Secureworks®

SERVICE DESCRIPTION

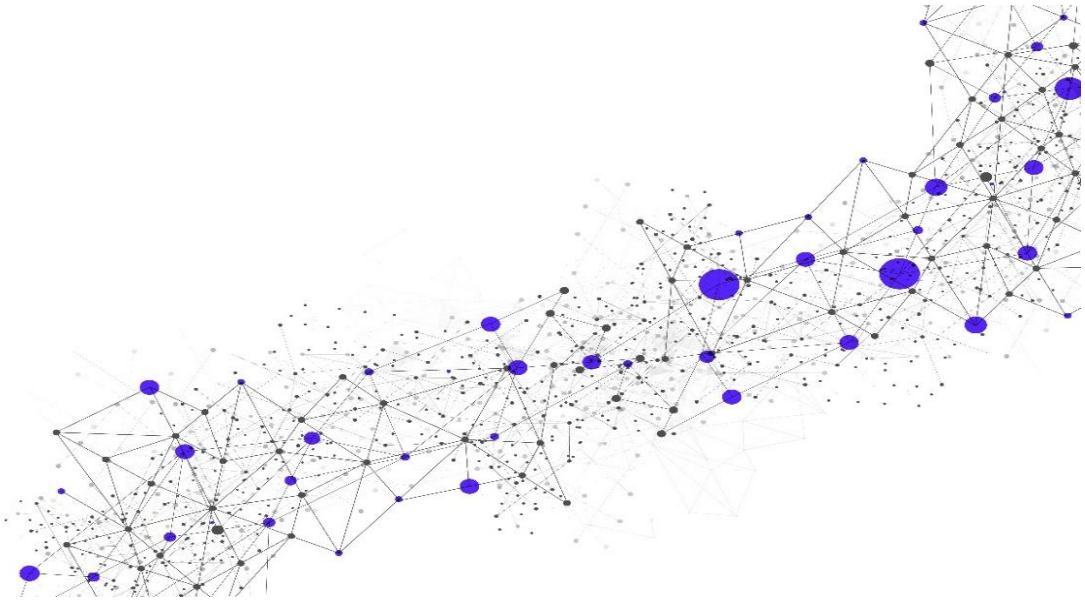
Enterprise Brand Surveillance: Information Brief

Release Date

October 12, 2020

Version

3.0



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

1 Service Introduction

This Service Description ("**SD**") describes the Enterprise Brand Surveillance Information Brief Service ("**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.

Note: The Service described herein, including the individual service components listed in Section 2.2, is only applicable to Customer as identified on the Service Order; the Service does not apply to any of Customer's subsidiaries or other affiliated companies, individual business units, or any other similar Customer entity. Customer can add subsidiary, other affiliated companies, business unit names, and similar Customer entities as keywords.

1.1 Overview

For five (5) consecutive Business Days (the "**Engagement Period**"), researchers on the Secureworks® Surveillance Team ("**Surveillance Team**") – who are members of the Secureworks Counter Threat Unit™ ("**CTU**") – will analyze publicly accessible resources on the Internet, conducting an Open Source Intelligence ("**OSINT**") investigation to provide Customer with a report on the risk profile of Customer's organization based on a set of high-value keywords provided by Customer. The investigation will include surface web, dark web, and deep web locations. The information collected will be representative of what an attacker could compile about Customer's organization, to either capitalize on the information for malicious purposes or serve as a basis for a future targeted attack against Customer's organization. Customer can use this information to prevent and detect threats and threat actor activity.

The Service includes the following components:

- Enterprise Brand Surveillance ("**EBS**") Briefing Findings Report
- Raw Data
- Report Debrief Meeting (teleconference)

See Section 2, Service Details, for more information about the Service, including further explanation of the components listed above.

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 ("**SLAs**") 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 the Service and/or SLAs.

1.2.1 Keyword Identification

Customer will provide Secureworks with a list of high-value keywords prior to the first day of the Engagement Period. The keywords will be used as the scope of focus for all research and analysis conducted during the Engagement Period. The number of keywords shall not exceed 20. Common keywords that are used include company brands, names of confidential internal projects, IP ranges/CIDR blocks, top level/mail domains, and names of key personnel employed by Customer.

1.2.2 Communications

Customer will communicate with Secureworks through telephone (with authentication) and email. Customer will submit all service requests through email to the Secureworks point of contact ("**POC**"). In all cases, it is Customer's responsibility to ensure that its authorized contact list is up

to date. Customer is responsible for timely responses to email communications sent from the Surveillance Team.

1.2.3 General

- Customer will ensure that Customer personnel are scheduled and available to assist as required for the Service.
- Customer will provide to Secureworks all required information (key personnel contact information, credentials, and related information), using the EBS Information Brief onboarding document, prior to work being started.
- Customer will promptly reply to all requests from Secureworks.
- Customer will provide all information necessary to implement the Service, including identifying up to 20 keywords to use for the Service.

2 Service Details

The subsections below contain details about the Service and how it will be implemented.

2.1 Service Implementation

Secureworks will contact Customer within five (5) to ten (10) Business Days after execution of the Service Order ("**SO**") to provide Customer with the EBS Information Brief onboarding document. Customer must complete and return the document, which requests Customer POC(s) and keywords (maximum of 20). The document also advises Customer of the next available start date for the five-day Engagement Period. Lead times for start dates are usually two (2) to four (4) weeks from the date Customer receives the EBS Information Brief onboarding document, and could be longer depending on workload.

Customer and Secureworks will designate respective POCs to facilitate communication and support ongoing activities related to delivery of the Service.

On the first day of the Engagement Period, the Surveillance Team will begin the investigation, using Customer-provided keywords to analyze publicly accessible resources on the Internet, as well as surface web, dark web, and deep web locations. The first business day after the five-day Engagement Period ends, the Surveillance Team will start compiling the EBS Briefing Findings report, and deliver it to Customer POC(s) by the conclusion of the third business day following the end of the Engagement Period. The Surveillance Team will schedule a Report Debrief meeting with Customer (see Section 2.2.3).

Notes:

- Secureworks will attempt to use as many Customer-provided keywords as possible for each collection source; however, some keywords cannot be used for some collection sources.
- This Service is provided on a best-effort basis and the collection sources used for this Service can change for reasons beyond the control of Secureworks and/or at the discretion of Secureworks. Secureworks will attempt to identify as many relevant threats and risks to Customer as possible; however, due to the dynamic nature of collection sources, data ingestion and processing, and overall volume of data to review, Secureworks cannot guarantee that every information disclosure relating to Customer will be identified and provided to Customer.

2.2 Service Components

The subsections below contain information about the components of the Service.

2.2.1 EBS Briefing Findings Report

Secureworks will provide Customer with a structured report of key findings during the investigation, and recommendations on methods to resolve any exposures identified during the investigation. The report will be emailed to Customer POC(s) within three Business Days following the conclusion of the five-day Engagement Period.

2.2.2 Raw Data

Secureworks will provide Customer the raw data collected during the Engagement Period. The raw data will be emailed to Customer POC(s) within three Business Days following the conclusion of the five-day Engagement Period.

2.2.3 Report Debrief Meeting

The Surveillance Team will schedule and facilitate a Report Debrief meeting with Customer POC(s) for a mutually agreed-upon date and time. Audio and visual teleconference will be used as the delivery method for the meeting. The meeting will be used to discuss findings and recommendations, and answer Customer questions.

2.3 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.3.1 Counter Threat Unit (CTU) – Surveillance Team

The Surveillance Team, a specialized team within the Secureworks CTU, delivers this Service. The team is dedicated to performing surveillance activities, and will conduct the activities described herein for the five-day Engagement Period, the EBS Briefing Findings report, and the Report Debrief meeting.

2.3.2 Business Days and Business Hours

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. Secureworks will answer Customer questions as soon as possible.

2.3.3 Service Location(s) and Languages

The Service will be delivered remotely from a Secureworks location(s). Voice and email support are provided in English only. Other components of the Service that are visible to Customer (such as reports and documentation) are provided in English only. Service options and availability may vary by country; contact Secureworks sales representative for details.

2.3.4 Customer and Secureworks Responsibilities

The responsibility assignment matrix below describes the participation required by both Customer and Secureworks in completing tasks or deliverables for a project or business process to facilitate successful service delivery. Secureworks uses standard RACI role criteria for managing Customer projects and deliverables. These roles are defined as follows:

- R – Responsible: Role(s) assigned to do the work.
- A – Accountable: Role(s) that make the final decision and has ultimate ownership.
- C – Consulted: Role(s) consulted as the subject matter expert ("**SME**") before a decision or action is taken.
- I – Informed: Role(s) updated with status of work being done, status of ongoing work, and results of work completed.

EBS Information Brief			
Activity	**Task**	**Customer**	**Secureworks**
Service Preparation	Provide contact information for authorized contacts regarding Customer's account	R, A	I
Service Implementation	Provide EBS Information Brief onboarding document to Customer	I	R, A
	Complete and return EBS Information Brief onboarding document (includes 20 keywords)	R, A	I
	Conduct investigation during Engagement Period	I	R, A
	Compile and deliver EBS Briefing Findings Report to Customer POC(s) through email	I	R, A
	Schedule and facilitate Report Debrief Meeting	C, I	R, A

2.4 Out of Scope

The information in Section 2 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 described in the subsection(s) below are examples of services and activities that are out of scope. Upon request, Secureworks may provide out-of-scope technical support on a time and materials basis pursuant to a separate SO or Statement of Work ("**SOW**").

Providing this Service, including all of the individual service components listed in Section **Error! Reference source not found.**, to any of Customer's subsidiaries or other affiliated companies, individual business units, or other similar Customer entity is out of scope. Customer can add subsidiary, other affiliated companies, business unit names, and similar Customer entities as keywords.

2.4.1 Enterprise Brand Surveillance – Information Brief

The Service is focused on use of the 20 Customer-provided keywords to conduct the investigation during the five-day Engagement Period only. The engagement does not include on-going monitoring of threats beyond the five-day Engagement Period.

2.4.2 Threat Remediation

The Service does not include efforts to remove any sensitive content, items that are a security concern, or other findings from the locations where they have been identified. When possible, the Surveillance Team will provide recommendations on steps Customer can take to have content removed.

3 Service Fees and Related Information

Service Fees are based on the scope and term of Service. See Customer's MSA or CRA (as applicable), and SO or SOW (as applicable) for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

3.1 Invoice Commencement

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

4 Recommended Add-on Services

The Secureworks offerings listed below are optional and are sold independent of this Service or bundled with this Service. In addition, output from the Service can be used in delivering these add-on services for an additional charge.

- **Managed Security Services**
  - **Enterprise Brand Surveillance** (***Annual Subscription***)**:** Secureworks will provide Customer with monthly monitoring reports, monthly update meetings, monitoring and alerting, and direct access to the Surveillance Team through the Secureworks Client Portal.
  - **Global Threat Intelligence ("TI"):** Secureworks will make available to Customer through the Secureworks Client Portal a collection of threat intelligence (i.e., reports, data feeds, and related content and information about any technique or software used to exploit vulnerabilities) that will help Customer to understand the threat landscape, protect against cyber threats and vulnerabilities, and mitigate risk in its environment. The TI provides Customer with analysis of emerging threats and vulnerabilities, and deliver early warnings and actionable global TI. A monthly TI webinar that Secureworks hosts will be available to Customer.
- **Professional Services**
  - **Incident Management Retainer ("IMR"):** Secureworks will provide Customer with emergency and/or proactive incident response services such as incident response readiness, planning, workshops, and related services; digital forensic analysis; and threat hunting.
  - **Threat Hunting:** Secureworks will use proprietary methodology, expertise, and intelligence related to advanced threat actors and their techniques, tactics, and procedures (TTP) to hunt for threats that are specific to Customer; can include reviewing evidence that may persist in endpoints and other relevant Customer data to identify indicators of compromise, and deeper forensic analysis. Secureworks will assist Customer with remediation and eviction guidance for identified threats.

5 Additional Considerations and Information

The Service is intended to be conducted using keywords that are associated with Customer's organization or as requested. All keywords that Secureworks receives are assumed to be solely associated to Customer's organization. Customer shall defend, indemnify, and hold Secureworks harmless from any and all claims, actions, or allegations, including tortious interference claims, that may result from the investigation or use of keywords related to a third party for whom Customer requests information.

6 Service Level Agreements ("SLAs")

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

SLA	Definition	Credit
Information Brief Findings Report	A formal report of the aggregated findings from the Engagement Period shall be shared with authorized Customer POC(s) within three (3) Business Days following the conclusion of the Engagement Period.	1/30th of fee for Service for each day after the SLA is not met

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 SLA set forth above is subject to the following limitations:

- The SLA shall not apply if any act or omission by Customer prohibits or otherwise limits Secureworks from providing the Service or meeting the SLA, including but not limited to misconduct, negligence, provision of inaccurate or incomplete information, modifications to the Service.
- The SLA shall not apply to the extent Customer does not fulfill and comply with the obligations and responsibilities set forth within this SD.
- The SLA shall not apply if Customer-Side Technology is unreachable due to network connectivity issues, authentication issues, configuration issues, or public cloud downtimes that are outside the direct control of Secureworks.

For Customer to receive an SLA credit, subject to the limitations above, the notification of the SLA failure must be submitted to Secureworks within thirty (30) days of the date of such SLA failure. Secureworks will research the notification and respond to Customer within thirty (30) days from the date such notification is received. The total amount credited to Customer in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. The foregoing SLA credit(s) shall be Customer's sole and exclusive remedy for failure to meet or exceed the foregoing SLAs.

7 Glossary

Term	Description
Counter Threat Unit ("**CTU**")	Internal team of security experts that research and analyze threat data across Secureworks customers, and actively monitor the threat landscape. The team provides threat intelligence that extends visibility into cyber threats beyond the edges of the networks of Secureworks customers. The threat intelligence, applied to technology and the Secureworks suite of services, enables customers to expand visibility and reduce the time it takes to see and respond to threats, thereby resisting and avoiding cyberattacks.
Open Source Intelligence ("**OSINT**")	Understood in the intelligence community to mean any non-classified, unclassified, or publicly available information, as opposed to information that is acquired through covert or clandestine means for official purposes. In the context of the Service, OSINT describes an approach to intelligence analysis where non-proprietary sources of information are considered for the purposes of collecting and synthesizing data.
Service Level Agreement ("**SLA**")	A legally-binding arrangement to meet defined standards for the Service.