Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2.1

July 2018

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	CrowdStrike, Inc.		DBA (doing business as):		
Contact Name:	Cayce Beames		Title:	Director, Risk & Compliance	
Telephone:	530-830-8208		E-mail:	cayce.beames@crowdstrike.com	
Business Address:	150 Mathilda Place, Suite 300		City:	Sunnyvale	
State/Province:	CA	Country:	USA	Zip:	94086
URL:	www.crowdstrike.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	CrowdStrike Falcon operating in US-1, US-2, EU-1, and GovCloud including: Device Control, Discover, Falcon for Datacenters, Falcon Forensics, Horizon, Insight, Prevent, Prevent for Home Use, Spotlight, Threat Graph; Falcon X including Intel, Sandbox, Malquery; Falcon Overwatch; Falcon Complete.

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☒ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."*

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed:	CrowdStrike Falcon Network, Forensics Services, On-Premises Falcon Sandbox.

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☒ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Provide a brief explanation why any checked services were not included in the assessment:	CrowdStrike Falcon Network and Forensics Services are separate operational products and teams assessed under a separate Service Provider SAQ where applicable.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	The CrowdStrike products and services addressed by this SAQ are not intended to store, process, or transmit cardholder data. Cardholder data may be transmitted and stored as part of the services offered to the customer, but are incidental to the service. Customers are responsible for ensuring that cardholder data is not transmitted to CrowdStrike.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	The CrowdStrike products and services may unintentionally collect cardholder data through though collection of files and suspected of containing malware, or being involved in regular monitoring of systems for unauthorized or suspicious system behavior or information access. CrowdStrike's Falcon Complete Team team will have access to systems within a customer's (if a merchant or service provider) cardholder data environment in a capacity that could impact the security of cardholder data.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Retail outlets	*3*	*Boston, MA, USA*
AWS and Colocation Facilities	22	Santa Clara, CA USA; San Jose, CA USA; Seattle, WA, USA; San Francisco, CA USA; Rancho Cordova, CA; USA; Hillsboro, OR, USA; Portland, OR, USA; Seattle, WA, USA; Moses Lake, WA, USA; Denver, CO USA; Las Vegas, NV USA; Reno, NV, USA; McCarran, NV, USA; New York, NY, USA; Ashburn, VA USA; Frankfurt, Germany
Crowdstrike HQ	1	Sunnyvale, CA USA
Field Office	22	El Segundo, CA USA; Irvine, CA USA; Columbia, MD USA; Minneapolis, MN USA; St Louis, MO USA; Kirkland, WA USA; Arlington, VA USA; El Segundo, CA USA;Boston, MA, USA;Austin, TX, USA; New York, NY, USA; London, UK; Reading, UK; North Sydney, AUS; Seattle, WA USA; Bucarest, Romania; Aachen, Germany; Dubai, UAE; Tokyo, Japan; Singapore; Pune, India; Gloucestershire, UK

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The Falcon services require the use of an executable file that collects file execution and system metadata and uploads to CrowdStrike's cloud environment in Amazon Web Services. This metadata may also be transmitted and stored within the CrowdStrike colocation data centers. CrowdStrike execution and system metadata is used to detect malware and indicators of attack. Although Falcon does not intentionally collect, process or store credit card data, it may unintentionally collect username and passwords as part of command line execution string data. This may include administrator login credentials of the system being monitored. Additionally, because CrowdStrike provides file analysis services, files not properly sanitized by the customer containing card data may be uploaded to CrowdStrike systems. Because CrowdStrike's Falcon Platform can be used to fulfill a number of PCI requirements either fully or partially, should a customer use those features to address their PCI obligations, the CrowdStrike Falcon Platform will be in-scope for those features used. The data collected by Falcon host is encrypted (AES 128+ bits) and transmitted to Falcon's cloud sensor proxy server (within AWS). Note: CrowdStrike's sensor proxy server begins each client handshake using TLS v1.2 to encrypt transmission data. The transmission is protected against man-in-the-middle attacks as a certificate is pinned to the sensor. Information collected is analyzed for characteristics of how the process interacts with the operating system and other processes that would indicate malicious activity. Data at rest is encrypted using the AES 256bit cipher. Raw data in the User Interface is deleted after 30 days and the remaining summary data after 90 days. Raw data is kept in storage outside of the user interface for at least 1 year. GovCloud customers must obtain a feed of data to keep for a period longer than 90 days. CrowdStrike's access to collected data is limited to employees with a need to know and requires 2 factor vpn and ssh access to specific systems. Access is logged to a central server. All employees receive job specific security awareness training and are required to affirm via signature their adherence to Crowdstrike's and where applicable, customer security policies. Access controls and CrowdStrike's policy management program is reviewed quarterly by the security compliance group and by a reputable 3rd party as part of CrowdStrike's SOC2 Type 2 attestation. Crowdstrike has implemented numerous controls to ensure adequate segmentation of customer data. All sensor data is tagged with unique, but anonymous “Customer ID” and “Agent ID” values

	that conform to the UUID4 format. The Customer ID field, or CID is mapped in a separate provisioning system to a particular customer company name, so the company name is not stored anywhere with the actual event data itself. The Agent ID field, or AID, is assigned randomly any time a sensor connects that does not already have an AID value. From that point forward, the AID is the means by which a specific endpoint is identified. Whenever the sensor connects, one of the events that it sends will provide the current name of the computer, as well as any Active Directory Domain to which it might be joined. We use the most recent computer name for the UI, but the AID is the sole internal identifier for that endpoint. If a sensor is completely uninstalled and reinstalled, or if a machine is reimaged, it will get a new AID upon connection to the cloud. All data access within the system is managed through constrained APIs that require a customer-specific token to access only that customer's data. Event data, which consists of activity relevant to the security posture of the system (e.g., filenames, command lines, process start/stop times, network connection activity, etc.) are stored in dedicated encrypted data stores. Analysis engines act on the raw event data, so they only leverage the anonymized CID and AID values for clustering of results. Whenever data with intelligence value is discovered, such as the presence of an adversary on one or more CIDs, select, authorized employees have the ability look up the company mapping from the CID(s), however, none of that identifying information is used in any external Intelligence product. At most, general information such as an industry sector or geographic location would be used to identify the targeting trends of the attacker in question and to warn our customers to be on the lookout for that tradecraft if their profile matches the victimology of the attacker. The Falcon Complete Team is a a managed service offering where the team operates the CrowdStrike Falcon Platform that the customer has purchased. This includes real-time response services to investigate and eradicate malware and adversary threats. Falcon Overwatch is a service offering where the team seeks out new threat perspectives across the subscribing client's data pool to find and report evidence of current or past attacks against customers. CrowdStrike environments that are in-scope include:

	Facilities, network boundary firewalls and IDS, connections to the storage environment,strong remote authentication and role based access controls, critical system components such as VPNs, web services, access control systems, data storage systems, etc., and operating systems of our platform systems delivering the Falcon services to our customers

Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

Part 2f. Third-Party Service Providers (Continued)

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**
Amazon Web Services	Amazon Web Services (AWS) provides the cloud based hosting and infrastructure used by the Falcon platform
Colocation Facilities	Zayo in Denver, CO and Ashburn, VA; Switch in Las Vegas, Reno, and McCarran, NV; CoreSite in Santa Clara, CA; EdgeConnex in Santa Clara, CA, Rancho Cordova, CA, and Hillsboro, OR; Equinix in San Jose, CA, Seattle, WA, NY, NY, and Frankfurt, Germany; Flexential in Hillsboro, OR; EdgeConneX, Hillsboro, OR; Pittock in Portland, OR; Cyxtera in Moses Lake, WA. Cyrus One, Frankfurt, Germany; Interxion, Frankfurt, Germany; KDDI, Frankfurt, Germany; Maincubes, Offenbach, Germany;
Okta	Authentication service provider for single sign-on

Duo Security	Authentication service provider for multi-factor authentication

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full – The requirement and all sub-requirements were assessed for that Requirement, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the SAQ.
- Partial – One or more sub-requirements of that Requirement were marked as "Not Tested" or "Not Applicable" in the SAQ.
- None – All sub-requirements of that Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the SAQ
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed:	CrowdStrike Falcon operating in US-1, US-2, EU-1, and GovCloud including: Device Control, Discover, Falcon for Datacenters, Falcon Forensics, Horizon, Insight, Prevent, Prevent for Home Use, Spotlight, Threat Graph; Falcon X including Intel, Sandbox, Malquery; Falcon Overwatch; Falcon Complete.

PCI DSS Requirement	Details of Requirements Assessed			
	Full	Partial	None	Justification for Approach (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	☐	☐	
Requirement 2:	☐	☒	☐	**2.1.1, no wireless networks. 2.6, CrowdStrike not a shared hosting provider.**
Requirement 3:	☐	☐	☒	**PAN data is not collected, processed or stored.**
Requirement 4:	☐	☐	☒	**PAN data is not collected, processed or stored.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.4.3, CrowdStrike does not store, process or transmit card data, thus no PANs are used in development.**
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	**8.7 CrowdStrike does not store, process or transmit card data, thus no databases contain PANs**
Requirement 9:	☒	☐	☐	
Requirement 10:	☐	☒	☐	**PAN data is not collected, processed or stored, therefore 10.2.1 does not apply**
Requirement 11:	☐	☒	☐	**11.1.1, No wireless connected to in-scope networks. PAN data is not collected, processed or stored, therefore 11.2.2 does not apply. Scans performed with internal resources.**
Requirement 12:	☐	☒	☐	**12.3.10, CrowdStrike does not store, process or transmit card data. Therefore, no policy specifies this requirement.**
Appendix A1:	☐	☐	☒	**CrowdStrike is not a shared hosting provider.**
Appendix A2:	☐	☐	☒	**CrowdStrike leverages strong cryptography for transmission of sensitive information.**

Section 2: Self-Assessment Questionnaire D – Service Providers

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	November 25, 2020	
Have compensating controls been used to meet any requirement in the SAQ?	☐ Yes	☒ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements in the SAQ identified as being not tested?	☐ Yes	☒ No
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated *November 25, 2020.*

Based on the results documented in the SAQ D noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: (***check one):***

☒	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *CrowdStrike, Inc.* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provide Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	PCI DSS Self-Assessment Questionnaire D, Version *3.2.1*, was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☐	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *(ASV Name)*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **11/25/2020**
Service Provider Executive Officer Name: **Jerry Dixon**	*Title:* **Chief Information Security Officer**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☐	☐	N/A
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	N/A
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	N/A
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections.	☐	☐	N/A