exabeam

WHITE PAPER

EXABEAM HELPS PROTECT INFORMATION SYSTEMS

Meeting the Latest NIST SP 800-53 Revision 4 Guidelines

SECURITY GUIDELINE COMPLIANCE

There has been a rapid increase in malicious insider threats, sensitive data exfiltration, and other advanced threats targeting organizations today. Organizations not only need security technologies to protect themselves from such threats, but also need to comply with security regulations and follow best practices in order to manage cyber risks.

Traditional security is insufficient to protect today's hybrid infrastructure. With increasingly dynamic environments enabled by trends such as bring your own technology (BYOT), more data in the cloud, and a growing number of points of entry to your infrastructure, modern threats can do major damage to an organization. They could take years to discover and stop.

This white paper focuses on some of the main information security controls and requirements addressed by NIST SP 800-53 revision 4. It maps key Exabeam solution capabilities to NIST SP 800-53 revision 4 guidelines, describing how they can be used to manage risk to federal information and prove compliance.

What is NIST?

The National Institute of Standards and Technology was founded in 1901 and is part of the US Department of Commerce. It's responsible for the Cybersecurity Framework that provides guidelines and best practices to manage cybersecurity-related risks. NIST isn't just for federal, state, or local government systems; over 50 percent of US organizations will be using its guidelines by 2020.[1]

[1] HTTPS://WWW.NIST.GOV/INDUSTRY-IMPACTS/CYBERSECURITY

WHY NIST COMPLIANCE MATTERS

NIST published SP 800-53 to provide guidelines on security controls for federal information systems. It's to help agencies develop appropriate security policies and controls to protect all federal information systems. It also offers its Cybersecurity Framework[2] to help organizations understand cybersecurity risks and how to reduce these risks using customized measures.

The framework also helps organizations know how to respond to and recover from cybersecurity incidents—prompting them to analyze root causes and consider how to make improvements.

NIST SP 800-53 REV. 4 COMPLIANCE WITH EXABEAM

Organizations often begin with a gap assessment to examine compliance across their enterprises. Exabeam offers solutions to satisfy many threat detection use cases and meet your security and compliance needs. Here is an Exabeam product line overview:

Exabeam Data Lake - A security data lake that helps enterprises to collect and store unlimited amounts of security data to detect threats and meet compliance use cases; all for a predictable, flat rate.

Exabeam Advanced Analytics - A User and Entity Behavior Analytics (UEBA) solution—that can be deployed on top of Exabeam Data Lake or legacy SIEM tools. It can detect malicious insiders, compromised and rogue insiders, data exfiltration, malware, and other advanced threats.

Exabeam Entity Analytics - Focuses on tracking assets in your organization. It provides end-to-end network visibility, establishes baseline behavior (using communication patterns, ports and protocols, servers, and operating activity), and automatically identifies irregular activities that are indicative of a security incident.

Exabeam Incident Responder - A Security Orchestration and Automated Response tool (often called a SAO or SOAR solution). It provides a Case Management—central console to track and manager incidents and Automated Response —automate collection of evidence for investigations using response playbooks and centralized workflows.

Exabeam Threat Hunter - Not requiring a complex query language, Threat Hunter provides SOC with a simple GUI to perform threat hunting. This gives all analysts levels the ability to run complex searches with context-aware data.

> "Exabeam helped us exceed our SOC 2 regulation requirements while reducing the time required by a few quarters and helping us delay analyst hires"
>
> **CISO AT PUBLICLY-TRADED CYBERSECURITY COMPANY**

[2] HTTPS://WWW.NIST.GOV/CYBERFRAMEWORK

Access Controls

The NIST SP 800-53 rev. 4 Access Control (AC) section addresses access policies and procedures, account management, and access enforcement related to information systems. It requires access control implementation in order to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Exabeam provides role-based controls to permit access to information stored in databases, servers, or cluster nodes.

AC – ACCESS CONTROLS		
Control ID	Control Name	Compliance with Exabeam
AC-2	Access Management	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam enables access to information and actions that administrators take based on roles.
AC-5	Separation of Duties	**Advanced Analytics; Entity Analytics; Data Lake; IR:** Enables security control separation. Exabeam provides role-based access control, with roles having separation of duties.
AC-6	Least Privilege	**Advanced Analytics; Entity Analytics; Data Lake; IR:** User management can limit the user access privileges to a minimum.
AC-7	Unsuccessful Login Attempts	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam alerts on multiple authentication failures and can identify anomalous login activities.
AC-17	Remote Access	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam automatically analyzes remote access data and alerts on anomalous access.
AC-18	Wireless Access	**Data Lake:** Provides evidence and alerts in response to rogue wireless access points.
AC-20	Use Of External Information Systems	**Data Lake:** Exabeam can verify and control connections to external systems but may not limit those connections.
AC-23	Data Mining Protection	**Advanced Analytics; Entity Analytics:** Exabeam has access control policies and defined storage objects. It monitors access and audit logs to detect and protect against data mining.

Audit and Accountability

This section of NIST SP 800-53 rev. 4 addresses audit requirements to ensure that access controls are enforced while effectively restricting unauthorized data access. It requires organizations to audit relevant information access and keep a detailed record of such events. Organizations should be able to:

- Define events that require auditing
- Review and analyze audit data
- Provide granular reporting capabilities with effective controls
- Store data for audits and investigations

AU – AUDIT AND ACCOUNTABILITY		
Control ID	Control Name	Compliance with Exabeam
AU-3	Content of Audit Records	**Data Lake:** Exabeam provides detailed audit records that contain information about events. This includes data and time of the events, their source location, who and how many times events were accessed.
AU-4	Audit Storage Capacity	**Data Lake:** Exabeam provide configurable storage options for audit records.
AU-5	Response to Audit Processing Failures	**Data Lake:** Exabeam logs and alerts on any processing failure of audit information.
AU-6	Audit Review, Analysis, and Reporting	**Data Lake:** Exabeam provides predefined reports for compliance, health and various activities. It provides access to information real-time for review, analysis and reporting.
AU-7	Audit Reduction and Report Generation	Users are able to filter and search for data. Original data ingested cannot be altered, as it might be made available for analysis and security investigations.
AU-8	Timestamps	**Data Lake:** Exabeam uses the system clock to generate timestamps for all records.
AU-9	Protection of Audit Information	**Data Lake:** Strict controls for authorized access are enforced. Data can be masked for non-administrators.
AU-10	Non-repudiation	**Data Lake:** Exabeam logs all system changes, and any changes made by administrators and users.
AU-11	Audit Record Retention	**Data Lake:** Exabeam enables organizations to retain audit data and it archive for future use.
AU-12	Audit Generation	**Data Lake:** Exabeam enables organizations to generate granular audit records and customized records based on audited events.
AU-13	Monitoring for Information Disclosure	**Data Lake:** Exabeam monitors unauthorized exfiltration of organizations' information. It monitors connections to external data services, transmission of files and data to external storage devices, and any authorized use of remote assets.
AU-14	Session Audit	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam logs all content (users, events, assets) related to a user session in real-time.
AU-15	Alternate Audit Capacity	**Data Lake:** Exabeam can send logs to another system that serve as alternate audit system.

Security Assessment and Authorization

The Security Assessment and Authorization section requires assessment to determine the effectiveness of security controls. Exabeam provide tools to centrally manage and assess your security controls. In addition to security log management, it provides analytics and reporting capabilities that organizations can leverage to ensure security controls are in place. And it lets you continuously monitor administrative assets, databases, file systems, endpoints, servers to assess any unauthorized access attempts.

CA – SECURITY ASSESSMENT AND AUTHORIZATION		
Control ID	Control Name	Compliance with Exabeam
CA-2	Security Assessments	**Data Lake:** Exabeam log analysis tools and reports can be leveraged for security assessments to verify that security controls are in place.
CA-3	Information System Connections	**Advanced Analytics; Entity Analytics:** Exabeam monitors servers, databases, high-value assets and file server connections and alerts on any unauthorized access.
CA-7	Continuous Monitoring	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam provides continuous monitoring to assess high-value assets, file systems, databases, and server controls. It identifies any changes made to security controls.
CA-9	Internal Systems Connections	**Advanced Analytics; Entity Analytics:** Exabeam provides real-time internal systems status by monitoring for anomalous activity and identifies any changes made to security controls.

Configuration Management

The Change Management (CM) section addresses configuration control requirements for information systems and the maintaining of a current system baseline configuration. Any configuration changes must be approved and documented, while unauthorized changes should be restricted.

Exabeam monitors configurations of high-value assets, file systems, servers, endpoints, and databases, capturing configuration changes in real-time. Alerts respond to deviations from authorized configurations, with such deviations also being documented.

CM – CONFIGURATION MANAGEMENT		
Control ID	Control Name	Compliance with Exabeam
CM-2	Baseline Configuration	**Data Lake:** Exabeam provides correlation rules which can detect any deviations from the baseline configurations.
CM-3	Configuration Change Control	**Data Lake:** Exabeam collects and analyzes all configuration changes from critical systems in your organization. Any configuration changes are alerted and documented for security responders to investigate further.
CM-6	Configuration Settings	**Data Lake:** Exabeam centrally manages all configuration settings. Any settings change triggers an alert and is logged.
CM-7	Least Functionality	**Data Lake, Advanced Analytics; Entity Analytics:** Exabeam can identify unauthorized and unneeded functions for services, ports, database functions and/or connections, system connections, remote access controls, web service connections, and network ports.

Identification and Authentication

The Identification and Authentication (IA) section requires that information systems to uniquely identify and authenticate users or processes acting on behalf of organizational users and devices with information systems. Exabeam's real-time monitoring of users, and devices, and assets makes it very easy for organizations to identify any anomalous authentications.

IA – IDENTIFICATION AND AUTHENTICATION		
Control ID	**Control Name**	**Compliance with Exabeam**
IA-2	Identification and Authentication	**Advanced Analytics; Entity Analytics; Data Lake** Exabeam provides real-time monitoring of users and assets in your organization to identify authorized users who access their assigned assets. Exabeam enables you to: • Provide evidence and reports for all authentication activities • Alert on authentication failures and unauthorized asset access by users. • Identifies and alerts in response to unauthorized asset access by non-organizational users (e.g., partners, vendors).
IA-3	Device-to-Device Identification and Authentication	
IA-8	Identification and Authentication (non-organizational users)	

Incident Response

The Incident Response (IR) section addresses handling requirements for security incidents— including detection, analysis, and incident response procedures.

Exabeam provides a central console for security analysts to manage and prioritize incidents. It lets them add evidential artifacts to incidents by triggering playbooks to gather more information for an investigation. Exabeam can investigate, contain, and mitigate all related security incidents in an automated manner to significantly shorten mean-time-to-detect (MTTD) and mean-time-to-resolution (MTTR). In doing so it leverages prebuilt API integrations with IT infrastructure and security solutions, eliminating tedious, manual tasks that free security teams to work on more important, value-add activities.

IR – INCIDENT RESPONSE		
Control ID	**Control Name**	**Compliance with Exabeam**
IR-3	Incident Response Testing	**Incident Responder:** Exabeam provides a case management console to handle security incidents and provides tools to respond to incidents by playbook integrations and automated response capabilities.
IR-4	Incident Handling	
IR-5	Incident Monitoring	**Advanced Analytics; Entity Analytics; Incident Responder:** Exabeam tracks abnormal behavior and creates incidents if risk scores exceed a set threshold value. It integrates with other SIEM solutions to take in notable events/alerts and provide automated response capabilities
IR-6	Incident Reporting	**Advanced Analytics; Entity Analytics; Incident Responder:** Exabeam provides security incident reports that includes open and closed incidents, work distribution, and metrics such as mean-time-to-respond (MTTR).

IR – INCIDENT RESPONSE (CONTINUED)		
Control ID	Control Name	Compliance with Exabeam
IR-7	Incident Response Assistance	**Advanced Analytics; Entity Analytics; Incident Responder:** Exabeam attaches smart timelines from Advanced Analytics to aid investigators in pinpointing anomalous behavior and quickly mitigate incidents.
IR-8	Incident Response Plan	**Advanced Analytics; Entity Analytics; Incident Responder:** Exabeam has integrated products to manage all security incidents as part of case management. Built-in functionality automatically gathers evidence as part of the response plan.
IR-9	Information Spillage Response	**Advanced Analytics; Entity Analytics; Incident Responder:** Exabeam monitors all logs and events so it can isolate a contaminated information system. It provides automated action as part of the workflow to remove information spills or stop contaminated system access.
IR-10	Integrated Security Analytics Team	**Advanced Analytics; Entity Analytics; Incident Responder:** Exabeam provides a integrated platform – a central incident tracking console, collect evidences through centralized workflows, automates responses, and collaborates across your SOC Operations team.

Physical and Environmental Protection

The Physical and Environmental Protection (PE) section addresses the creation of policies and procedures for the effective implementation of selected security controls and control enhancements with respect to physical access to information systems.

PE – PHYSICAL AND ENVIRONMENTAL PROTECTION		
Control ID	Control Name	Compliance with Exabeam
PE-3	Physical Access Control	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam monitors physical access to information systems to detect and alert in response to related incidents. All access logs-—physical, remote, and system access—are monitored, providing a detailed analysis of any intrusion.
PE-6	Monitoring Physical Access	

Personnel Security

The Personnel Security (PS) section discusses effective security controls implementation on systems and services with respect to personnel. It establishes personnel security requirements, addresses how systems should be handled upon personnel termination, and logical/physical access authorizations to information systems/facilities when individuals are reassigned or transferred.

PS – PERSONNEL SECURITY		
Control ID	Control Name	Compliance with Exabeam
PS-4	Personnel Termination	**Advanced Analytics; Entity Analytics, Data Lake:** Exabeam alerts if information system access (account, physical access, software/system access) is not disabled upon termination of individual employment. A watch list tracks any occurrence of user movements related to departed employees.
PS-5	Personnel Transfer	**Data Lake:** Exabeam reviews logical and physical access authorizations to information systems when personnel are reassigned/ transferred to other departments, or move to other physical locations.
PS-7	Third-Party Personnel Security	**Advanced Analytics; Entity Analytics, Data Lake:** Exabeam monitors third-party personnel compliance within the organization. It monitors them in relation to lateral movements, remote asset access, physical and logical access. Exabeam provides a third-party personnel watch list. Notable events that exceed a set threshold create incidents for investigators to investigate.

Planning

The Planning (PL) section refers to the organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes.

PL – PLANNING		
Control ID	Control Name	Compliance with Exabeam
PL-9	Central Management	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam provides a central management to manage all security controls— rules, configurations, access controls, users, start/stop services, content, and admin operations.

Systems and Services Acquisition

The Systems and Services Acquisition (SA) section discusses considerations for effective implementation of security controls and enhancements on systems and services. This section discuss the need to develop secure systems and testing these systems to evaluate their weaknesses and develop a remediation process.

SA – SYSTEM AND SERVICE ACQUISITION		
Control ID	Control Name	Compliance with Exabeam
SA-7	User-Installed Software	**Advanced Analytics; Entity Analytics, Data Lake:** Exabeam alerts on any unauthorized or anomalous installation of software by users. Access and installation logs are correlated to alert on any unauthorized installations.

System and Communication Protection

The Systems and Communications Protection (SC) section discusses controls related to this topic. It requires separation of duties to ensure that system administrators don't tamper with security controls to hide their own misdoings. It requires protection of information in shared resources from unauthorized access and use, as well as from denial of service attacks.

Exabeam provides a solution to monitor and audit all access and usage logs. This helps protect systems from service attacks, threats, network assaults, and data exfiltration. And it makes sure all security services that administrators access are logged in the system.

SC – SYSTEM AND COMMUNICATION PROTECTION		
Control ID	Control Name	Compliance with Exabeam
SC-5	Denial of Service Protection	**Data Lake:** Exabeam identifies any denial of service attacks by analyzing and monitoring security logs.
SC-7	Boundary Protection	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam collects peripheral device logs from firewalls, VPN servers, and routers to monitor and alert in response to suspicious and unauthorized activities. It reports and provide analysis on boundary activities and threats.

Systems and Information Integrity

The Systems and Information Integrity (SI) section addresses controls to monitor information system activity to identify unauthorized use and change of information, and ensure information integrity. Only authorized personnel should have the ability to input information into the system and the input syntax and semantics should be validated to prevent the content from being unintentionally interpreted as commands.

SC – SYSTEM AND COMMUNICATION PROTECTION		
Control ID	Control Name	Compliance with Exabeam
SI-3	Malicious Code Protection	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam prevents non-privileged users from adding code, introducing removable media, or updating new releases on information systems. It alerts in response to malware infections, signature updates, or system threats.
SI-4	Information System Monitoring	**Advanced Analytics; Entity Analytics:** Exabeam monitors system events and detects threats and unauthorized information systems use.
SI-11	Error Handling	**Advanced Analytics; Entity Analytics; Data Lake:** Exabeam generate error messages that provide information for administrators to take corrective actions.

exabeam

CONCLUSION

NIST SP 800-53 rev.4 provides guidelines on security controls for federal information systems. Organizations that process or store federal information are obligated to secure it so as to minimize risk of unauthorized access and improper usage.

Exabeam is a modern SIEM that combines end-to-end data collection, analysis, and response in a single management and operations platform. It offers a single, fully integrated, and centrally managed solution that reduces TCO while enabling phased, seamless deployment.

In addition, Exabeam has a rigorous testing methodology and quality assurance process implemented during all phases of its software development lifecycle. Accelerating your deployment with quick time-to-value, it provides prepackaged security reports and search capabilities. Customers can quickly and painlessly satisfy FISMA, ISO 27001, HIPAA requirements to secure related data and information systems.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.