INTRODUCTION

THIS MIGRATION GUIDE IS FOR ORGANIZATIONS THAT ARE CURRENTLY USING SPLUNK ENTERPRISE SECURITY (ES) AND ARE MIGRATING THEIR SIEM TO THE EXABEAM SECURITY MANAGEMENT PLATFORM (SMP).

Migrating a legacy SIEM to new technology is a complex process. Exabeam’s 8-step model for SIEM migration presents a process that accounts for typical scenarios such as augmenting a legacy SIEM with behavioral analytics or replacing a legacy SIEM entirely. For a strategic overview of preparing for SIEM migration, please see our whitepaper, Eight Steps for Migrating Your SIEM.

This guide assumes you have already completed steps 1-3 including having determined the business priorities for migration to Exabeam, selected use cases for the migration, and that you have scoped the data sources required for log collection (see Figure 1). This guide focuses on activities related to steps 4-6 of Exabeam’s migration model and a high-level overview of the activities needed to get Exabeam up and running.

Specifically, this guide provides a task-list that describes how to:

A. Install and Configure Exabeam Advanced Analytics
B. Set up Context and Event Ingestion
C. Select Exabeam’s Out-of-the Box Use Cases
D. Install and Configure Exabeam Data Lake
E. Install and Configure Exabeam Cloud Connectors
F. Migrate High-Value Correlation Rules
G. Forward Event Data from Exabeam Data Lake to Exabeam Advanced Analytics
H. Decommissioning Splunk ES
I. Forward Incidents to Exabeam Case Manager
J. Implement Playbooks in Exabeam Incident Responder
K. Prepare Reports for Compliance and KPIs
These tasks do not necessarily have to happen in sequence. Administrators have the option to start by deploying Advanced Analytics or they can start by deploying Data Lake. Administrators also have options related to whether they initially augment or replace Splunk ES. For example, one option is to set up Exabeam in parallel with Splunk ES. Once your Security Operations Center (SOC) is comfortable with using Exabeam SMP, you can then proceed to shut off Splunk ES if desired.

FIGURE 1: EIGHT STEPS TO MIGRATE YOUR SIEM
Preparing for SIEM Augmentation

An effective starting point when replacing a legacy SIEM is to first ease the workload on your SOC analysts by implementing a User and Entity Behavioral Analytics (UEBA) solution like Exabeam Advanced Analytics. Traditional SIEMs generate enormous volumes of unactionable alerts that must be investigated – and subsequently create a major waste of time. Augmenting Splunk ES with Advanced Analytics, you will dramatically reduce the typical volume of alerts flowing into the SOC while improving the productivity of your analysts by adding powerful investigation capabilities such as Exabeam Smart Timelines™. Smart Timelines eliminate wasted time and effort by revealing user and asset activity via dynamic behavior modeling. Exabeam’s tightly integrated case management and security orchestration capabilities, respectively Exabeam Case Manager and Exabeam Incident Responder, can also be used to assist and accelerate analyst workflows and reduce the time required to resolve incidents.

Implementing the full Exabeam platform, including Exabeam Data Lake, should lead to improved collection of user and event data, automatic detection of anomalies, easy investigation of root causes and faster incident response. The tasks described in this guide can be used to start feeding high fidelity alerts to your security teams to achieve these benefits.

FIGURE 2: EXABEAM PROVIDES ALL OF THE FEATURES OF AN INNOVATIVE AND EFFECTIVE MODERN SIEM COVERING THE FOUR PHASES OF SOC OPERATIONS: COLLECTION, DETECTION, INVESTIGATION AND RESPONSE.
A. Install and Configure Exabeam Advanced Analytics

Exabeam Advanced Analytics is available in hardware appliance, virtual machine and Amazon Web Services AMI template formats. Installation and configuration is quick and easy thanks to an easy to understand web user interface. User and asset context information is easily retrieved from Microsoft Active Directory or other LDAP sources, as well as from CSV and other popular human resource systems. Event information can be absorbed through syslog or API calls to the source systems.

Advanced Analytics provides powerful alert prioritization that allows SOC analysts to focus on the highest risks. This should be a significant change from your experience with Splunk ES where alerts are typically voluminous and difficult to investigate due to the lack of context.

FIGURE 3: NOTABLE EVENTS IN SPLUNK ES ARE SINGLE DIMENSIONAL AND CONVEY LITTLE CONTEXT
FIGURE 4: EXABEAM PROVIDES EVENT CONTEXT AND A TIMELINE OF ACTIVITY TO ACCELERATE INVESTIGATIONS
B. Set Up Context and Event Ingestion

Advanced Analytics can acquire event data from Splunk ES using the Splunk API interface, making it easy to augment your existing SIEM with behavioral analytics. Additionally, API queries can retrieve historical event data. This results in faster time to value as that historical data builds baselines of normal activity faster than if you just used real-time queries alone.

Using this API interface, we recommend retrieving the specific event types that map directly to the Exabeam behavioral analytic models for your desired use cases (see Activity C). This eliminates you needing to forward your entire event stream. Advanced Analytics can easily be configured to pull specific event types from your Splunk ES instance. Next, configure Advanced Analytics to pull user and asset information from Microsoft Active Directory (AD) or another LDAP source.

After completing these activities, you should have an instance of Advanced Analytics installed, configured and starting to learn your environment.

FIGURE 5: AUGMENTING SPLUNK ES WITH EXABEAM ADVANCED ANALYTICS (USER AND ENTITY BEHAVIOR ANALYTICS)
C. Select Exabeam’s Out-of-the-Box Use Cases

Advanced Analytics includes more than 400 out-of-the-box machine learning models to support your use cases. They are a powerful replacement for legacy static correlation rules, which are often noisy and sometimes of little value. As soon as event data is flowing into Advanced Analytics, Exabeam starts learning both user and asset behavior and will begin providing high confidence alerts based on anomalous behavior.

<table>
<thead>
<tr>
<th>Account Creation and Management</th>
<th>Account Switches</th>
<th>Anomalous Access</th>
<th>Application / Cloud Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised Credentials</td>
<td>Data Loss/Exfiltration</td>
<td>Database Analytics</td>
<td>Email Analytics</td>
</tr>
<tr>
<td>Endpoint Analytics</td>
<td>Executive Users</td>
<td>Failed Logons and Account Lockouts</td>
<td>File Access Analytics</td>
</tr>
<tr>
<td>High Risk Employees</td>
<td>High Value Assets</td>
<td>Physical Access</td>
<td>Privileged Users</td>
</tr>
<tr>
<td>Security Alerts</td>
<td>Service Accounts</td>
<td>VPN Remote Access</td>
<td>Web Activities</td>
</tr>
</tbody>
</table>

FIGURE 6: A SAMPLE OF PRE-CONFIGURED EXABEAM MODELS

Advanced Analytics also offers static rules (called Factual-based rules), which can be used to replicate your existing static rules where appropriate. For example, a static rule could entail adding risk factors into user or asset sessions based on Indicators of Compromise (IOC) or a violation of company security policy.

D. Install and Configure Exabeam Data Lake

This task entails preparation for ingesting and retaining event data in Data Lake to replace Splunk ES event forwarders, indexers and storage as your log management platform. Data Lake is the collection and consolidation tier of the Exabeam SMP for any events that could possibly have security value.

Many SIEMs, like Splunk ES, license based on data ingest volumes. As data volumes grow most organizations struggle to afford licenses. This financial variable is a negative incentive that forces security teams to make decisions on what data sources to not ingest into Splunk ES. Choosing to not collect data results in lower visibility. Even with sufficient license capacity, older pre-big-data technology can lead to queries taking a long time to execute, sometimes timing out and hindering investigations.

By contrast, Exabeam licenses using a predictable user-based pricing. With the ability to ingest all needed data, including logs from cloud and SaaS applications, your visibility into user actions can be dramatically expanded. This is one more benefit of migrating from Splunk ES to Exabeam.
Data Lake is available in hardware appliance, virtual machine and Amazon Web Services AMI template formats. Similar to Advanced Analytics, installation and configuration is quick and easy with a typical install taking less than a morning with the easy-to-understand web user interface. By using Exabeam collectors, Data Lake can ingest event data from syslog, Windows, databases, eStream, files, Kafka, as well as common cloud SaaS platforms. Exabeam has prebuilt collectors for over 200 products, with over 2500 parsers.

E. Install and Configure Exabeam Cloud Connectors

This step entails installing Cloud Connectors to ingest logs from popular SaaS solutions including AWS, Azure, Box, Cisco AMP, CrowdStrike, Dropbox, Duo, G-Suite, GitHub, Office 365, Okta, OneLogin, Proofpoint, Sales Force, and ServiceNow. Other cloud logs can be ingested using Exabeam’s custom API connector (see task D).

**FIGURE 7: AN OVERVIEW OF HOW EVENTS FLOW INTO DATA LAKE AND CLOUD CONNECTORS**
F. Migrate High-Value Correlation Rules
Splunk ES customers will likely have a large number of custom rules that they have built over time, many of which consist of layers of static correlations in a building block format. Static correlation rules are good for detecting known threats, such as matches to indicators and warnings or violations of security policy. All of these are candidates for replication in Exabeam.

Correlation rules can be configured in Data Lake to create actionable or informational alerts. Informational alerts can be forwarded to Advanced Analytics for inclusion in user and asset Smart Timelines, while actionable alerts can be forwarded to create an incident for investigation.

Advanced Analytics also uses a focused set of correlation rules (Factual rules) in the default content to highlight risky events in user and asset Smart Timelines when specific conditions are met.

G. Forward Event Data from Exabeam Data Lake to Exabeam Advanced Analytics
As previously discussed, Data Lake is the collection and consolidation tier of the Exabeam SMP. It can be used to ingest any event that could possibly have security value through syslog, Windows, databases, eStreamer, files and cloud APIs. There will be a subset of those events that will be Events of Interest for the desired use cases in Advanced Analytics.

Any Events of Interest can easily be forwarded from Data Lake to Advanced Analytics by using preconfigured filters or adding custom log types.

H. Decommissioning Splunk ES
With cutover of event ingest through Data Lake, you can begin the decommission process for your Splunk ES systems, which will save maintenance and support funds.
I. Forward Incidents to Exabeam Case Manager and Exabeam Incident Responder

Splunk ES SOCs are typically overwhelmed by huge numbers of alerts that are difficult to investigate and require large numbers of personnel due to the lack of context and lack of substantial automation. The Exabeam SMP includes rich case management in Case Manager and security orchestration through Incident Responder. One of the ways to improve your SOC operations workflow and significantly reduce time to investigate incidents using Exabeam is to forward incidents to Case Manager and Incident Responder. Alerts can be forwarded from both Data Lake and Advanced Analytics.

The first step in this task entails configuring the conditions for static correlation alerts to be forwarded from Data Lake to Case Manager and Incident Responder (blue arrow in Figure 9). This is easily done in Data Lake using the Correlation Rule UI.

![FIGURE 9: EVENT FLOW IN THE EXABEAM SMP](image)
Next, configure trigger conditions for alerts to be sent from Advanced Analytics to Case Manager and Incident Responder based on additional analytics findings for notable alerts and/or all anomalies (green arrow in Figure 9). These alerts will also appear in Smart Timelines in Advanced Analytics. Configuring these forwarding actions immediately enables automated case creation.
J. Implement Playbooks in Exabeam Incident Responder

Improving the capability maturity level of the SOC can be done by implementing playbooks within Incident Responder. Automated investigation of incidents enables junior or tier one analysts to be more productive while Incident Responder performs the repetitive steps required to undertake the initial response. Use of Incident Responder allows SOC teams to reduce alert fatigue and case management pain while improving investigative velocity.

FIGURE 12: AN EXAMPLE MALWARE INVESTIGATION PLAYBOOK VISUALIZATION IN INCIDENT RESPONDER
K. Prepare Reports for Compliance and KPIs

The last step in preparing your transition to Exabeam entails report preparation. Configure Advanced Analytics and Incident Responder to forward findings and Key Performance Indicator (KPI) events back to Data Lake. Set up comprehensive reporting to address selected use cases, compliance mandates and KPI reports. Your organization’s Risk Manager can provide specific requirements for compliance. 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).

CONCLUSION

As you conduct the migration process from Splunk ES to Exabeam Security Management Platform, your SOC team will quickly discover many new benefits that improve analyst productivity. For example, Exabeam SMP’s features will eliminate the manual rote work created by Splunk ES’s stream of alerts. This will free their time to focus on issues that matter. More importantly, Exabeam SMP will help your analysts rapidly zoom in on incident root causes to quickly resolve those issues. As a result, your enterprise will become more secure.

During this journey, we invite your SOC team to take advantage of the education and professional services offerings provided by Exabeam and our service partners to help complete the transition. Please contact Exabeam or your service partner to learn more.
ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We empower enterprises to detect, investigate, and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines™, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques, and procedures. ▲

Exabeam, Smarter SIEM, Smart Timelines and Security Management Platform are trademarks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Exabeam, Inc. All rights reserved.