PCI Policy and Procedure Design Service

Service: PCI Policy and Procedure Design Service
Date: September 2018
Order Code: Contact Professional Services Management Team at PS@extremenetworks.com

Extreme Network's PCI Policy and Procedure Design service helps customers establish the necessary set of information security policies and dependent procedures that fulfill Requirement 12 of the Payment Card Industry (PCI) Data Security Standard (DSS). This service defines new policies where gaps exist with the requirements established by the PCI DSS and reviews existing policies for compliance.

NOTE: Extreme Network's PCI Planning and Assessment service is a prerequisite for this service.

Our Responsibilities

Overall Scope

Under this Service, Extreme will:

- Prepare a Scope of Delivery (SOD) and project plan with the customer team.
- Complete a policy review of the customer's existing Information Security policies associated with the Cardholder Data Environment (CDE).
- Interview customer staff to determine operations requirements, roles and responsibilities, data owners, and other questions related to business processes.
- Interview customer staff to determine level of security policy awareness.
- Agree with customer on the set of security policies to be written.
- Provide guidance for required policy documents.
- Prepare and present an executive summary of the recommended actions.

Project Coordination

We will designate an Engagement Manager and, as part of the pre-on-site phase, coordinate logistics and scheduling with the customer's Point of Contact (POC) for performing the service.

Scope of Delivery (SOD)

Prior to beginning the engagement, Extreme will prepare and deliver an SOD, including a service project schedule which will define the scope and boundaries for the services and provide detailed information about the service content to be performed and delivered as part of the project.

Service Process

During the service engagement, Extreme will:

Conduct Off-Site, Pre-Policy Assessment Activities With Customer Team

- Schedule a project kick-off meeting.
- Conduct SOD development meetings with customer team, leading to completion, delivery and customer approval of the project SOD.
- Prepare the project schedule.
- With customer, determine if sufficient current information is available from Extreme Network's PCI Planning and Assessment service.
- Customer will provide:
  - Existing security policies and practices in the customer's organization.
  - Organizational structure with departments and staff involved in CDE processes.

Conduct On-Site Reviews with Customer

- Review business environment to determine scope and depth of the required PCI security policies.
- Conduct staff interviews to determine PCI-related security policies.
- Perform document review for policies currently in practice.
- Establish types of documentation in use.
- Examine relationship between documentation and security practices.

- Determine documentation maintenance cycles.
- Identify CDE assets to be protected.
- Identify roles and responsibilities by job description and document existing access levels to CDE.

Conduct Off-Site Data Analysis, Policy, and Procedures Development

- Analyze review data to determine the policy or set of necessary policies.
- Identify new documentation to be created and documentation to be updated.
- Map policies, procedures and documentation to PCI DSS requirements.
- Individually address PCI DSS policy gaps identified in Extreme Network's PCI Planning and Assessment service and document closure through service deliverables.
- Provide policy and procedure guidance to customer.

Deliver Executive Report and Conduct Project Closeout

- Create an executive report.
- Deliver presentation.
- Conduct project closeout.
  - Identify open actions and plan for resolution.
  - Complete resolution of open actions.
  - Obtain customer acceptance (project sign-off).

Customer Responsibilities

Confirmation of Scope

Customer will receive and must acknowledge in writing the PCI Policy and Procedure Design service SOD and terms of service provided by us in advance of us beginning this engagement.

Contacts

Customer must appoint at least one (1) project POC responsible for coordinating logistics, schedules and technical information with our Engagement Manager. The POC must be knowledgeable of the project objectives and able to assist our Engagement Manager in answering any technical or business process questions. The POC must also be empowered to act for the customer where approvals of our deliverable are required during the service engagement. Customer's partners, consultants or any third parties involved in the project shall likewise provide access to their resources, and shall not restrict access by us to customer resources.

Service Questionnaire

Customer is responsible for working with us to complete the service questionnaire and all responses thereto as part of the requirements gathering portion of the service.

Access to Resources

Customer must provide appropriate access to the physical sites and personnel to enable us to perform the service. Customer is responsible for all fees incurred, including labor costs and any customer-contracted third-party services, to provide such access.

Access to Essential Documentation

Customer must provide access to applicable documents and other written information required by us to perform this service. Customer must also provide us with specific information pertaining to the IT hardware and software associated with payment card data in transit or at rest.

PCI Planning and Assessment

Extreme Network's PCI Planning and Assessment service is a prerequisite for this service. If Extreme Network's PCI Planning and Assessment service has not been performed, customer agrees that it will be conducted by us as an addition to the scope of this service, at additional charge. We will not implement a third-party design with this service.

Access to Network and Security Information

Customer must provide us with access to required documentation to assist in our understanding of customer's existing CDE and security design. Such documents may include, but are not limited to:

- Network design documents; network architecture standards, policies and guidelines.
- Security policies and procedures; security architecture and access control documents.
- Results of past vulnerability sca.ns, penetration tests and security assessments.
- Network management systems definition, security software update processes, configuration management plans, data backup and off-site storage details, and definition of CDE-related services performed by third parties.

Project Support

Customer must complete any and all tasks assigned by us as part of the service engagement in a timely manner in keeping with the overall engagement schedule.

Safety Rules

Customer must provide any site safety rules to Extreme in advance of the engagement.

Administrative Resources

To facilitate the on-site portion of this service, customer must provide reasonable office space, including customer's standard office furnishings, telephone with voicemail, Internet access, access to mail and e-mail systems, access to meeting/conference room, parking at or near the facility where the office space is provided, and such other reasonable requirements identified by us. Customer is responsible for all costs incurred with the use of these amenities.

Exceptions

Customer must inform us of any exceptions or specific requests during the kick-off meeting. For example, if the customer adheres to ISO 27002 standard, it needs to maintain compliance while addressing the PCI DSS policy development.

Limitations and Restrictions

1. Extreme Network's PCI Policy and Procedure Design service does not guarantee the security of the customer's cardholder data. Customer bears full responsibility at all times for the protection of this data. We disclaim all responsibility, financial or otherwise, for breaches of security that compromise or potentially compromise customer or its customers' cardholder data. See Extreme Network's terms and conditions of service for additional details.

2. Extreme Network's PCI Policy and Procedure Design service does not include a PCI DSS audit. This service establishes PCI DSS-specific (Requirement 12) information security policies and recommends procedures for implementing them. The policies are prepared by us in response to gaps identified in a PCI DSS assessment. Customer is responsible for completing a PCI DSS audit following completion of this service.

3. Extreme Network's PCI Policy and Procedure Design service does not include implementation of the Information Security policies established by this service, or testing of recommended procedures. Customer is responsible for implementing any new or revised policies recommended by us through this service.

4. Service delivery and documentation is available in English only unless otherwise agreed to by us in advance in writing.

5. This service requires at least four (4) weeks advance notice from the acceptance by us of a purchase order for planning the on-site work.

6. Customer can request changes to this service. However, any such changes must be confirmed in writing and signed by authorized representatives of both the customer and us. A reasonable price adjustment may be made if any change affects the time of performance or the cost to perform the services.

7. If delays occur in our performance of the PCI Policy and Procedure Design service that are caused by the customer's actions or omissions during the project, we reserve the right to modify the performance schedule or identify a reasonable increase in the service price.

Availability

To check availability in a particular country or for further details, please contact the Professional Services Management Team at PS@extremenetworks.com.

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact / Phone +1-408-579-2800