Splunk to Exabeam Transition Blueprint

Organizations use a security information and event management (SIEM) platform because it's a critical, necessary component of a multilayered security control infrastructure

In a large enterprise, security and IT system logs and other inputs can easily reach millions of events every day requiring terabytes of daily log storage. As organizations embrace the cloud and consider monitoring their IoT devices, this event volume continues to rise. No longer is the Splunk approach of logging everything practical. This mindset adds to the cost of operating a SIEM, and introduces productivity challenges for security operations teams. As the number of cyberattacks and breaches rise, the performance of legacy SIEM products, such as Splunk, are under scrutiny because they lack an outcomes-based approach, and their inability to automate across the entire threat detection, investigation, and response workflow.

The cost, complexity and limited capabilities of Splunk requires "experts" to perform the most basic tasks. The combination of these make Splunk an expensive solution to both own and operate. For these reasons, many enterprises are re-evaluating their reliance on Splunk as a SIEM and migrating to more modern offerings. Migrating any SIEM is no trivial task — this white paper outlines the transitions steps to put your organization on a path to success. The paper also includes the benefits resulting from migrating to the Exabeam Security Operations Platform as you look to reduce costs, and improve productivity, and increase the speed of threat detection, investigation, and response (TDIR). Our guidance is aimed toward business leaders, security leaders, and other stakeholders to help ensure a successful collaboration.

What creates a SIEM effectiveness gap

- Most SIEMs leverage generic log management capabilities. Security context is not added to ingested data in motion and needs to be added to data at rest.
- Resources for security teams are limited and talent is hard to find. Organizations using most SIEM products must recruit specialized, hard to find and expensive talent
- Most legacy SIEM products use specialized or proprietary query languages. This requires advanced knowledge to operate. Because of the specialization required, few users can fully realize the power of these products because of the complexity involved.
- Attacks are only becoming more sophisticated and hard-to-detect
- Compromised credentials are the key access point — investigating user behavior like lateral movement, and privilege escalation is resource intensive, delayed, and inconclusive.
- Many SIEM products encourage you to collect all the data — not just the right data. This turns out to be inactionable and expensive.
- Most SIEM analysts are buried in alerts with limited context — limiting the effectiveness of most investigations

While no tool can prevent all attacks, some can detect intrusions and malicious activity better than others. Far too often, the effectiveness of your security information and event management (SIEM) solution is limited due to a lack of specialized expertise, limited analytics, or it's too costly 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.

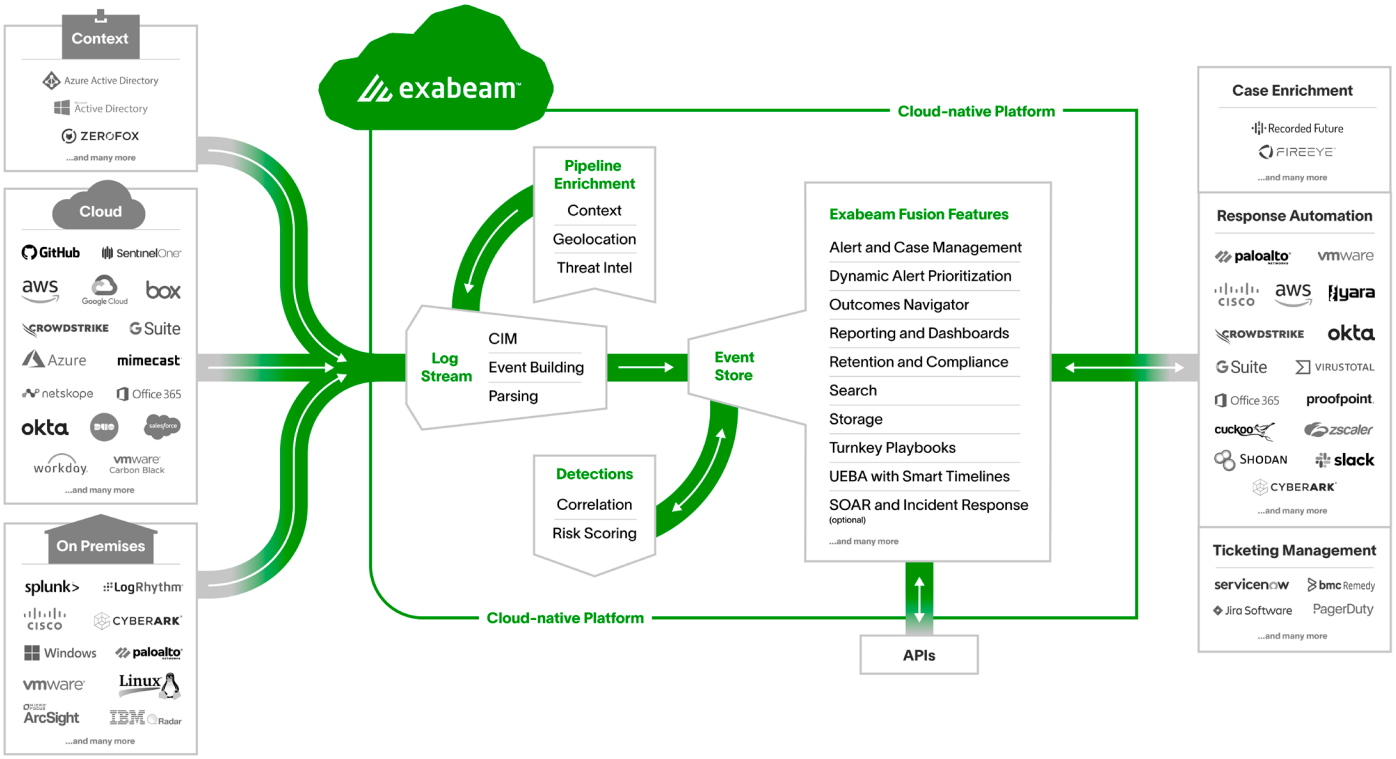
New-Scale SIEM™

Whether it's phishing, ransomware, malware, or another external threat, valid credentials are now the adversaries' primary target. This demands a shift in investment from legacy on-premises, rule-based detections such as what's in Splunk Enterprise Security to cloud-native SIEM platforms designed to identify abnormal behavior and automate the entire threat detection, investigation, and response (TDIR) workflow.

Security operations success requires a new approach: New-Scale SIEM™ from Exabeam. New-Scale SIEM is a breakthrough combination of the capabilities security operations staff need in products they want to use. These capabilities include rapid data ingestion, a cloud-native data lake, hyper-quick query performance, powerful behavioral analytics for next-level insights that legacy tools (like Splunk) miss, and automation that changes the way analysts do their jobs.

New-Scale SIEM includes three essential components that every customer in cybersecurity should demand from their SIEM vendors. First, you have to be able to rapidly ingest, parse, store, and search data at lightning speed with cloud-scale Security Log Management. Next, behavioral analytics can baseline "normal" behavior of users and devices, so that you can detect, prioritize, and respond to anomalies based on risk. Finally, you need an automated investigation experience to quickly identify incidents, effectively triage them, and respond efficiently.

Figure 1.
Data flow diagram of Exabeam Fusion™



Why transition from Splunk to Exabeam?

There are a lot of SIEMs in the marketplace from which to choose. But how do you distinguish between Exabeam and solutions such as Splunk to find the right fit for your organization? Here are four security scenarios that confirm why Exabeam stands out as a superior SIEM choice:

1. **The cost of securing your enterprise with Splunk is too high**
   Splunk encourages you to log all the data and not just the right data. This can be expensive to ingest and store. Getting all the data isn't necessary or actionable without mapping use cases to the data being captured.

   Another driver for cost is the need for experts to operate Splunk and the industry-wide shortage of cybersecurity professionals, and the need for unique expertise, training, and customization to operate Splunk. Using Exabeam, your team can leverage automation to streamline and accelerate security operations without the need for expert-level staff or a specialized set of skills. It's not uncommon to hear an Exabeam customer say in a short period of time their Level 1 analysts can handle Level 2 and Level 3 activities.

2. **Compliance retention is increasingly expensive — and hard to search in daily operations**
   Only store the most important part of the logs — parsing via a Common Information Model allows your security teams to keep all the logs needed for compliance in a more affordable way in the cloud, with lightning-fast search. If a need to look at logs from years ago arises, SOC teams can spend hours or days just getting the data re-loaded from backup and frozen storage. Centralizing your long-term security compliance logs in the cloud and searching with Exabeam speeds up operations, avoiding long delays and painful search query experiences.

3. **You're not able to distinguish normal from abnormal**
   It is important for a SIEM system to distinguish normal from abnormal user behavior because it helps identify hard-to-detect security threats missed by legacy SIEM tools. Normal user behavior patterns can be established over time and deviations from these patterns can indicate malicious or unauthorized activities. By detecting these deviations, the SIEM can alert security teams to investigate and take appropriate action to prevent damage or data loss. Be wary of solutions that use statistical analysis and call it machine learning and look out for UEBA solutions that are not well integrated with the SIEM platform - loose integrations and work in progress toolkits impact productivity and capabilities.

4. **Manual investigation and remediation**
   When legacy SIEM technology limits automation, the organization faces increased risk and longer durations of exposure to threats. For example, once an event becomes an incident each investigation requires the construction of a timeline to assess the impact, understand the scope, and prepare a response. For legacy SIEMs, those steps are usually manual and time-consuming. Constructing a timeline in Splunk typically requires nearly 300 queries from a highly specialized analyst.

   Attacks are becoming increasingly sophisticated, hard-to-detect, and credential-based attacks are multiplying — your automation needs to work harder and extend across the entire threat detection, investigation, and response workflow. Legacy SIEMs like Splunk cannot keep up.

Why Exabeam is a better choice for SIEM

The Exabeam Security Operations Platform provides cloud-native security log management, powerful behavioral analytics, and an automated investigation experience across the TDIR workflow. No product on the market – including Splunk – can provide you with more advanced TDIR capabilities.

Relieving your team of the resource-intensive tool, putting a strain on their time and expertise

Exabeam doesn't require any proprietary search language – anyone on your team can perform complex queries. It is easy to use and includes use case content, threat intelligence feeds, correlation rules, UEBA, and response automation (SOAR) within a single product experience.

An outcome-based approach to Use Cases

Exabeam offers three use case categories with 20 use cases. With compromised credentials being at the root of over 90% of breaches, understanding the behavior of valid credentials is critical to any security program. The days of knowing precisely what to look for have been turned upside down. Exabeam Outcomes Navigator is a new feature providing you with coverage analysis of your use cases, and recommends the data and parsing configuration changes needed to close any gaps.

Meet Compliance needs

Many organizations use manual processes and disparate security products to meet regulatory requirements, like General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Sarbanes-Oxley (SOX). These ad hoc processes leave organizations at risk for audit failure, fines, and disclosure reporting. Exabeam provides detection rules, models, retention, and compliance reports to show auditors that security controls are in place and work as designed.

Cost saving

Why not deploy a solution that uses automation to cut the time spent on security tasks by 51%? Through natural language querying, context-enhanced parsing, and data presentation, Exabeam improves analyst investigation efficiency and effectiveness — from collection to response.

The cost of deploying a SIEM can be an expensive undertaking for any organization. **Based on recent customer wins, the cloud native Exabeam SIEM can save users up to 30%.** But not only do you need to find the most cost-effective solution, you need to quickly realize value and earn a return on investment. The cost of deploying and operating Splunk is significant, and many organizations are slow to realize true security value from its use.

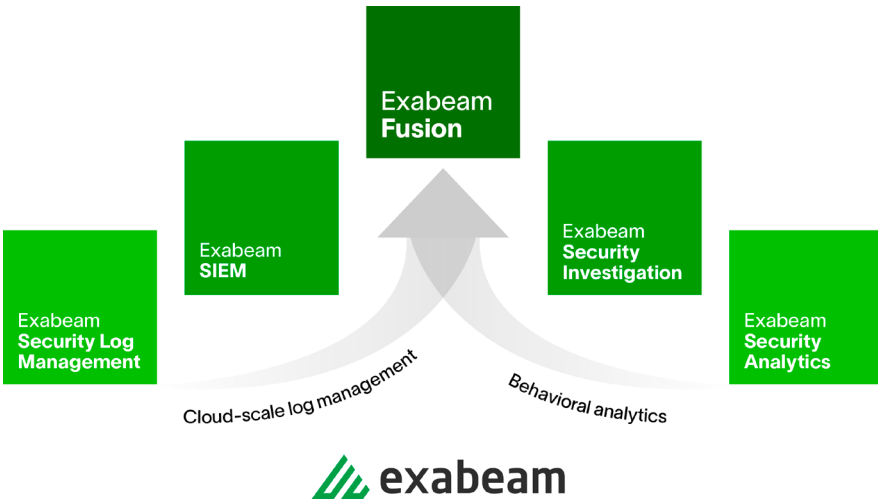


Figure 1.
Data flow diagram of Exabeam Fusion™

See how much you can save with the Exabeam Fusion SIEM ROI calculator →

	exabeam	Splunk
Detection Content		
Behavior-Based Models to Detect Abnormalities	750+ Behavioral Models	85+ Behavioral Models
Detection Rules to Detect Known Threats	1,800+	✓
Integrated Commercial-Grade Threat Intelligence	✓	Open Source
Detection Content Mapped to Use Cases	✓	X
Investigative Automation		
Automatically Generated Smart Timelines	✓	Query-Based Workflows
ML-Based Alert Prioritization	✓	Static Rule Severity Scoring
Pre-Built Watchlists for Risky Users and Entities	✓	Partial
Granular Risk Based Scoring	✓	X
Log Management		
Self-Service Data Collection Interface	✓	X
Search Query Builder Assistant	✓	X
Up to 10 Years of Searchable Data Without Rehydration	✓	X
Deployment Architecture		
Fully Cloud Native	✓	"Lift and Shift"
Multitenant	✓	✓
Integrated SIEM + UEBA + SOAR	✓	Must purchase UBA and Phantom – On-Prem Only

Figure 2. Exabeam and Splunk comparison

Transition process from Splunk to Exabeam

Being a strategic effort, SIEM transition will touch many areas of the 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 are intellectual property (IP), customer records, financial records, personnel records, systems running critical applications, networks, and security devices.

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

Transition does not necessarily require a wholesale replacement and can take a custom approach. It may suffice to augment Splunk with Exabeam's New-Scale SIEM capabilities such as behavioral analytics or automated response capabilities. Or perhaps a phased approach is better, which temporarily runs Exabeam in parallel with Splunk. 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: on-premises, a public cloud, a hybrid cloud, or to software-as-a-service (SaaS).

The estimated time of transition from Splunk to Exabeam typically takes 7-8 weeks.

Before we start the transition process, SOC teams are advised to 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 customer specific requirements such as unsupported log sources, unsupported log formats, and scoped custom work. Transition of security content is not included, but can be parsed for custom correlation, dashboard, and search transition assistance as time and materials (T&M).

Project Plan

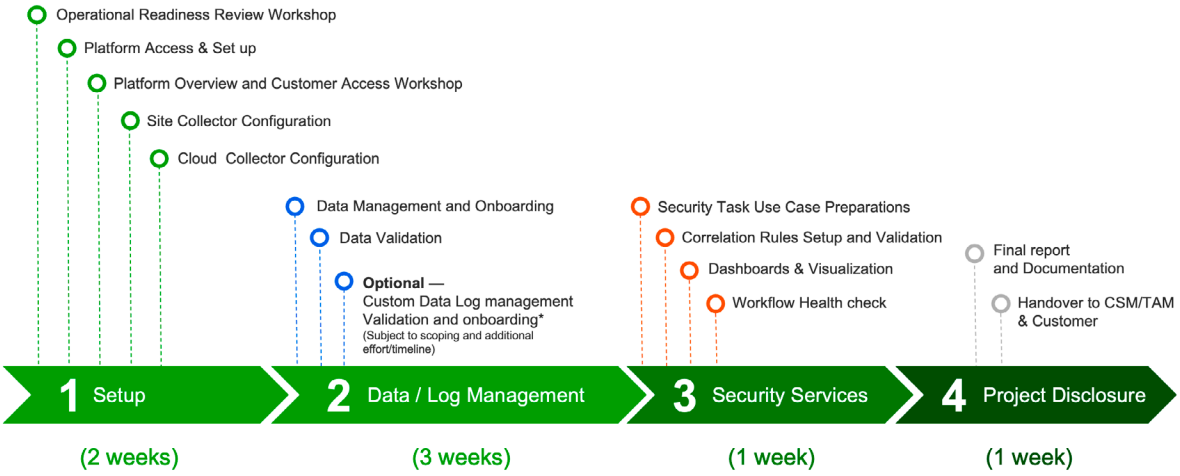


Figure 3.
Image of project plan and execution timeline

Transition Steps

Step 1: Setup (estimated 2 weeks to complete)

Operational readiness review workshop

In preparation for the customer journey, an Operational Readiness Review is conducted to help translate security goals into Operational Outcomes and tasks to achieve them. The Operational Readiness Review validates the scoped service deliverables, validates technical scoping to ensure a successful production deployment from the beginning, and discovers client information to guide adoption efforts for the entire life of the customer.

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 customer use. This is typically followed by a workshop introducing the customer to the applications and their operation.

Cloud Connector and/or Site collector configuration

The Cloud Connector and/or Site collector configuration steps of the deployment builds upon the deployment prerequisites by configuring logging infrastructure such as the site collector and cloud collectors to ingest from SaaS solutions including AWS, Azure, Box, Cisco AMP, CrowdStrike, Dropbox, Duo, G-Suite, GitHub, Office 365, Okta, OneLogin, Proofpoint, Salesforce, ServiceNow, and many others. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service at scale from on-premises, cloud, and context sources.

Step 2: Data/Log Management (estimated 3 weeks to complete)

Data management and onboarding

During the Data Management and Onboarding section of the deployment, logs begin flowing into the system. As scoped data sources are ingested, Exabeam's engineers validate that the log sources are parsing as expected, that parsed fields are parsing and accounted for, and ensure that the Exabeam environment has a healthy data pipeline. If the customer is augmenting Splunk, there is the ingestion option of fetching data directly from Splunk.

Step 3: Security Services (estimated 1 week to complete)

Security task use case preparations

Review the ORR to understand customer 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 the customer an understanding of the platform's capabilities and end user workflows. Exabeam offers over 100 pre-built correlation rules and models matching some of the most common use cases of malware and compromised credentials.

Dashboard and visualization

Validate pre-packaged dashboards and visualizations are working as expected. This allows you to print, export, with pre-built dashboards helping with search and visualization, as well as security operations. Customers can create their own dashboards specific to their needs. Any dashboard can be exported as a PDF to support reporting requirements. Exabeam Community offers opportunities for video instruction on how to build dashboards, with potential sharing of useful dashboards created by other users in other organizations.

Workflow health check

Validate that correlation outcomes and security alerts are populating in Alert and Case Manager.

Step 4: Project Closure (estimated 1 week to complete)

Final report and documentation

The final step in the deployment process is to create and deliver the Exabeam Deployment Final Report as part of the deployment project closure meeting. This report highlights the deployment tasks as well as the configurations that were made.

Post-transition activities

It is recommended that security operations teams run instances of Exabeam and Splunk in parallel for 30 days to ensure QA and validation. Another recommendation is to use Outcomes Navigator at the end of the implementation to understand and improve your use case coverage. Outcomes Navigator maps the feeds that come into Exabeam products against the most common security use cases to identify gaps and suggests ways to improve coverage.

Prepare reports for compliance and KPIs

One of the last steps in preparing for your transition to Exabeam 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. Exabeam out-of-the-box parsers categorize activity to allow you to create 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 transition is complete users need to write search queries. On average Exabeam users have about 40 searches. In order to execute these queries analysts need the following skills:

- Knowledge of syntax
- Knowledge of logic available
- Knowledge of use cases
- Knowledge of data sources
- How to get help when stuck

Conclusion

Splunk is a powerful data platform, designed for log search. It was not founded as a security company and never intended to provide security functionality. Splunk has an excellent track record as a tool for searching, sorting, and monitoring big data for many businesses. From application troubleshooting, to supply chains and distribution models, to moving goods, inventory, and other business intelligence functions, Splunk remains a good solution. But the fact remains, Splunk was never built for security, and instead has relied on bolt-on apps and capabilities from their UBA and SOAR acquisitions. Relative to the investment required to own and operate Splunk, security value is very hard to realize.

At Exabeam, we help you Detect the UndetectableTM? As important as cybersecurity is to your organization, doesn't it make sense to look for solutions and providers that are purpose-built for this critical function? Exabeam was built by security people for security people, a pioneer of the UEBA market, and one of the world's most successful standalone security companies.

What's next?

Getting the most out of your security investment and successfully moving from Splunk to Exabeam goes beyond the platform technology. Access to a supportive and knowledgeable professional services team can shift your security team from users to champions. Exabeam Professional Service resources will not only complement your short or long-term project requirements, but improve your team's ability to design, deploy, optimize, and sustain the value and effectiveness of the Exabeam Security Operations Platform solution.

A well-defined framework of deployment packages with customer-specified bespoke services and platform management services are available to help you get up and running quickly to maximize your investment in Exabeam.

- **Design** – Pre-packaged services designed and fully specified for seamless implementations and enhance time to value.
- **Deploy** – Enable your use of the Exabeam platform with proven standard or customized deployments to meet your unique requirements.
- **Optimize** – Fully operationalize your team's use of the platform to create the most effective use of time and resources.

With Exabeam Professional Services, you can extend your reach and supplement your team resources with our experienced professional services staff. Your organization can choose from a:

Full Time dedicated Resident Engineer

or

Part-Time designated Partial Resident Engineer

Dedicated Resident Engineers (RE) are full-time remote personnel responsible to ensure you receive immediate, sustained, and optimal value from the Exabeam Security Operations Platform. Embedded as a core member of the Exabeam Professional Services Team within your organization to handle the configuration, deployment, and management of your platform, you have immediate access to resolving your needs.

Resident Engineers support your team by:

- Ongoing data source management
- Facilitating integrity, validation, monitoring, and maintenance of data
- Conducting systems assessments and security solution implementations
- Creating documentation for your existing implementation
- Assisting with incident reporting and coordination with Exabeam Customer Support for resolution
- Testing lab/sandbox design and development
- Leading or participating in your Quarterly Business Reviews (QBRs)

For organizations that do not require full-time support, the Partial Resident Engineer (PRE) offers remote management or assistance with the operation of the Exabeam Security Operations Platform. The PRE is a remote, part-time resource who plays a vital role in your security operations teams, ensuring you receive immediate, sustained, and optimal value from your security platform.

Resident Engineer Services

Exabeam Resident Engineer consultants provide your security team with a full-time dedicated resource without having to teach them extensive processes. As a result, our consultants are uniquely qualified to partner with your team to ensure your organization gets the most out of the Exabeam security solution of your choice. Exabeam Resident Engineers provide:

- A focus on data onboarding and data integrity monitoring to ensure the Exabeam platform is running optimally
- Assistance in scaling pilot configurations to your production security platform
- Capturing your unique requirements and configuring Exabeam to meet those specifications
- Education through informal workshops, coaching sessions, design reviews, and documentation to expand your in-house technical expertise of the Exabeam platform
- Expertise in troubleshooting Exabeam product issues and interoperability issues with other security and network vendors used in your enterprise infrastructure
- Security analysis and threat hunting expertise using Exabeam insights
- Remote or onsite support based on your needs, working alongside your team for day-to-day operations

Service Alignment

Product	Packaged SKU	Add-On SKU
Exabeam Security Log Management	PS-DS-PKG-SLM →	PS-DS-ADD-ON-LOG-SLM
Exabeam SIEM	PS-DS-PKG-SIEM →	PS-DS-ADD-ON-LOG-SIEM
Exabeam Fusion	PS-DS-PKG-FUSION →	PS-DS-ADD-ON-LOG-FUSION
Exabeam Security Investigation	PS-DS-PKG-SI →	PS-DS-ADD-ON-LOG-SI
Exabeam Security Analytics	PS-DS-PKG-SA →	PS-DS-ADD-ON-LOG-SA

Education Services

Exabeam Education provides remote and hands-on courses to up-level your security analysts or engineers with instructor-led training or self-paced online classes. Your team will learn to maximize the features and functionalities of Exabeam products to get the most value out of the platform and get you up and running as quickly and efficiently as possible.

Specifically we have EDU-2201 to help analysts search and create dashboards and EDU-3201 to administer, configure, support, troubleshoot, and optimize your exabeam environment.

Our Education team is constantly working to create new courseware for all learning types. You will find these courses in our Training Center. Additionally, there are frequent seminars, monitored Q&A, and other resources available via Exabeam Community.

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 →