Rapid HIPAA Security Assessment Service

Service: Rapid HIPAA Security Assessment Service
Version: 1.0
Date: September 2018
Order Code: PS-SEC-HIPAA

Service Overview

Extreme Networks Rapid HIPAA Security Assessment is a consulting service that helps customers proactively maintain compliance with Health Insurance Portability and Accountability Act (HIPAA) - Security Rule requirements to protect electronic Protected Health Information (ePHI). During this service, an Extreme Security Consultant will examine your current Healthcare Information Technology (IT) diagram that documents all connections to ePHI data and shows ePHI data flows across systems and networks. After the review, an enterprise tools based security scan will be performed to identify potential vulnerabilities that could be exploited. At the conclusion of the service, a final report will be provided, which will include security vulnerabilities findings, along with recommendations for closing discovered vulnerabilities.

Rapid HIPAA Security Assessment (PS-SEC-HIPAA)	Service Scope
Healthcare IT — ePHI Data Network Diagram 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	PS-SEC-HIPAA

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:

Healthcare IT – ePHI Data Environment Diagram Review

- Review customer provided Healthcare IT – ePHI data flow network diagram for one physical location.
- Review all connections to ePHI data including wireless networks.

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 Healthcare IT environment with ePHI data assets in-scope for HIPAA compliance (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 Results 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 will designate a Point of Contact (POC), to coordinate logistics and scheduling with the customer's POC.

Scope of Delivery (SOD)

Prior to beginning the engagement, Extreme Networks will prepare and deliver a detailed SOD which includes a service project schedule for the purchased service.

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 Networks Will Perform Interviews With Customer Personnel.
- Collect Healthcare It – ePHI Data Environment Diagram.
- Perform Vulnerability Scans.

Data Review: Off-Site

- Review vulnerability tools output data/results.
- Review ePHI network diagram and related data flow.

Report: Off-Site

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

Data Handling

This service doesn't involve capturing or handling ePHI. In the event that ePHI data was captured during the execution of this service, it will be handled pursuant to the agreed upon SOD.

Customer Responsibilities

Confirmation of Scope

Customer will receive and must acknowledge in writing the service SOD and Terms and Conditions provided by us in advance of ordering this 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 Healthcare IT 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.

Access to Network Infrastructure

Customer must provide network access to enable us to connect testing and monitoring tools. This access is required to complete the tasks in responsibilities outlined within the SOD. If direct access is unavailable, customer must provide an appropriate technical resource with network access permissions to accomplish necessary testing and monitoring at our direction.

Safety Rules

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

Project Closure

Upon our completion of all project milestones and deliverables, customer must complete and sign our Customer Acceptance Form (CAF), signifying successful completion of all project activities.

Limitations and Restrictions

- This service is not intended to perform comprehensive HIPAA gap analysis.
- This service may require at least four (4) weeks' 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 & 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 HIPAA 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.

- Healthcare IT HIPAA Gap Analysis and Security Assessment Service (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 HIPAA 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 found at http://learn.extremenetworks.com/rs/extreme/images/Professional-Services-Terms-and-Conditions.pdf