Simplifying PCI Compliance with the Preempt Platform

Introduction

The Preempt Platform allows organizations to proactively enforce policies based on identity, behavior, and risk. The ability to build highly flexible policies, while also delivering real-world enforcement makes Preempt uniquely capable of meeting a wide variety of the requirements established by PCI-DSS 3.2.1. This document provides a high-level introduction to how Preempt capabilities can be applied to various PCI requirements.

Build and Maintain a Secure Network and Systems

Requirement 1: Install And Maintain a Firewall Configuration to Protect Cardholder Data

Preempt provides a potential compensating control to a traditional firewall by enforcing access based on identity, role, ownership and more in addition to traditional elements such as network locations. Segmentation based on identity lets organization tightly control access to the cardholder data environment. Furthermore, Preempt can enforce policies to protect router configuration files and control access from WiFi network segments.

- Relevant PCI-DSS Requirements: 1.2, 1.2.1, 1.2.2, 1.2.3

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Preempt continuously monitors all passwords in the environment including based on data from well-known breaches, password dictionaries, and vendors defaults. The system also restricts access to services based on membership, can force password changes for non-compliant passwords, and even trigger additional identity controls such as MFA based on policy. In fact, MFA can be used as an additional control to protect any network asset or service to easily protect any insecure applications or protocols. Preempt also maintains an always-up-to-date inventory of all entities in the environment which can easily be analyzed in terms of group and risk.

- Relevant PCI-DSS Requirements: 2.1, 2.2, 2.2.1, 2.2.2, 2.2.3, 2.2.5, 2.4

Maintain a Vulnerability Management Program

Requirement 6: Develop and Maintain Secure Systems and Applications

Preempt constantly monitors systems behavior in real time, and detects vulnerabilities that don't have a patch and are commonly used to compromise accounts and steal data. Examples include Pass-the-Hash, Skeleton Key, Forged Pack, use of stealthy administrators, use of well known attack tools and more. All entities are automatically scored by risk and can be controlled based on this risk score. Additionally, Preempt can add a second authentication factor to any application and or network resource using Kerberos or LDAP for authentication and by that turning it into a secure authentication.

- Relevant PCI-DSS Requirements: 6.3, 6.3.1, 6.4.1, 6.4.2, 6.4.3

Implement Strong Access Control Measures

Requirement 7: Restrict Access to Cardholder Data by Business Need To Know

Preempt can segment and add access control to network resources based on roles, risk levels, activity, network locations and many other parameters resulting in a flexible rule base that adapts to almost any scenario. Preempt can locate all user and service accounts on the network and identify privileged accounts to ensure a least privileged model. Preempt policies can restrict access to systems and computers based on administrative and/or business roles. With the use of Preempt profiling and Threat Hunting capabilities, it is possible to determine if users need to access specific systems in order ito complete their work. Preempt can help setting network access authentication controls on any network resource that uses Kerberos or LDAP for authentication as well as restricting the usage of vulnerable NTLM protocol in the network.

- Relevant PCI-DSS Requirements: 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3

Requirement 8: Identify and Authenticate Access to System Components

Preempt adds MFA to any network resource or application without the need to change it's code. Various conditions can be added to the policy basing this on account attribute, risk, subnet or other parameters and applying different actions based on the goal. This achieves network segmentation which is based on identity.

Password management is made easy because Preempt can identify weak and stale passwords and require password resets and session re-authentication or lock-out. Preempt allows for you to implement flexible password policy by removing inactive users, managing remote access credentials, limiting repeat access attempts, setting lockout times, and requiring MFA for all remote and administrative access.

Preempt detects shared accounts and it allows to make service accounts accountable by setting a human administrator as the authorizor for their activity. Preempt also detects elevation of rights, creation of new privileged users accounts, automatically detects and tracks unused stale or dormant accounts.

Preempt monitors access activity and constantly process this data to detect security events such as excessive access, anomalous access, activity from abnormal network locations and or geographical locations, detection of attack tools and much more.

- Relevant PCI-DSS Requirements: 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.3, 8.3.1, 8.3.2, 8.4, 8.5

Regularly Monitor and Test Networks

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

Preempt audits all access requests to any entity on the network. This information is based on analysis of actual network traffic and is thus not subject to log manipulation by an attacker. The solution also detects any changes to AD accounts, creation of new accounts, rights elevation and other types of events. Preempt monitors access activity and constantly process this data to detect security events such as excessive access, anomalous access, activity from abnormal network locations and or geographical locations, detection of attack tools and much more.

- Relevant PCI-DSS Requirements: 10.1, 10.2, 10.2.3, 10.2.4, 10.2.5, 10.4, 10.6, 10.6.1

Requirement 11: Regularly Test Security Systems and Processes

Preempt continuously assess the network configuration for known vulnerabilities such as weak passwords, exposed passwords in the sysvol, uses of suspicious protocol implementations, stealthy admins, new accounts, use of pass-the -hash and other logical vulnerabilities. This information can be used to augment the scanning reports from traditional vulnerability scanners, which don't monitor for these issues. Preempt can be used as a continuous prevention and detection solution which goes beyond the common attack vectors detected by a signature based solutions. This includes compromises of accounts with Pass-the-Hash, Pass-the-Ticket, Forged PAC, Over-Pass-the-Hash, uses of credential spraying techniques and many more which aren't detected by a traditional solutions.

- Relevant PCI-DSS Requirements: 11.2, 11.3.2, 11.4

Maintain an Information Security Policy

Requirement 12: Maintain a Policy that Addresses Information Security for all Personnel.

Preempt continuously assesses risk of the organization as well as for individual users and entities. Preempt automatically classifies entities in the network based on role, use and many other parameters which allow the organization map the critical assets and set policy on them.

Preempt also enables setting human authorizers for accounts - this means that when authorized account try to access specific environment the approval process can be automated and authorization must be granted explicitly. This can be applied to internal users as well as external 3rd party users such as vendor support when they connect remotely even after they passed VPN authentication. Preempt can add additional factor to any network resource including application which uses kerberos or LDAP for authentication including for any remote access.

- Relevant PCI-DSS Requirements: 12.2, 12.3.1, 12.3.2, 12.3.3, 12.3.9

Summary

This document provides an overview of how the Preempt platform can support your compliance with the PCI-DSS. If you have questions or would like to learn more about specific sections of the standard, requirements, and controls, we encourage you to reach out at info@preempt.com or contact your Preempt account manager.