IMPLEMENTING PCI DSS CONTROLS WITH EXABEAM

May, 2018

exabeam

The Payment Card Industry Data Security Standard (PCI DSS) is a broadly-implemented set of security controls created to improve the safety of payment card information. Used at large and small retailers for many years, recent changes require updates to existing controls and reporting capabilities. This white paper describes how Exabeam helps organizations implement effective security controls that map to the PCI DSS.

PCI DSS 3.2

PCI DSS has 12 requirements and over 300 security controls that apply to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. With PCI DSS 3.2, changes to SSL/TLS, stricter authentication controls (e.g., multi-factor authentication), and increased scrutiny of service providers have been introduced. Most organizations seek to address these requirements by deploying multiple standalone products. These weave together disparate technologies to create an expensive, inefficient, and time-consuming integration burden.

THE ROLE OF SECURITY MANAGEMENT IN PCI COMPLIANCE

Traditional regulatory compliance management—system log event monitoring, diagnosis, and root cause analysis—involves several manual processes. Combined with large data sets typically processed by an organization, stricter requirements involve tedious efforts to collect, analyze, store, and protect relevant log events to achieve compliance. Security information and event management (SIEM) tools play a key role in resolving these issues; they quickly identify and analyze security events in a comprehensive manner. Instead of a SIEM doesn't rely on a single source of security data to detect a threat, abnormal activity, or compliance issue. Instead it collects data from multiple sources to enable real-time, end-to-end assessments of security information. A SIEM also helps streamline compliance reporting, making that a simpler process during audits. A SIEM provides an essential role in any a compliance framework via:

· Log collection and management

· Real-time threat detection

· Automated incident response

· PCI compliance reporting and dashboards

LOG COLLECTION AND MANAGEMENT

Log and event monitoring is at the core of diligent information security and compliance. Either directly or via a SIEM/log management system/data lake, IT teams use security intelligence platforms to ingest event logs to identify risky, anomalous activity related to financial reporting. These include file access logs, email logs, windows event logs, other security solution logs and web proxy logs. Log collection and management is foundational; event logs and security alerts provide the data required to prove compliance with nearly every regulation.

REAL-TIME THREAT DETECTION

Another PCI DSS precept is to apply security controls to help combat fraud or security breaches caused by malware or other threats. This makes improving threat detection critical to any PCI DSS compliance effort. By aggregating data across disparate security tools, a SIEM provides a holistic view of an organization's security posture. Using a combination of machine learning, AI, and behavioral modeling, next generation SIEMs go a step further by enabling automated, real-time analysis of log and security event data.

AUTOMATED INCIDENT RESPONSE

Threat and breach prevention being a core PCI DSS tenet, it has historically been the focal point for many IT security initiatives. But threats do occur, thus incident management must also be a top priority of any comprehensive security effort. A SIEM tool can help your organization investigate threats and respond to incidents more quickly. It gives your responders a way to drill down and gather evidence about everything that occurred during an event. Next-gen SIEMs include case management to help organize response efforts, in addition to security orchestration and automation. Collectively they run response playbooks to automate all of those tedious, manual tasks—freeing your security team to work on more important, value-add activities.

PCI COMPLIANCE REPORTING AND DASHBOARDS

Providing simple yet comprehensive visibility, PCI compliance reporting and dashboards quickly demonstrate your organization's compliance to an auditor. And they help maintain continuous security monitoring afterward. A SIEM solution typically delivers predefined PCI DSS reports out of the box, providing adherence with security controls. It also tracks specific items, such as "Top suspicious users," that map directly to common PCI DSS requirements.

HOW EXABEAM CAN HELP

The Exabeam Security Intelligence Platform, a next generation SIEM, provides your organization with comprehensive, end-to-end detection, analytics, and response capabilities—all from a single security management and operations solution. Its advanced machine learning architecture ingests and analyzes data at any scale—all at a predictable set cost.

Exabeam provides your security and compliance personnel with a means to identify, track, and attest to all activity, thereby eliminating data loss risk and potential non-compliance with regulations and internal policies. Being a suite of tightly integrated solutions, the Exabeam Security Intelligence Platform delivers:

- Unlimited compliance logging and reporting via Exabeam Data Lake
- Early, accurate threat detection using Exabeam Advanced Analytics' behavioral analysis
- Effective, automated incident response offered by Exabeam Incident Responder

EXABEAM SECURITY INTELLIGENCE PLATFORM

UNLIMITED COMPLIANCE LOGGING AND REPORTING WITH EXABEAM DATA LAKE

Monitoring and analyzing events—as well as having continuous visibility to maintain compliance—are a crucial component of PCI DSS. Exabeam Data Lake is a high-performance, modern data management system that can be deployed alongside, or as a replacement for, traditional log management or SIEM systems.

Data Lake is a horizontally scalable collection, indexing, and visualization platform for log and machine data. Built atop open-source technologies such as ElasticSearch and Apache Kafka, it integrates them in a thoroughly modern log management solution. And vetted by such large enterprises as LinkedIn and Netflix, Data Lake offers large scale aggregation, log storage, and unlimited scalability.

Streamlined for completing security workflows, Data Lake's customized ElasticSearch UI makes it easy to use. With its emphasis on the user experience, its dashboard simplifies visualization and report generation. Its wizard-based approach helps analysts quickly build desired visual elements based on sample search queries. And they can easily adjust any visualization to meet their needs.

Data Lake's unlimited log management system can store over seven years of data, enabling comprehensive reports to internal compliance stakeholders and external auditors. Predefined PCI DSS reports, such as "Failed VPN Logins" and "Remote Session Timeouts," makes it easy to prove compliance to any auditor—and helps maintain continual security monitoring afterward. In addition, its predefined reports can be fully customized to meet specific auditor requests.

PREDEFINED COMPLIANCE REPORTS

EARLY, ACCURATE THREAT DETECTION WITH EXABEAM ADVANCED ANALYTICS

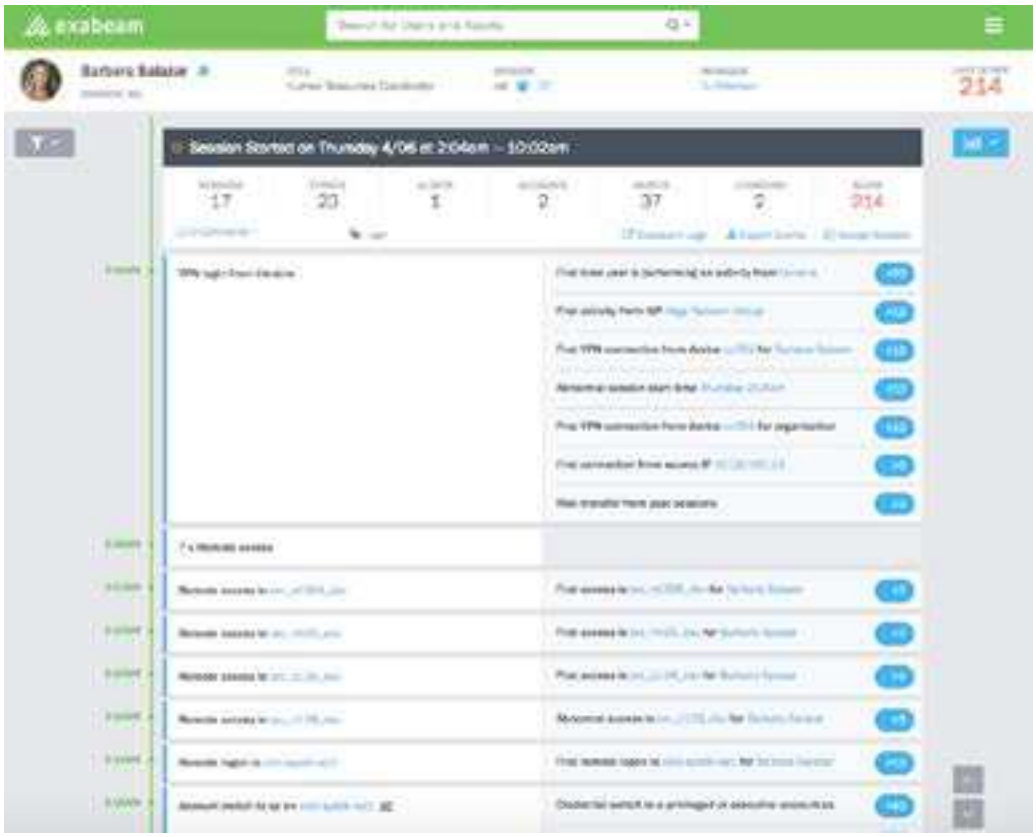
Ensuring rapid threat detection is a key PCI DSS requirement. It also emphasizes continuous account monitoring—especially for privileged users and third-party vendors having special access. But such credential use can often appear legitimate, such that malicious activity potentially goes unnoticed. For every anomaly, Advanced Analytics provides context for security teams to take quick, decisive action.

Supporting real-time risk scoring, Exabeam Advanced Analytics detects insider threats, compromised accounts, data loss, and other advanced threats via machine learning and behavioral analysis. It also accurately models alert behavior from other security solutions.

Advanced Analytics establishes a normal behavior baseline for all organization users and assets—including communication patterns, ports and protocols used, and operating activity. After baseline comparison, new activities are reported as anomalies if deemed inconsistent. A pre-constructed session timeline is created for each detected incident, thereby automating analyst investigations. Proactive analysis is made both easier and faster.

PCI DSS emphasizes the importance of continuous account monitoring, —especially that of privileged users and third-party vendors who have special access. However, such credential use can often appear as legitimate business, resulting in malicious activity potentially going unnoticed.

Advanced Analytics detects anomalies, by accurately modeling the behavior of users, entities, and even alerts from other security solutions. Being able to reveal anomalous activity in this way enables Exabeam to provide context for security teams to take quick, decisive action.



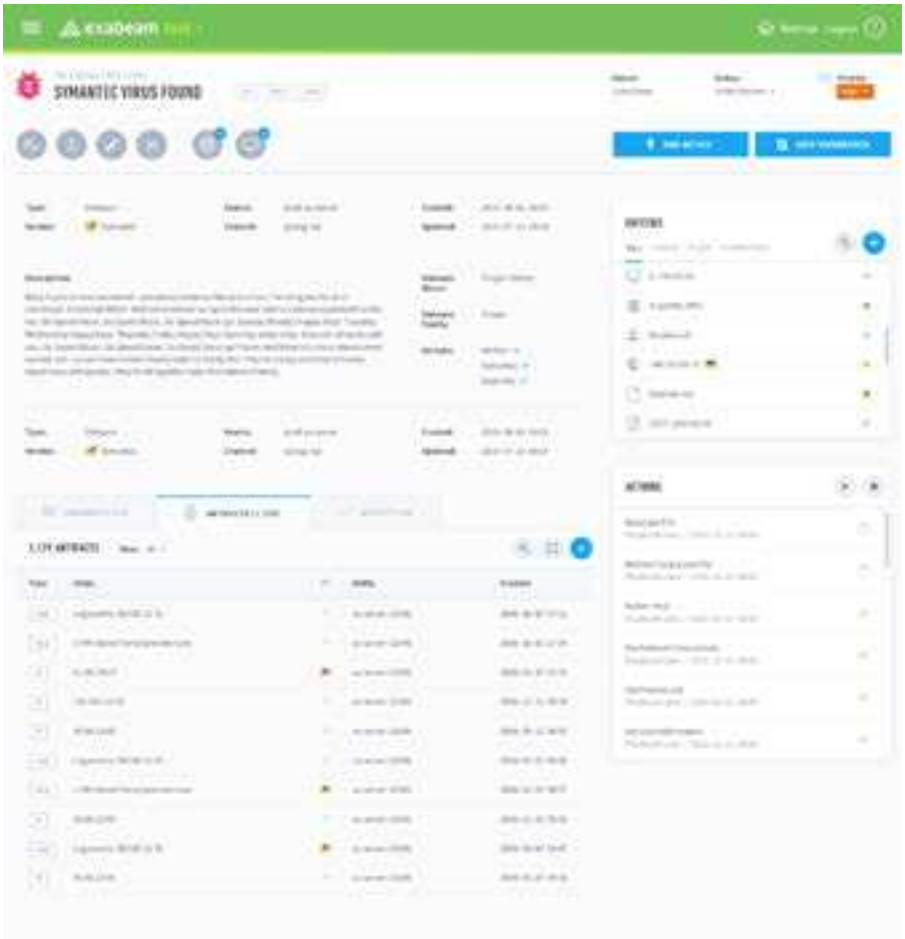
RAPID INVESTIGATION WITH PREBUILT TIMELINES

EFFECTIVE AUTOMATED INCIDENT RESPONSE WITH EXABEAM INCIDENT RESPONDER

Another tenet of PCI DSS is to quickly and effectively respond to any incident that may occur. By way of security orchestration and workflow automation, Exabeam Incident Responder can investigate, contain, and mitigate security incidents in a semi- or fully automated manner. In doing so it leverages prebuilt API integrations with IT infrastructure and security solutions. Eliminating tedious, manual tasks frees security teams to work on more important, value-add activities.

With Exabeam's comprehensive security orchestration:

- Security products, log management systems, data lakes and UEBA tools are natively integrated. Prebuilt API integrations are able to programmatically pull data from, or push actions to, hundreds of third-party IT and security infrastructure solutions
- Automated response workflows trigger corrective actions using existing security solutions. These range from being passive (analyst notification), informational (warning emailed to an employee), to full force (access lock down and response instigation)
- Teams are enabled to ingest detected incidents and fact-based security alerts to quickly and easily initiate and manage breach investigations. Rapid investigation and response from a centralized console for enterprise security and PCI-compliance stakeholders is enabled
- Exabeam's intuitive UI lets even junior analysts understand and take action on threats—unlike existing triage and case management systems used by most SOCs.



DRILL-DOWN INCIDENT DETAILS

MAPPING EXABEAM FUNCTIONALITY TO PCI DSS REQUIREMENTS

The following table specifies how Exabeam supports the twelve PCI section requirements.

PCI DSS REQUIREMENT	EXABEAM PCI CAPABILITIES
1: Install and maintain a firewall configuration to protect data.	
1.1 Establish firewall and router configuration standards.	Exabeam collects and centrally stores logs from various data sources, including internal and external firewalls. It does this to generate comprehensive reports that detect devices and services that may allow connections between an untrusted network and other system component. Exabeam also monitors configuration changes to firewalls and routers to provide reports that help develop firewall and router configuration standards.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Exabeam can collect and analyze logs from corporate firewallsto determine unusual activity or unauthorized access. Exabeam provides details of allowed/ denied network traffic between the DMZ environment and the organization's internal network environment with various out-of-the-box, as well as customized, reports.
1.3 Prohibit direct public access between the internet and any system component in the cardholder data environment.	Exabeam provides rules, alerts, investigations, and violation reports to support requirements 1.2 and 1.3.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Centralized logging of firewall activity helps Exabeam facilitate the creation of security policies and procedures. Exabeam also identifies anomalous activity by modeling firewall logs to look for unusual user and entity behavior that could be indicative of threats. Finally, the solution provides prebuilt reporting and notification to alert affected parties.
2: Do not use vendor-supplied defaults for system passwords and other security parameters.	
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Malicious insiders often use default configurations and other default settings, user accounts, and passwords to compromise systems. Exabeam monitors, logs, and reports on accounts having default passwords, those having passwords that don't expire, etc. Exabeam also monitors anomalous activities performed by service accounts that typically have default configurations and higher level of privileges.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Exabeam can set rules to monitor password and configuration changes to network traffic. It can also provide reports for insecure protocols, services, scripts, etc.

PCI DSS REQUIREMENT	EXABEAM PCI CAPABILITIES
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	Exabeam creates a highly accurate inventory of all in-scope network systems and accurately identifies workstations, servers, privileged accounts, and executive accounts, as well as the owners of each. Exabeam also supports users to provide a list of PCI systems and databases requiring a higher level of scrutiny. Exabeam can pull in information from various sources such as Active Directory (AD) and Configuration Management Database (CMDB), enriching it with data science and modeling to provide greater insights.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Exabeam detects use of shared administrator passwords or dormant admin passwords/accounts. This is especially important if organization policy requires minimal use of shared accounts. Exabeam can identify first-time or unusual behavior of scripts, drivers, etc., as these are often indicators of new malware. Exabeam provides relevant reports and alerts to notify all affected parties.
3: Protect stored data.	
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Exabeam monitors users who access critical systems or restricted network zones, creating an access audit trail. Exabeam provides various tools to monitor all logs from PCI database and build reports to identify anomalies in the cardholder environment.
4: Encrypt transmission of cardholder data across open, public networks.	
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open public networks.	Exabeam can monitor and report unauthorized or unencrypted services, such as passwords sent in clear text, to ensure that only the proper protocols are used in the cardholder data environment.
5: Protect all systems against malware and update anti-malware applications.	
5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).	While Exabeam is not itself an antivirus or antimalware system, it's able to ingest and model data from such systems to provide significant detection benefit. For example, if someone disables an antivirus or antimalware system, Exabeam alerts and notifies all relevant parties. Exabeam significantly improves the effectiveness of these solutions by combining their data with that of other security tools for holistic visibility.
5.2 Ensure that all antivirus mechanisms are current, actively running, and generating audit logs.	Antimalware systems can crash, could be purposely disabled, or simply detuned because of too many alerts. Exabeam can ensure that these systems are running and that they're not disabled. Additionally, Exabeam models antimalware systems behavior to make them more effective and to reduce false positives. It generates audit logs, as well as provides many out of the box reports in support of requirement 5.2.

PCI DSS REQUIREMENT	EXABEAM PCI CAPABILITIES
5.3 Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Exabeam can run reports to detect whether antivirus protection is disabled on a system and send alerts to notify relevant parties. While PCI DSS addresses having a signature-based known threat approach, it's equally important to protect against unknown, zero-day threats. Exabeam delivers advanced threat detection through a combination of machine learning and AI models, combined with a unique session data model.
6: Develop and maintain secure systems and applications.	
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	Exabeam uses sources such as reputation and threat intel feeds, in addition to management systems logs for security vulnerability information. Exabeam provides a unique session data model that supports real-time risk scoring and ranking.
6.3 Develop internal and external software applications in accordance with PCI DSS (for example, secure authentication and logging) based on industry standards and/or best practices and incorporate information security throughout the software development lifecycle. 6.4 Follow change control procedures for all changes to system components.	Exabeam provides visibility and reports for logs written by custom software. Exabeam also automatically identifies systems by role. Exabeam can detect violations, such as a dev/test account used in production, or a separation of duties violation where a user may violate a policy, obscuring the violation by using multiple accounts.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.	Exabeam analyzes and models vulnerability and log information for public facing applications—including custom application logs—and monitors them to ensure that applications are secure. Exabeam also monitors user and administrator activities in cloud environments, such as Azure and AWS, and within cloud applications (e.g., Office 365). Using behavioral analysis, Exabeam can detect and identify new threats and vulnerabilities, including phishing, compromised credentials, and malware.
7: Restrict access to data by business need-to-know.	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Access control systems can easily be misconfigured, allowing users access to forbidden systems. As employees change roles over time, they often retain access privileges they no longer need or should have. Exabeam can ingest and analyze role, identity, and access control information in real-time to quickly detect violations. Exabeam logs and models data to ensure that access anomalies don't occur.

PCI DSS REQUIREMENT	EXABEAM PCI CAPABILITIES
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	Exabeam collects data for access to cardholder systems and data, changes in permissions and access rights, and suspicious behavior in real-time. Investigations can be rapidly performed for any suspected compromises to PCI DSS protected data. Shared account use can be easily spotted, as well as afterhours access or unusual account access frequency. It can track actions even as a user changes devices or account identities.
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Exabeam can monitor policy enforcement by alerting and generating reports if any user is in violation, and can identify violations across multiple user accounts. Exabeam can produce—on demand or as it unfolds—the entire chain of events leading to any potential security violation, across file systems, email systems, web systems, etc. Exabeam also provides relevant reports and alerts to notify all affected parties.
8: Assign a unique ID to each person with computer access.	
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.	Exabeam provides account management activity details, such as account creation, account deletion, and account modification via reports and alerts. In relation to account sharing, Exabeam can monitor same account password accesses from different locations/IP addresses. It also provides details on vendor account management and authentication activity via investigations and reports.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.	Exabeam can identify user account risk by highlighting accounts having non-expiring passwords, shared accounts, and administrators across local, domain, and cloud accounts. Exabeam provides rules and alerts for account violations.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Exabeam, in partnership with MFA vendors, can monitor and restrict access to application and data for accounts displaying risky or anomalous behavior.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods.	Exabeam can generate alerts and reports when shared, dormant, or generic accounts and passwords are detected.
9: Restrict physical access to cardholder data	
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Exabeam supports physical access control (e.g., badge reader) logs and can link badge access to data access for any given user. With Exabeam, access patterns can be visualized; anomalous or unauthorized activities can be modeled and reported, with alerts being generated.

PCI DSS REQUIREMENT	EXABEAM PCI CAPABILITIES
10: Track and monitor all access to network resources and cardholder data.	
10.1 Implement audit trails to link all access to system components to each individual user.	Exabeam tracks and monitors all access to network resources and cardholder data. It supports log analysis, including successful and invalid login attempts. And it presents both audit trails and contextual reporting information to auditors and security personnel.
10.2 Implement automated audit trails for all system components to reconstruct events. 10.3 Record at least the following audit trail entries for all system components.	Exabeam automates collection, centralization, and monitoring of logs from servers, applications, security, and other devices. Exabeam provides alerts and reports on authentication failures from default, disabled, terminated, and privileged accounts. It provides details regarding user access failures/successes to audit log files, cardholder data files, system-level objects, and applications via out-of-the-box as well as customized reports. Exabeam also provides details of privileged account management such as creation, deletion, modification, authentication failures and successes, granting/revoking of access, privilege escalation, and failures/successes to access files, objects, and applications.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	Exabeam can review logs and security events from various system components and perform its analytics continuously, 24×7. Exabeam detects violations as they occur (rather than after-the-fact) during a daily log review, provide real-time visibility into all logs, and alert relevant parties about suspicious access to critical systems.
11: Regularly test security systems and processes.	
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.	Exabeam can ingest data from vulnerability scans created by various sources—including logs from IDS, IPS, and other PCI systems—to create visualizations and dashboard that help detect compromised security controls. Exabeam can provide reports and alerts for suspicious IPS and IDS activity.
12: Maintain a policy that addresses information.	
12.3 Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.	Exabeam provides data and centralized intelligence needed to develop policies for critical technologies. Exabeam provides alerts and reports on account management activity, authentication successes or failures, remote session overview, failed VPN logins, and remote session timeouts.

PCI DSS REQUIREMENT	EXABEAM PCI CAPABILITIES
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	Exabeam provides an automated incident response plan via security orchestration and workflow automation. Exabeam can be rapidly deployed within hours of a breach detection, and can provide comprehensive investigation timelines—often before an external consulting firm has completed writing their contract.

CONCLUSION

With Exabeam's Security Intelligence Platform, organizations handling payment information can easily and efficiently comply with PCI DSS regulations. They can:

- Benefit from a central, scalable logging platform, where all collected log types support compliance initiatives
- Detect and control all privileged, shared, and executive accounts
- Ensure that users only have access to systems that are inline with their roles and policies, and that violations are immediately detected
- Track and monitor all privileged, administrative, executive, and unusual access to sensitive systems such as databases, file shares, applications, and cloud/SaaS services.
- Uniquely identify all users, even if they attempt to obscure their identity via device or account switching
- Analyze and identify all anomalous behavior, whether by privileged, regular, or machine accounts, and then alert and assist in investigation of such activity
- Benefit from prebuilt PCI reports to help meet compliance objectives

Effective monitoring of access controls is an excellent method for implementing PCI DSS. Other regulations, such as Sarbanes-Oxley (Section 404), also require process and information controls. In deploying the Exabeam Security Intelligence Platform—with its built-in analytics and models for detecting data control violations—organizations of any size can help ensure the security of client card information and improve compliance, all with lower cost and effort.

ABOUT US

Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information. The Exabeam Security Intelligence Platform uniquely combines a data lake for unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products. The result is the first modern security intelligence solution that delivers where legacy security information and event management (SIEM) vendors have failed. Built by seasoned security and enterprise IT veterans from Imperva, ArcSight, and Sumo Logic, Exabeam is headquartered in San Mateo, California. Exabeam is privately funded by Lightspeed Venture Partners, Cisco Investments, Norwest Venture Partners, Aspect Ventures, Icon Ventures, and investor Shlomo Kramer. Follow us on Facebook, Twitter, and LinkedIn.