Secureworks®

SERVICE DESCRIPTION

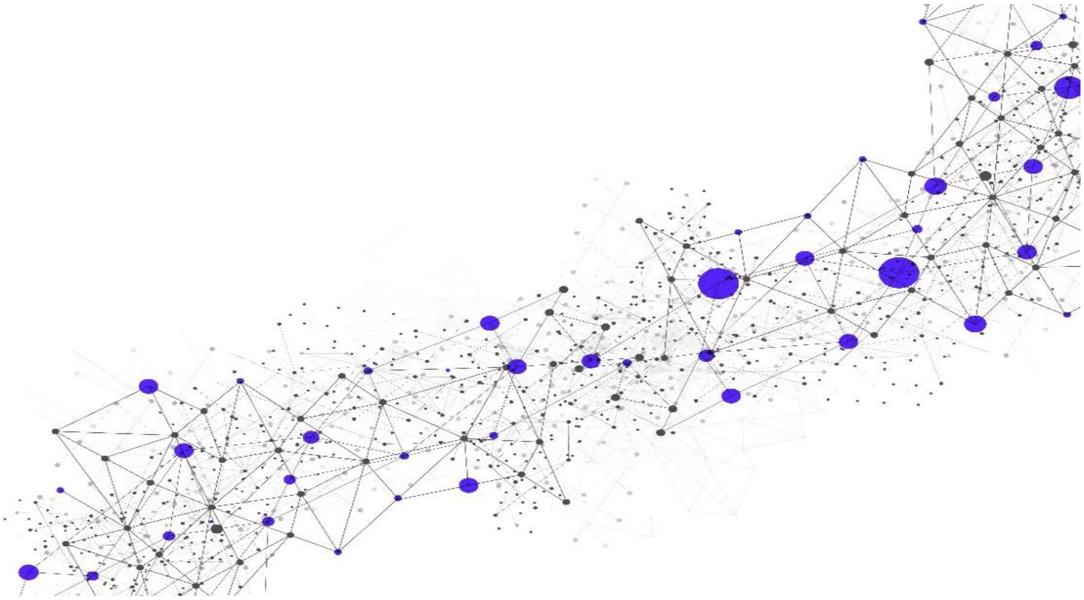
Taegis VDR: PCI Attestation Service

Release Date

August 23, 2022

Version

1.0



www.secureworks.com
A Dell Technologies Company

Global Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
Phone: +1 877 838 7947
Email: info@secureworks.com
Additional office locations: https://www.secureworks.com/about/offices

Table of Contents

Copyright

1 Service Introduction

1.1 Overview

The Payment Card Industry Data Security Standard Attestation Service (“**Service**”) is an add-on service to the Secureworks® Taegis™ Vulnerability Detection and Response (“**VDR**”) Cloud Service. Customer must purchase VDR, which is the software that Customer must use for the Service. All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement.

This Service is for providing support to customers who require attested reports for satisfying Payment Card Industry Data Security Standard (“**PCI DSS**”) requirement 11.2.2, which requires vulnerability scanning for publicly accessible external Assets in the Cardholder Data Environment as specified by the PCI Security Standards Council (“**SSC**”). Secureworks is a PCI SSC Approved Scanning Vendor (“**ASV**”). Secureworks will serve as the ASV that will attest to scan compliance in accordance with the PCI ASV Program Guide.

This Service consists of the following:

- Support for attestation-specific components in VDR
- Reviews of report components
- Attestation of scan compliance

The above-listed components are explained in Section 2, Service Details.

VDR includes a self-service PCI solution that supports the PCI compliance workflows necessary for generating quarterly reports for attestation (workflows include exceptions and false positives). VDR will:

- Indicate vulnerabilities that would result in a failed ASV report
- Allow for false positives, exceptions, and PCI Special Notes to be reviewed by the ASV

Note: This Service is only available in English.

1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder, including meeting the Service Level Agreements (“**SLOs**”) listed further below, are dependent on Customer’s compliance with these obligations. Noncompliance with Customer obligations relative to this Service may result in suspension of SLOs. Customer will do the following:

- Identify PCI in-scope Assets
- Configure scan schedules within VDR
- Ensure Customer has authorization to scan all Assets deemed in scope for the Service
- Execute scans within VDR
- Review scan results and report output for accuracy
- Identify any false positives
- Submit requests to Secureworks through VDR for reviewing false positives
- Submit any required evidence for false positive requests
- Identify any anomalies, errors, or network impacts regarding scan results and adjust scan schedules and network infrastructure as necessary
- Ensure adherence with licenses purchased for the Service
- Modify Customer’s environment to allow scanning
- Develop and maintain a remediation program or strategy
- Remediate vulnerabilities
- Identify and apply patches to hosts
- Submit attestation report requests to Secureworks ASV professionals for signature
- Submit attested reports to acquirers
- Complete PCI SAQ
- Submit SAQ to necessary entities
- Work with a QSA as necessary
- Submit requests to Secureworks through VDR for reviewing exceptions and PCI Special Notes

Customer will also perform the activities described below to enable Secureworks to provide the Service:

- Identify publicly accessible (external) Assets in the card holder data environment; within VDR, tag these Assets and activate the tag for PCI – see instructions within the online VDR documentation for how to tag the Assets (https://docs.ctpx.secureworks.com/vdr/userGuide/generalUse/creating_new_tags/)
- Define and initiate scans to execute continuously or at an interval of Customer's choosing within a 90-day period (see the online VDR documentation for instructions); Customer can also execute ad-hoc scans
- Within VDR:
  - Review scan results, add PCI Special Notes, and conduct re-scans
  - Submit requests for false positives, exceptions, and PCI Special Notes to be reviewed by Secureworks ASV professionals who will assess, then accept or reject
  - When Customer has a passing or failed state that they wish to have attested, Customer will generate an attestation report and submit it for a Secureworks ASV professional to assess, and a Secureworks ASV professional will sign or reject and return it to Customer
  - Customer retrieves signed report and stores it electronically in Customer's environment
- Send the attestation report to Customer's acquiring bank or to Customer's QSA who will prepare, review, and submit the attestation report according to their own process

2 Service Details

2.1 Service Components

The components of the Service are explained in the subsections below.

2.1.1 Support for Attestation-specific Components in VDR

Secureworks will provide support to Customer as needed for this Service. For example, if Customer has an issue with VDR that is specific to the attestation capabilities, then Customer can contact Secureworks using the contact methods indicated within VDR.

2.1.2 Reviews of Report Components

Customer will submit requests to Secureworks for reviews of false positives, exceptions, and PCI Special Notes that become part of Customer's attestation report as applicable to Customer's publicly accessible (external) Assets in the card holder data environment only. Secureworks will review and respond to these requests according to the SLOs defined below. Responses will indicate whether the false positive, exception, or PCI Special Note is accepted or rejected in accordance with the PCI DSS Approved Scanning Vendors Program Guide. Secureworks will also help Customer to understand scan results in support of determining actions to take next.

- PCI Special Notes are evaluated for accuracy and appropriate content.
- If Customer suspects that a finding is a false positive, then Customer can submit the finding as a false positive and if Secureworks (as the ASV) agrees with the supporting evidence, then it will be accepted as a "Pass" for 90 days in accordance with the ASV program guide. At the discretion of Secureworks as the ASV, other exceptions may be granted.

2.1.3 Attestation of Scan Compliance

Customer will conduct activities to produce reports. When required according to PCI DSS requirement 11.2.2, Customer will submit reports to Secureworks for attestation. Secureworks will attest to a maximum of four (4) reports for each 12-month period during the Services Term.

PCI Scanning Reporting – The following PCI-specific information is available to Customer from within VDR and can be included in any attested report:

- ***ASV Scan Report Summary:*** Provides Customer network information while summarizing the PCI scan results. If Customer meets all requirements set forth in the PCI procedures and/or requirements, then the Attestation of Scan Compliance will contain a statement of compliance or non-compliance.
- ***ASV Scan Report Vulnerability Details:*** Provides a detailed and technical view of the scan results and includes a section that categorizes discovered vulnerabilities according to the PCI procedures.
- ***Attestation of Scan Compliance:*** Provides a summary of Customer's network, PCI scan compliance (pass or fail) assertions by Customer, and the ASV that the scan complies with PCI DSS requirement 11.2.2.

PCI Workflow Enablement – The PCI workflows necessary for using this Service are enabled by default in VDR. Secureworks will not attest to any report containing information that is older than 30 days.

PCI False Positive and Exception Handling – Upon request from Customer, Secureworks (the ASV) will review false positives and exceptions. Customer is required to submit any supporting documentation or evidence as required by Secureworks. Evidence may include logs, screenshots, configuration information, or other similar digital evidence. Secureworks will determine acceptance or non-acceptance of the submission and will document these work products per the ASV Program Guide.

2.2 Out of Scope

The information above comprises the Secureworks standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Items listed below are examples of services and activities that are out of scope. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document.

- Engagement of a Qualified Security Assessor ("**QSA**")
- Any PCI DSS requirements that are not within requirement 11.2.2
- Customer's internal Assets (PCI council does not require ASV-certified reporting of Customer's internal Assets)
- Interaction between Secureworks (the ASV) and Customer's QSA
- Modifications to Customer's environment for allowing scanning (Customer must make modifications)
- Assets in excess of the amount licensed for the Service
- Proper scoping of all Assets (referred to as components by PCI DSS) that are included in the PCI DSS scope
- Proactive identification of false positives (Customer must identify all false positives; upon receipt of a review request from Customer, Secureworks will review them)
- Remediation of vulnerabilities in Customer's environment
- Remediation guidance in addition to the guidance already provided within the VDR user interface
- Product support that is specific to VDR, including all features except those specific to this Service

3 Service Level Objectives ("SLOs")

The table below contains the SLOs that are applicable to the Service.

Name	SLO
Reviews of Report Components	Requests for reviewing false positives, exceptions, and PCI Special Notes will be responded to with acceptance, rejection, or request for additional evidence within 5 Business Days.
Attestation Requests	SCWX will respond to the request for attestation within two (2) Business Days.

Warranty Exclusion: While the Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Secureworks makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer's network.

The SLOs set forth above are subject to the following limitations:

- Secureworks schedules maintenance outages for Secureworks-owned equipment that is being used to provide the Service and will provide Customer-designated contact(s) with 24 hours of notice of an outage. The SLOs shall not apply during scheduled maintenance outages.
- The SLOs shall not apply if any act or omission by Customer prohibits or otherwise limits Secureworks from providing the Service or meeting the SLOs, including but not limited to misconduct, negligence, provision of inaccurate or incomplete information, modifications to the Service, or any unauthorized modifications made to any managed hardware or software Devices, by Customer or its employees, or third parties acting on behalf of Customer.
- The SLOs shall not apply to the extent Customer does not fulfill and comply with the obligations and responsibilities set forth within this SD.
- The SLOs shall not apply if customer-side technology (e.g., servers or other components in Customer's environment that Secureworks may need to access in order to deliver the Service) is unreachable due to network connectivity issues, authentication issues, configuration issues, or public cloud downtimes that are outside the direct control of Secureworks.

4 Service Fees and Related Information

Service Fees are based on the number of Internet Protocol ("**IP**") addresses and web applications (Assets) to be scanned; minimum of five (5) Assets for the Service. Customer will receive a maximum of four (4) ASV-signed attestation reports for each 12-month period during the Services Term (one each quarter). Contact account manager or refer to the official terms as stated on Customer's Transaction Document from purchase for the most up-to-date details.

4.1 Invoice Commencement and Related Information

See the Service-specific Addendum or Transaction Document for information about invoice commencement.

5 Additional Information

See the documentation about Taegis™ VDR (https://docs.ctpx.secureworks.com/vdr/) for information about using VDR. Other information is also available, including release notes.

6 Glossary

Term	Description
Assets	An Asset is a server or a website. See Definition of an Asset for details.
Business Days	Business Days for Secureworks global headquarters are Monday – Friday and Business Hours are 8 a.m. – 5 p.m. US Eastern Time, excluding US holidays. Business Days and Business Hours for all other Secureworks locations vary according to local time zone and country.