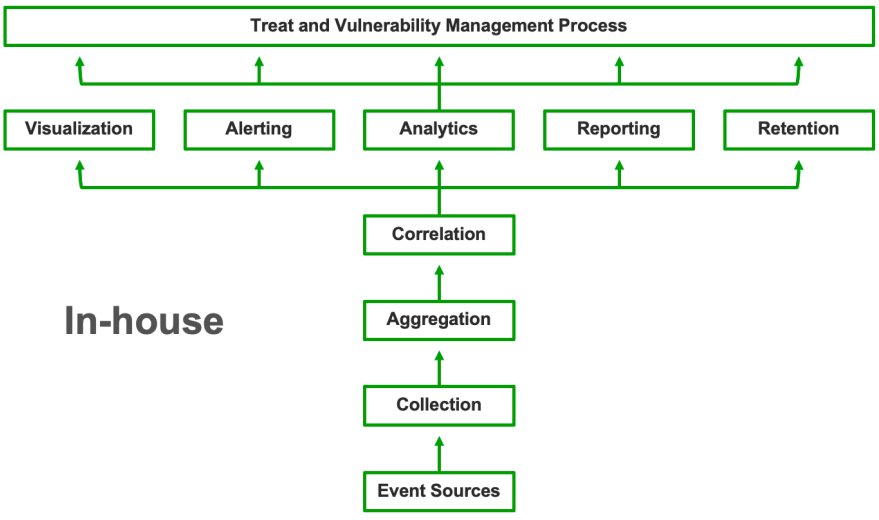
With a modern, cloud-native SIEM, threats can be detected in near-real time with minimal traffic overhead and unlimited processing power. Ingested data and logs can be enriched with context data as they are fed into the SIEM, then quickly analyzed. With traditional SIEM, detection analysis is often delayed until traffic flow is less demanding on the solution. With cloud-native SIEM, security intelligence data is integrated into a unified view. Rapid, guided search boosts productivity and ensures immediate data access — exactly when it's needed.

Which cloud-native SIEM hosting model is right for you?

SIEM integrations

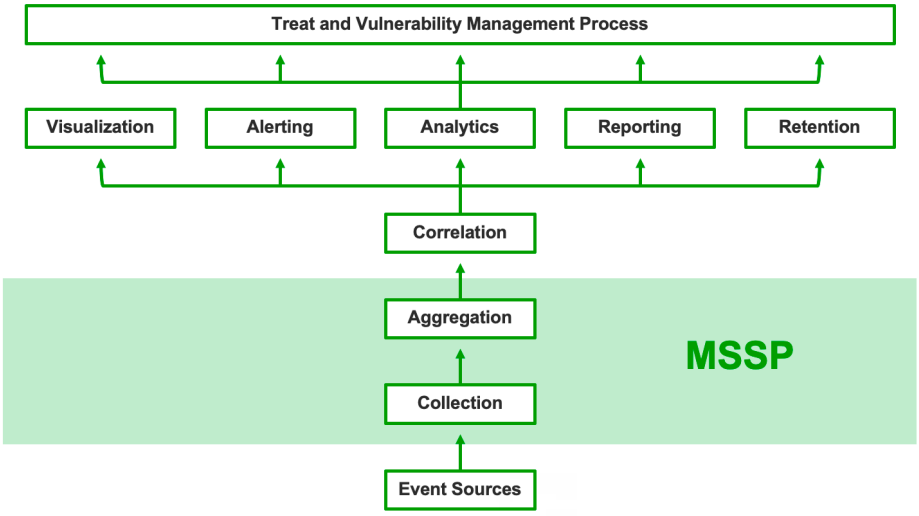
The following four SIEM models illustrate the responsibilities that fall to your organization and to the MSSP or vendor you might select for your cloud-native SIEM, depending on the model you choose.

Self-hosted, Self-managed



This is the traditional SIEM deployment model: host the SIEM in your data center, often with a dedicated SIEM appliance, maintain storage systems, and manage it with trained security personnel. This model made SIEM a notoriously complex and expensive infrastructure to maintain.

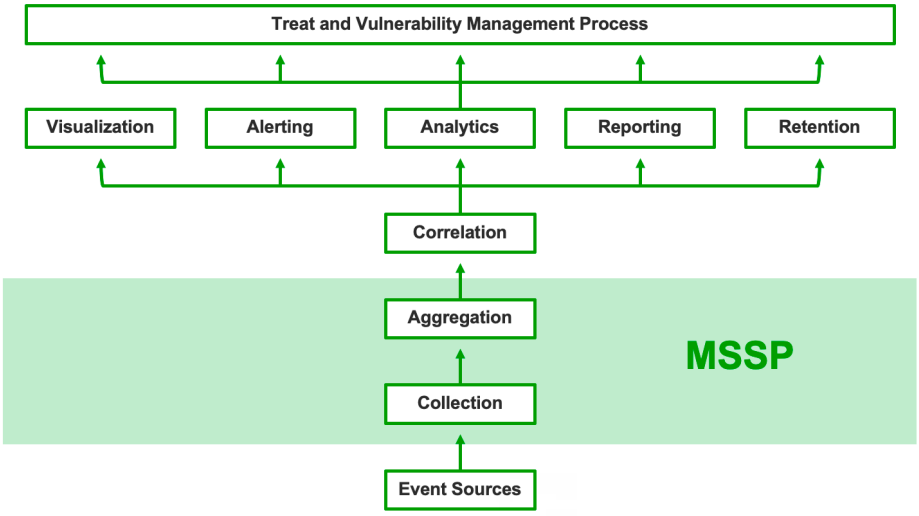
Cloud SIEM, Self-managed



MSSP handles: Receiving events from organizational systems, collection, and aggregation

You handle: Correlation, analysis, alerting and dashboard, security processes leveraging SIEM data

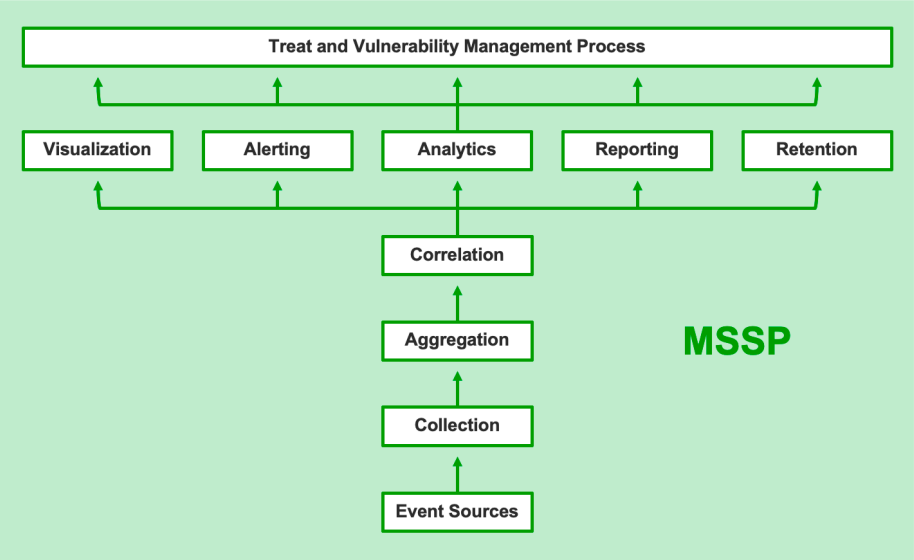
Self-hosted, Hybrid-managed



You handle: Purchasing software and hardware infrastructure

MSSP together with your security staff: Deploys SIEM event collection / aggregation, correlation, analysis, alerting, and dashboards

SIEM as a service



MSSP handles: Event collection, aggregation, correlation, analysis, alerting, and dashboards

MSSP together with your security staff: Security processes leveraging SIEM data

Which hosting model is right for you?

The following considerations can help you select a SIEM deployment model:

- Do you have an existing SIEM infrastructure? If you've already purchased the hardware and software, opt for self-hosted, self-managed, or leverage an MSSP's expertise to jointly manage the SIEM with your local team.
- Are you able to move data off-premises? If so, a cloud-hosted or fully managed model can reduce costs and management overhead.
- Do you have security staff with SIEM expertise? The human factor is crucial in getting true value from a SIEM. If you don't have trained security staff, rent the analysis services via a hybrid-managed or SIEM as a service model.

Cloud-native SIEM and international regulation compliance

Many organizations use manual processes and disparate security products to meet regulatory requirements, including the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and the Sarbanes-Oxley Act of 2002 (SOX).

These ad hoc processes leave organizations at risk for audit failure, fines, and disclosure reporting. Most cloud-native SIEM solutions provide detection rules, models, and compliance reports that show auditors that security controls are in place and work as designed.

Data residency

Many cloud-native SIEM solutions are available globally, so you can choose where your data is hosted and leverage cloud-native SIEM for TDIR while satisfying your data residency requirements. Some vendors deploy a multi-tenant cloud architecture by which each tenant is isolated and invisible to other tenants to protect the privacy of your data.

If your organization has data residency requirements, choose a cloud-native SIEM provider that can meet these requirements.

Focus on threat-centric use cases

Here are common cloud-native SIEM use case examples, from traditional uses, such as compliance, to cutting-edge use cases, such as insider threat detection and IoT security.

Compliance

PCI compliance

PCI DSS was created to secure credit cardholder data from theft and misuse. It defines 12 security areas in which companies should enhance protection for this type of data. The requirements apply to anyone involved in credit card processing, including merchants, processors, and third-party service providers.

Five ways cloud-native SIEM can help with PCI compliance:

1. **Perimeter security** — Detecting unauthorized network connections and correlating with change management, searching for insecure protocols and services, and checking how traffic is flowing across the demilitarized zone (DMZ)
2. **User identities** — Monitoring any event that results in changes to user credentials, and activity by terminated users
3. **Real-time threat detection** — Monitoring antivirus logs, monitoring insecure ports and services, and correlating with threat intelligence
4. **Production and data systems** — Searching for dev/test or default credentials, replicas, etc., on production systems
5. **Auditing and reporting** — Collecting system and security logs, including specific PCI logging requirements, auditing them in a format suitable for PCI reporting, and generating compliance reports

GDPR compliance

GDPR is Europe's framework for protecting security and privacy for personally identifiable information (PII), which came into force in May 2018. GDPR applies to any legal entity which stores, controls, or processes personal data for EU citizens. It focuses on two categories: personal data, such as IP addresses or usernames, and sensitive personal data, such as biometric or genetic data.

Five ways cloud-native SIEM can help with GDPR compliance:

1. **Data protection by design** — Verifying and auditing security controls to show that user data underwent appropriate treatment
2. **Visibility into log data** — Providing structured access to log information to enable reporting to individual data owners
3. **GDPR logging and auditing** — Monitoring critical changes to credentials, security groups, and so on; auditing databases and servers storing PII and automatically tracking assets that store sensitive data
4. **Breach notification** — Detecting data breaches, alerting security staff, analyzing the incident to uncover full impact, and quickly generating detailed reports as required by GDPR
5. **Record of data processing** — Identifying events related to personal data, auditing any changes to the data, and generating reports as required by GDPR

Warning:
The SIEM solution itself can represent a risk under GDPR, because log data might contain PII. GDPR permits retaining data for "legitimate interest" (Article 6), which may allow the retention of log files for security purposes. Consult with your legal counsel to understand what data you can or cannot retain in the SIEM under GDPR provisions, and work with your SIEM vendor to understand data masking and role-based access controls.

HIPAA compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a United States standard pertaining to organizations that transmit health information in electronic form. It applies to organizations of all sizes, from a single physician to national healthcare bodies. HIPAA's Security Management Process standard requires organizations to perform risk analysis and risk management, have a sanction policy for data breaches, and conduct information system activity reviews — a key element of the standard which ensures all the other parts are in order.

Nine ways cloud-native SIEM can help with HIPAA compliance:

1. Security management process — Discovering new IT assets; identifying systems at risk; monitoring access to system files, user activity, and privileges in critical systems
2. Employee access — Monitoring access to critical files and data, capturing login attempts and logins from terminated users
3. Information access management — Identifying logon success and failures, privilege escalation, and modification of user accounts
4. Security awareness — Detecting vulnerabilities and malware, detecting systems with no antivirus, monitoring logon to security devices and critical systems
5. Security incidents — Automatically detecting threats, generating alerts and prioritizing them, enabling threat investigation, and orchestrating automated response to incidents
6. Access control — Monitoring changes to credentials and permissions, session timeouts, and changes to encryption settings
7. Audit controls — Monitoring changes to policies, data loss prevention (DLP) events, file integrity, and log analysis for protected data
8. Data integrity — Monitoring modification of health information and changes to data policies
9. Transmission security — Identifying unauthorized communications and attempts to modify applications or storage containing health information

SOX Compliance

SOX is a regulation that sets requirements for US public company boards, management, and accounting firms. It was enacted as a reaction to several corporate accounting scandals, including Enron and WorldCom. Two frameworks commonly used by IT organizations to comply with SOX are COSO and COBIT.

The SOX regulation focuses on making sure an organization informs management, and is able to demonstrate, via SOX reporting procedures:

- Where sensitive data is stored
- Who has access to it
- What happened to it

SIEM can be helpful in gathering this data and recording it for SOX audits.

Five ways cloud-native SIEM can help with SOX compliance and audits:

1. **Security policies and standards** — Tracking information security policies (for example, an email security policy) and standards (for example, a standard way to secure Windows desktop machines), identifying which IT systems are in compliance with policies and standards, and alerting about violations in real time
2. **Access and authentication** — Monitoring account creation, change requests, and activity by terminated employees
3. **Network security** — Monitoring alerts from firewalls and other edge security devices, and identifying known attack patterns in network traffic
4. **Log monitoring** — Aggregating security events and alerting on invalid login attempts, port scans, privilege escalations, etc.
5. **Segregation of duties** — (The SOX standard requires that no one person controls an entire data process from start to end.) Ensure, for example, that data entry staff only access the data they are creating, and never view or modify other data.

Using SIEM for protection against trusted entities

Next-gen SIEM

Most of the capabilities in the following use cases are made possible by next-generation cloud-native SIEM solutions that feature UEBA capabilities. UEBA technology uses ML and behavioral profiling to establish baselines of IT users and systems and to intelligently identify anomalies. This goes beyond the rules and statistical correlations used by traditional SIEM solutions. Specifically, UEBA technology makes it possible to detect insider threats, perform more sophisticated threat hunting, prevent data exfiltration, and mitigate IoT threats, even when traditional security tools don't raise a single alert.

Insider threats

There is growing awareness of internal security threats, which can be categorized into three types:

1. **Malicious insider** – An individual who has authorized access to an organization's sensitive or confidential information and uses it to intentionally cause harm to the organization
2. **Negligent insider** — An individual who has authorized access to an organization's sensitive or confidential information and inadvertently causes harm to the organization due to carelessness, ignorance, or lack of proper training or supervision
3. **Compromised insider** – An individual with legitimate credentials who may have been coerced, bribed, or otherwise convinced to provide their access to an external entity who uses it to commit unauthorized or malicious acts

Cloud-native SIEM can help discover insider threat indicators via behavioral analysis, helping security teams identify and mitigate attacks.

Six ways cloud-native SIEM can help mitigate insider threats:

1. **Detecting compromised user credentials** — Using behavioral analysis to detect anomalous behavior by users, indicating a compromise, for example, logins at unusual hours, at unusual frequency, or accessing unusual data or systems
2. **Anomalous privilege escalation** — Detecting users changing or escalating privileges for critical systems
3. **Command and control communication** — Correlating network traffic with threat intelligence to discover malware communicating with external attackers. This is a sign of a compromised user account.
4. **Data exfiltration** — Using behavioral analysis to combine and analyze seemingly unrelated events, such as insertion of USB thumb drives or anomalous badge access, unusual system access, downloads or backups, use of personal email services, unauthorized cloud storage, or excessive printing
5. **Rapid encryption** — Detecting and stopping encryption of large volumes of data. This might indicate a ransomware attack, which often originates from compromised insiders.
6. **Lateral movement** — Detecting attack behavior, such as insiders attempting to switch accounts, machines, and IP addresses on their way to a target

Privileged access abuse

Privileged access abuse is a complex problem stemming from gaps in access control at organizations. Users with access to IT systems are able to perform undesirable actions, because they have more access rights than they need to do their jobs.

Five ways cloud-native SIEM can help stop privileged access abuse:

1. **Unwanted activity** — Monitoring and reporting on suspicious access to any sensitive data
2. **Third-party violations** — Monitoring activity by external vendors and partners who have access to organizational systems, to identify anomalous behavior or escalation of privileges
3. **Departed employees** — Alerting to any activity by terminated user accounts, or unexpected activity on accounts that are normally inactive
4. **Human error** — Alerting to anomalous activity that could be a disastrous human error, such as deletion of large quantities of data
5. **Overexposure** — Reporting on users who are accessing systems or data not within their regular usage profile

Trusted host and entity compromise

It is common for attackers to take control of user credentials or hosts within an organizational network, and carry out attacks stealthily for months or years. So a major goal for security teams is to detect and subvert attacks quickly.

Four ways cloud-based SIEM can help detect and stop trusted entity compromise:

1. **User accounts** – Identifying anomalous activity, alerting to it, and providing investigators the data they need to understand whether a privileged user account was breached
2. **Servers** – Creating a trusted baseline of server activity, detecting deviations from this baseline, and alerting security staff
3. **Network devices** – Monitoring traffic over time and detecting unusual spikes, non-trusted communication sources, insecure protocols, and other signs of malicious behavior
4. **Antivirus monitoring** – Looking at antivirus deployments broadly, reporting on events like protection disabled, antivirus removed, or status of threat updates

Using cloud-native SIEM for advanced security threat detection

Threat hunting

Threat hunting is the practice of actively seeking out cyberthreats in an organization or network. A threat hunt can be conducted on the heels of a security incident, but also proactively, to discover new and unknown attacks or breaches. Threat hunting requires broad access to security data from across the organization, which can be provided by cloud-native SIEM.

Seven ways cloud-native SIEM can help with threat hunting:

1. **Alerts from security systems** — Delivering actionable alerts that provide context and data to help investigate a potential incident
2. **Environmental anomalies** — Identifying anomalies using correlations and behavioral analytics
3. **New vulnerabilities** — Organizing data around a new vulnerability — timeline and systems, data and users affected
4. **Tips from peers or the media** — Searching historical data for attack patterns or signatures similar to known attacks
5. **Threat intelligence** — Combining threat intelligence with security data to intelligently detect attacks in IT systems, or searching for existing traffic or IoC within distributed security logs
6. **Hypotheses based on known risks** — Helping analysts frame a hypothesis and test it by exploring security data in the SIEM
7. **Similar incidents** — Checking if "this happened before" — searching security data for patterns similar to a current or previous security incident

Data exfiltration detection

Data exfiltration happens when sensitive data is illicitly transferred outside an organization. It can happen manually, when a user transfers data over the internet or copies it to a physical device and moves it off the premises, or automatically, as the result of malware infecting local systems.

Six ways cloud-native SIEM can help prevent data exfiltration:

1. **Backdoors, rootkits and botnets** — Detecting network traffic to command and control centers, and identifying anomalous communications and systems transmitting data to unauthorized parties
2. **FTP and cloud storage** — Monitoring network traffic over protocols that facilitate large data transfer and alerting when unusual quantities or file types are being transferred or when the target is unknown or malicious
3. **Web applications** — Monitoring usage of organizational web applications by outsiders or inside usage of external web applications, which might involve downloads or browser access to sensitive data
4. **Email forwarding** — Detecting emails forwarded or sent to entities other than the stated recipient
5. **Lateral movement** — Detecting lateral movement by applying behavioral detections and correlating data from multiple IT systems
6. **Mobile data security** — Monitoring data from the mobile workforce and identifying anomalies that might indicate information leakage via a mobile device

IoT security

Many organizations are using connected devices to manage critical operations. Examples include network-connected medical equipment, industrial machinery and sensors, and power grid infrastructure. Internet of Things (IoT) devices were not designed with security in mind, and many suffer from vulnerabilities. These vulnerabilities are difficult to remediate once the devices are deployed in the field. The first line of defense for IoT is often the service account controlling the system, which should be visible to your SIEM as part of log data.

Six ways cloud-native SIEM can help mitigate IoT threats:

1. **Denial-of-service (DoS) attacks** — Identifying unusual traffic from organization-owned IoT devices which might be leveraged by an attacker to perform an attack; applying automated responses to stop or block traffic based on certain conditions
2. **IoT vulnerability management** — Detecting old operating systems, unpatched vulnerabilities, and insecure protocols on IoT devices
3. **Access control** — Monitoring who is accessing IoT devices, what they connect to, and alerting when a source or target is unknown or suspicious
4. **Data flow monitoring** — Monitoring unusual data flows to and from IoT devices and alerting security staff
5. **Devices at risk** — Identifying devices at risk due to security vulnerabilities, access to sensitive data, or critical functions
6. **Compromised devices** — Identifying anomalous or suspicious behavior of IoT devices and alerting security staff that a device or fleet of devices has been compromised

Migrating to a cloud-native SIEM solution

Transitioning from an on-premises SIEM to one based in the cloud will touch many areas of your enterprise, so involving stakeholders is crucial. Foremost in this effort is protecting the organization's "crown jewels," whose compromise could result in considerable damage to the business. Examples include:

- Intellectual property (IP)
- Customer records
- Financial records
- Personnel records
- Systems running critical applications
- Networks
- Security devices

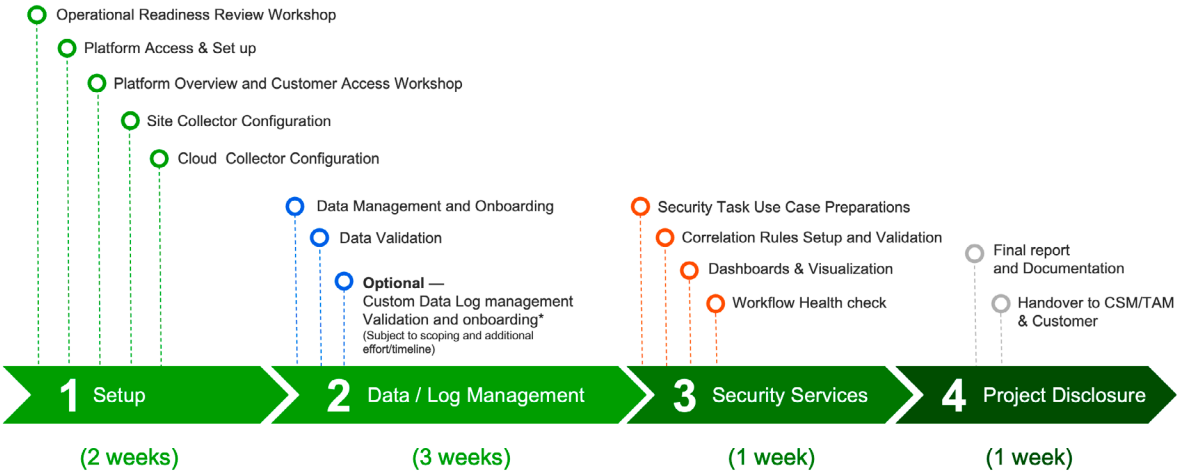
Your organization's risk management framework should guide setting priorities for transition, which might include compliance with pertinent industry guidelines, regulations, and statutes. We suggest you involve relevant executives and senior managers in this phase. These stakeholders will have a keen interest, because their job roles often are responsible for making IT drive business outcomes.

This transition does not necessarily require a wholesale replacement of the existing SIEM and can take a custom approach. It may suffice to augment your existing SIEM with cloud-native SIEM capabilities, such as behavioral analytics or automated response capabilities. Or perhaps a phased approach is better, which temporarily runs the cloud-native SIEM in parallel with your existing on-premises SIEM. A pending SIEM license renewal date may also affect your decision about when to decommission and cutover. You also need to consider the destination for your SIEM transition: partially on-premises, a public cloud, a hybrid cloud, or SaaS.

In our experience, the time of transition from legacy on-premises SIEM to cloud-native SIEM is typically seven to eight weeks.

Before you start the transition process, your security operations team should review their current goals for the SIEM, rules, data sources, use cases, reporting needs, user access, etc. The project timeline may increase in line with your specific requirements, such as unsupported log sources, unsupported log formats, and scoped custom work.

Project plan



Transition steps

Step 1: Setup (estimated two weeks to complete)

Operational Readiness Review workshop

To prepare for the transition, conduct an operational readiness review (ORR) to help translate security goals into operational outcomes and tasks necessary to achieve them. The ORR should validate the scoped service deliverables and technical scoping to ensure a successful production deployment from the beginning. The ORR should also discover information necessary to guide adoption efforts.

Platform access and setup

The platform access and setup step of the deployment is where your deployment engineer gains access to the system and ensures that licensed applications are operational and available for your use. This is typically followed by a workshop introducing your SOC to the applications and their operation.

Cloud connector and/or site collector configuration

The cloud collector and/or site collector configuration steps of the deployment build upon the deployment prerequisites by configuring logging infrastructure such as the site collector and cloud collectors to ingest from SaaS solutions that might include AWS, Azure, Box, Cisco AMP, CrowdStrike, Dropbox, Duo, G-Suite, GitHub, Office 365, Okta, OneLogin, Proofpoint, Salesforce, ServiceNow, and many others.

Step 2: Data/log management (estimated three weeks to complete)

Data management and onboarding

During the data management and onboarding phase of the deployment, logs begin flowing into the system. As scoped data sources are ingested, your vendor's engineers should validate that the log sources are parsing as expected, that parsed fields are parsing and accounted for, and that the cloud-native SIEM has a healthy data pipeline.

Step 3: Security services (estimated one week to complete)

Security task use case preparations

Review the ORR to understand your security expectations in preparation for following security tasks:

Correlation rule setup and validation

Based on the ORR, implement custom pre-defined correlation rules to give your SOC an understanding of the platform's capabilities and end-user workflows. Many cloud-native SIEM vendors offer pre-built correlation rules and models matching some of the most common use cases of malware and compromised credentials.

Dashboard and visualization

Check to ensure prepackaged dashboards and visualizations are working as expected. They should allow you to print and export, and help with search, visualization, and security operations. With most cloud-native SIEM solutions, organizations can create their own dashboards specific to their needs, and dashboards can be exported as PDFs to support reporting requirements.

Workflow health check

Validate that correlation outcomes and security alerts are populating where they should be.

Step 4: Project closure (estimated one week to complete)

Final report and documentation

The final step in the deployment process generally is to create and deliver a final report as part of the deployment project closure meeting. This report should highlight the deployment tasks completed and configurations implemented.

Post-transition activities

We recommend security operations teams run instances of the cloud-native SIEM and the legacy on premises SIEM in parallel for at least 30 days to ensure quality assurance and validation. We also recommend you review your case outcomes at the end of the implementation to understand and improve your use case coverage.

Prepare reports for compliance and KPIs

One of the last steps in preparing for your transition to your cloud-native SIEM entails report preparation. Setting up comprehensive reporting to address selected use cases, compliance mandates, and KPI reports will position you to meet and comply with any necessary KPIs and reports. These might include vendor-specific reports (for example, for Cisco, Symantec, or a VPN vendor) and compliance reports (for example, for PCI, HIPAA, NIST, etc.).

Transition detection rules

Once the transition is complete, users need to write search queries. In order to execute these queries your analysts may need some or all of the following skills:

- Knowledge of syntax
- Knowledge of logic and thus query combinations available
- Knowledge of use cases
- Knowledge of data sources
- Knowing how to get help when you're stuck

Additional considerations when evaluating cloud-native SIEM

1. Where is the solution delivered from and where is my data stored?
2. How is my data protected?
3. Does the solution provide the scaling and ease of management benefits of a true SaaS model?
4. How is my data collected and transported to the SIEM?
5. What is the expected impact on network or internet links?
6. How does the vendor balance the cadence of feature and function upgrades with adequate testing to ensure availability and quality?
7. How does the vendor support security technologies that are part of their platform?
8. Is the licensing and pricing model consumption based? Is there transparency in usage and is it easy to adjust?
9. How does the vendor ensure availability of the SIEM solution? How does it see the health of the log sources and parsers?
10. What happens at the end of the agreement? Do you own your data and is it accessible to you?

New-Scale SIEM™ from Exabeam

New-Scale SIEM is cloud-native SIEM at hyperscale with fast, modern search and powerful correlation, reporting, dashboarding, and case management. It includes a breakthrough set of capabilities security operations teams need in products they will want to use. New-Scale SIEM delivers:

- **Cloud-scale security log management** — Pull data from all sources, including context; easily ingest, parse, store, search, and present more of the right data from everywhere. Get instant results over petabytes and years of data.
- **Powerful behavioral analytics** — Establish a baseline of normal behavior with histograms, and detect and prioritize unusual events. Stay ahead of threats by detecting insiders as they move throughout the organization with built-in awareness of adversary tactics, such as aligning with the MITRE ATT&CK® framework.
- **Automated investigation** — Get a full picture and resolve incidents faster by automating investigations and response actions. Smart Timelines™ reconstruct the chain of incidents to find out what really happened. Analysts can recapture two-thirds of their time on detection, triage, and investigation.

Cloud-scale security log management

Exabeam SIEM securely collects data from on-premises or cloud data sources at scale using a single interface. Raw logs are parsed into security events, and named fields are identified and normalized using a standard format for accelerated analysis and added security context. A wizard enables custom parser creation from new or templated log sources making it easy to develop, deploy, and manage error-free parsers. Exabeam cloud-native SIEM processes events at a sustained rate of more than one million per second.

- Support for 200+ vendors and 500+ products
- Multiple transport methods: API, agent, syslog, SIEM data lake
- 34 cloud-delivered security products
- 11 SaaS productivity applications
- 21 cloud infrastructure products
- 9,000+ pre-built log parsers

Exabeam Security Log Management leverages a cloud-scale architecture to ingest, parse, store, and search data at lightning speed. An essential capability of Exabeam SIEM is Search — a single interface that allows analysts to search data at lightning speed. And there's no learning curve; analysts don't need to learn a proprietary query language. Create correlation rules and powerful visualization from your parsed log data quickly. Build a dashboard in a minute from 14 different pre-built chart types.

Exabeam extends the cloud-scale capabilities of Exabeam Security Log Management with additional features for TDIR. Exabeam SIEM includes Alert and Case Management, more than100 pre-built correlations, integrated threat intelligence, and powerful dashboarding capabilities. The solution delivers analysts new speed and multi-year search capability for query responses across petabytes (PB) of hot, warm, or cold data in seconds.

Cloud-scale visibility

Drive desired security outcomes to close critical gaps by understanding your data source coverage and configuration. Learn precisely what to do to improve your security posture by seeing recommended information, event streams, and parsing configurations. Exabeam cloud-native SIEM is a powerful and affordable log management solution, purpose-built for security, that your teams will want to use — and that doesn't require a massive learning curve.

Advanced correlation capabilities

Exabeam cloud-native SIEM turns your searches into powerful threat-hunting rules in one click. The solution's Correlation Rules app enables you to surface a broad range of behaviors and events. It enables your analysts to write, test, publish, and monitor custom correlation rules, including defining higher criticality for those that correspond to Threat Intelligence Service-sourced or other key context activity.

Alert and Case Management

A defining feature for a SIEM is the ability to sort alerts by severity and combine them into cases and incidents to be worked through to resolution by your analysts. Alert and Case Management centralizes events and alerts sourced from Exabeam and/or third-party products, letting an analyst review alerts individually or at volume — or set conditions to automate the alert triage workflow and escalate events and alerts into incidents. Alert and Case Management allows analyst teams to create incidents, add tags and events to the incident, collaborate across groups and timezones, and offers customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution, including APIs into outside ITSM systems.

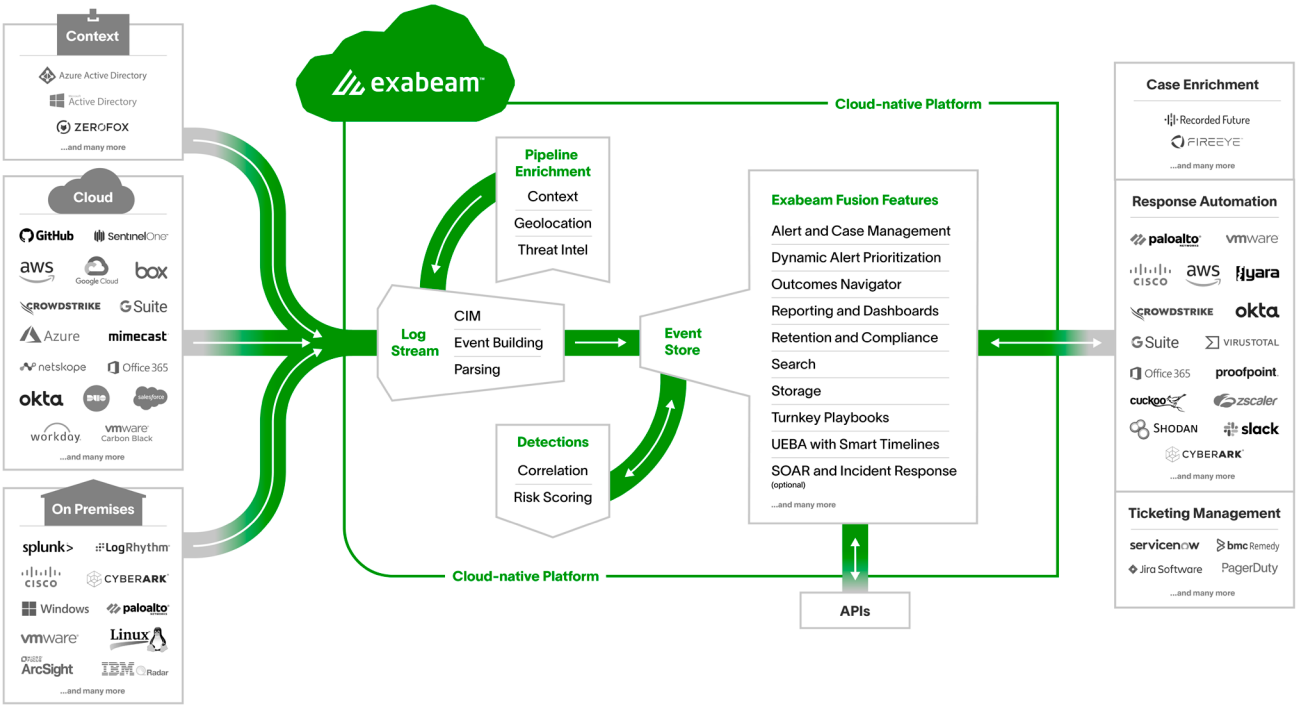
Behavioral analytics

New-Scale SIEM offers industry-leading UEBA that baselines the normal behavior of users and devices with histograms to detect, prioritize, and respond to anomalies based on risk. Understanding normal allows you to detect the behaviors, such as lateral movement, privilege escalation, credential swapping, and more, that are missed by other tools.

Automation

New-Scale SIEM offers automation across the TDIR workflow. Built-in timelines reconstruct the chain of events across all log sources, enriched with relevant context as well as scripted response actions allowing analysts to quickly see and act on meaningful alerts — recapturing two-thirds of the time an analyst spends on detection, triage, and investigation.

How it works



Get started with Exabeam

Whether you replace a legacy SIEM or complement a less effective SIEM solution by adding UEBA, automation, and TDIR content on top, the modular Exabeam Security Operations Platform makes it easy to achieve security operations success.

Exabeam Security Log Management

Exabeam Security Log Management is the industry's most advanced cloud-native solution in support of security use cases. The product represents the entry point to ingest, parse, store, and search security data in one place, providing a lightning fast, modern search and dashboarding experience. Exabeam Security Log Management delivers affordable log management at scale without advanced programming, query-building skills or lengthy deployment cycles.

SIEM replacement with Exabeam SIEM and Exabeam Fusion

Exabeam extends the cloud-scale capabilities of Exabeam Security Log Management with additional features for TDIR. Exabeam SIEM includes Alert and Case Management, more than 100 pre-built correlations, integrated threat intelligence, and powerful dashboarding capabilities. The solution delivers analysts new speed, processing at a sustained rate of more than 1M EPS.

Exabeam Fusion represents the industry's most powerful and advanced cloud-native SIEM and introduces New-Scale SIEM. It unites the combined capabilities of all Exabeam products: cloud-native data storage, rapid data ingestion, hyper-fast query performance, powerful behavioral analytics, and orchestration and automation that changes the way analysts do their jobs.

SIEM augmentation with Exabeam Security Analytics and Exabeam Security Investigation

Exabeam Security Analytics was designed to upgrade an organization's defenses and detect sophisticated and credential-based attacks. As the only UEBA product that can run on top of a third-party SIEM or data lake, Exabeam Security Analytics ingests, parses, and normalizes data using a common information model. Exabeam Security Analytics UEBA capability baselines normal behavior for users and devices to highlight anomalies and assigns a risk score to each notable event.

Exabeam Security Investigation combines content, workflows, and automation with UEBA to provide outcome-focused TDIR capabilities to ineffective SIEM. As another Exabeam product that works on top of a third-party SIEM or data lake, Exabeam Security Investigation helps teams standardize around TDIR best practices. Exabeam Security Investigation includes prescribed workflows for ransomware, phishing, malware, compromised insiders, and malicious insiders, with pre-built content focusing on specific threat types and attack techniques.

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now →