

Rapid PCI Security Assessment Service Extreme Networks Security Services

Service: Rapid PCI Security Assessment

Version: 1.0

Date: September, 2018

Order Code: PS-SEC-PCI

Overview

Extreme Networks Rapid PCI Security Assessment is a security planning and assessment consulting service that helps customers proactively review compliance with Payment Card Industry (PCI) Data Security Standards (DSS) requirements and protect payment card data. During this service, an Extreme Security Consultant will examine your current Cardholder Data Environment (CDE) diagram that documents all connections to cardholder data and shows cardholder data flows across systems and networks. After a review of the CDE, a security scan will be performed to identify potential vulnerabilities that could be exploited. Any vulnerabilities identified during the assessment are included in the final report provided to the customer at the conclusion of the service—along with recommendations for addressing the vulnerabilities.

Rapid PCI Security Assessment (PS-SEC-PCI)	Service Scope
Cardholder Data Environment (CDE) Review (Customer Provided)	Included
Internal Vulnerability Scan IP Addresses (Intrusive/Non-Intrusive)	Up to 50 IP Addresses
Assessment Report	Included
Physical Location	1
Order Number Availability	PS-SEC-PCI North America

NOTE: This service has very specific limitations detailed below, in order for to it to be accomplished in the allocated time frame.

Description of Services

Overall Scope

As part of this Service, Extreme Networks will provide:

Cardholder Data Environment (CDE) Review

- Customer provided CDE network diagram for one physical location.

- All connections to cardholder data including wireless networks.
- Customer provided data flow diagram.

Timeline: 1 day

Full Internal Vulnerability Scan IP Addresses (Intrusive/Non-Intrusive)

- Perform a full internal scan for security vulnerabilities.
- Up to 50 IP addresses within the CDE environment (Combined Set).

Timeline: 2 days

NOTE: Network scans will be performed in a Single Pass with all IPs accessible during the scan.

Assessment Report

- Analyze scan data.
- Prepare final report.

Timeline: 2 days

NOTE: The final report will be completed off site and available within five days following the completion of the engagement.

Project Coordination

Extreme Networks will designate a Point of Contact (POC) and, as part of the pre-site stage, coordinate logistics and scheduling with the customer's POC for performing the service.

Scope of Delivery (SOD)

Prior to beginning the engagement, Extreme Networks will prepare and deliver a SOD which includes a service project schedule for the purchased service. Detailed information about the services to be performed as part of the project will be provided.

Service Process

An Extreme Networks Consultant will complete the following process for this service:

Discuss service overview in a kick-off meeting with key stakeholders: Off-Site

- Review the Scope of Delivery.
- Discuss service process.
- Discuss current customer issues related to this service.
- Discuss timeline for deliverables and services.

Data Collection: On-Site

- Extreme will perform interviews with customer personnel.
- Perform vulnerability scans.
- Collect 1 ACL policy.
- Collect existing system configurations.

Data Review: Off-Site

- Review vulnerability tools output data/results.
- Review CDE network diagram.
- Review CDE data flow diagram.

Report: Off-Site

- Document findings and remediation recommendations.
- Deliver a final report that summarizes findings and remediation actions.

Customer Responsibilities

Infrastructure Requirements and Documentation

Prior to the consultant's arrival on site, customer must complete any and all prior infrastructure requirements. In addition, customer must provide Extreme Networks with documentation pertaining to business procedures, IT operations processes, configuration, and network topology details, and security policies/procedure data that is necessary for the service.

Contacts

Customer must provide reasonable access to all necessary resources, including but not limited to site management and team leaders, as requested by the Extreme Networks engagement team, to answer technical questions related to the wired infrastructure. Customers, partners or consultants involved in the project shall likewise provide access to their resources, and shall not restrict access to customer resources by Extreme Networks.

Reasonable Access to Information

Customer must provide Extreme Networks with reasonable access to any information necessary to facilitate operations and administration. Such requests may include temporary network access, passwords, and authorization to examine network traffic using commercial software "sniffing" utilities (provided by Extreme Networks).

Access to Network Infrastructure

Customer must provide reasonable access to network equipment rooms, server equipment and managed infrastructure (such as switches, firewall, and managed devices for the purpose of review/validation). The customer will provide the following:

- Network topology diagrams.
- CDE network diagram.
- CDE data flow diagram.
- Target IP Addresses or Appliance URLs.
- Appliances IDs and MAC Addresses.
- IP addresses and network connection for vulnerability scanning tools.

Limitations and Restrictions

- This service may require at least four (4) weeks advance notice from the acceptance by us of a purchase order for planning the work.
- The service is intended to be delivered in a single location with high-speed access to the assessed infrastructure elements. Multiple physical location will be a custom quote.
- Vulnerability analysis of the WLAN devices is excluded from this service.
- Each section has a specific ESU timeline. Any actions not completed during each portion of the service will require a change order/price adjustment.
- Remediation of product bugs, issues, and feature requests found during the life of this service are outside of the project scope;
- Transmittal of the final report will be via email (password protected document) unless a more secure method is provided by the customer.
- Extreme Networks will not be responsible for the performance or functionality of the assessed systems, nor will it be responsible for the sufficiency, completeness, adequacy or operation of any systems, policies, networks and security features used by the customer.

- **No Guarantee.** Customer acknowledges, understands and agrees that extreme networks does not guarantee or warrant that it will discover all of customer's security events. Extreme networks disclaims any and all responsibility for any and all loss or costs of any kind associated with security events, whether or not they were discovered by extreme networks. Customer agrees not to represent to any third party that extreme networks has provided such guarantee or warrant. Extreme networks disclaims any responsibility for customer's use or implementation of any recommendations provided in connection with the services. Implementation of recommendations does not ensure or guarantee the security of the systems and operations evaluated.
- **Possible Damage or Disruption.** "Customer" acknowledges, understands, and agrees that the equipment provided by or used by Extreme Networks to facilitate performance of the services may impact or disrupt information systems. Except to the extent set forth in the Sections on No Guarantee and Limitation of Liability, Extreme Networks disclaims responsibility for costs in connection with any such disruptions of and/or damage to Customer's or a third party's information systems, equipment, and the information and data, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision or delivery of the Service. Extreme Networks agrees to cooperate with Customer to schedule any such potential damage or disruption around Customer's information technology traffic and use patterns so as to reduce the risk of disruption during working hours.
- Except for personal injury or death, extreme networks total liability, whether for breach of contract, warranty, negligence, or otherwise, will be limited to the direct damages recoverable under law, but not to exceed one quarter of the contract price.

Although the parties acknowledge the possibility of such losses or damages, they agree that extreme networks will not be liable for any commercial loss; inconvenience; lost of use, time, data, good will, revenues, profits or savings; or otherspecial, incidental, indirect, or consequential damages in any way related to or arising from performance of the services by extreme networks.

This limitation of liability provision survives the expiration or termination of the services and applies notwithstanding any contrary provision.

- Your use of the Rapid Wired Security Assessment Service is subject to and conditioned upon your acceptance of Extreme's Professional Services Terms and Conditions, found at: <http://www.extremenetworks.com/company/legal/>. In the case of a conflict between this document any purchase order, or any other document, the terms found in Extreme's Professional Services Terms and Conditions control." No action for contract breach or otherwise relating to the transactions contemplated by this document may be brought more than one (1) year after the date of cause of such action.

Optional/Add-On Services:

In addition to the Services described in Section 1, the customer may choose to add one or more optional services when placing an order.

- Comprehensive wireless/wired Security Assessment (Optional/Recommended Service with comprehensive security assessment service).
- Comprehensive PCI-DSS Wireless compliance review (Optional Service - PCI-DSS Wireless Gap Analysis Service).

Availability

Extreme Networks Services are available worldwide. To check availability in a particular country or for further details, please contact an Extreme Networks Security Services representative.

General Definitions

The following terms definitions govern the scope of the Service described in this Service Description Document:

Configuration

Specific parameters that define End-User Customer specific operational design that relies on the specific functionality of such products. Product configuration is variable and is driven by factors including but not limited to End-User Customer's site-specific information, WLAN or WWAN related parameters.

Contract

The specific Contract, assigned a unique identification number, comprising the Order Acknowledgement, this Service Description Document and the Terms and Conditions.

Customer

The entity purchasing the service from Extreme Networks and/or its affiliates.

End-User Customer

The Customer or the ultimate end user of the Service (if different) whose Products are the object of the Service.

Product

The physical, tangible Hardware purchased from Extreme Networks which includes Software.

Service

The Rapid PCI Security Assessment service described in this Service Description Document.

Software

Any Extreme Networks-provided machine-readable instructions installed on the Product as shipped to the Customer.

Terms and Conditions

The [Professional Services Terms and Conditions](#).