Secureworks®

SERVICE DESCRIPTION

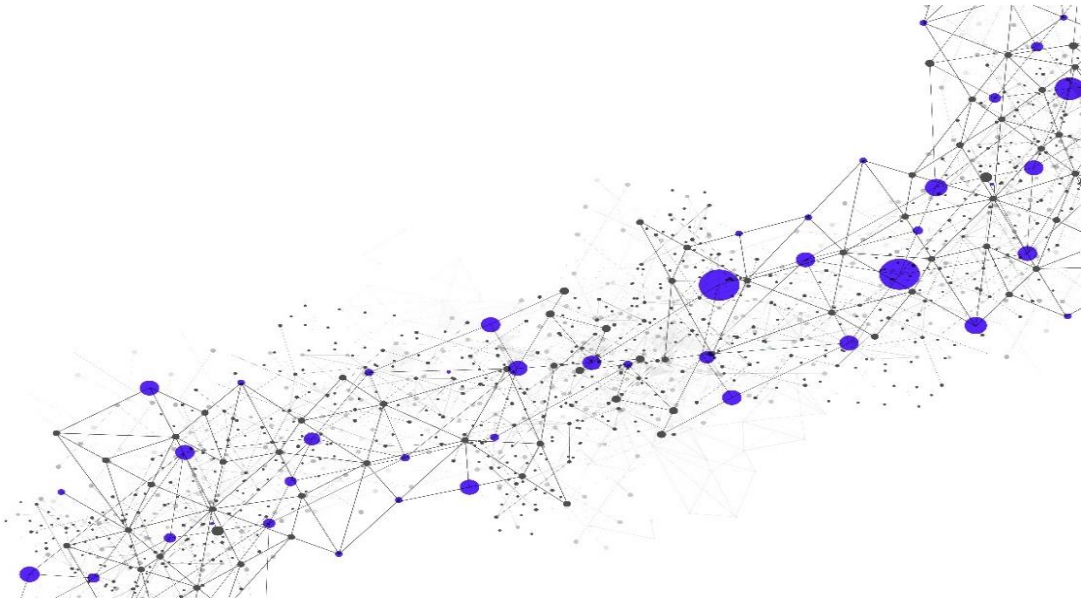
Enterprise Brand Surveillance

Release Date

October 01, 2021

Version

29.0



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 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 Transaction Document; 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

The Service consists of researchers on the Secureworks® Surveillance Team – who are members of the Secureworks Counter Threat Unit™ ("**CTU**") – conducting research and analysis to report and alert on security threats that are specific to Customer monthly as described in this SD. The Surveillance Team will analyze publicly accessible resources on the Internet and use Open Source Intelligence ("**OSINT**") collection capabilities and other research capabilities. Research and analysis 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 Threat Profile
- Monthly Monitoring Reports
- Monthly Update Meetings
- Monitoring and Alerting
- Access to the Secureworks Surveillance Team ("**Surveillance Team**") part of the Secureworks CTU™ research team)

The table below describes response times and deliverables as applicable to the Service.

Item	Description
Response Times	Secureworks will respond to all Customer inquiries within one (1) business day and within seventy-two (72) hours for requests made during weekends and holidays.
Alerts	The Surveillance Team will deliver alerts to Customer-designated POC(s) through email during normal Business Hours, according to the escalation procedures that Customer specifies.
Reporting	Reports will be delivered through encrypted email. ***Note:*** If Customer already has access to the Secureworks Client Portal ("**Portal**") as part of a separate Secureworks service, then reports can be delivered through the Portal.

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 managed components of the Service and/or SLAs, or a transition to monitor-only components of the Service.

1.2.1 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 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 250 keywords to use for the Service.

1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Transaction Document to schedule the first meeting during which Service Implementation will be discussed.

Customer and Secureworks will designate respective points of contact ("**POC**") to facilitate communication and support ongoing activities related to implementation of the Service.

2 Service Details

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

2.1 Service Implementation

The standard service implementation period begins after Secureworks reviews and approves Customer's signed Transaction Document, and ends when Customer receives the Enterprise Threat Profile report. The subsections below explain the implementation methodology and related activities.

2.1.1 Implementation Methodology

Secureworks will follow the Secureworks standard implementation methodology to implement the Service. The implementation methodology can be reasonably adjusted to meet Customer needs at the sole discretion of Secureworks. Below is a high-level overview of the Managed Security Services implementation methodology.

- **Organize:** Start the project, document success criteria, and finalize technical design of the Service
  - Secureworks will work jointly with Customer to validate accuracy of the information used to create the original Transaction Document against the actual Customer needs ("**Due Diligence**"). As a result of Due Diligence, changes may be identified ("**Identified Changes**"). Customer acknowledges that (i) in order for Secureworks to provide intended Service coverage across such Identified Changes, an amended or additional Transaction Document may be required, which may include changes to scope and fees, and (ii) without such an amended or additional Transaction Document, Secureworks may only be able to provide services as scoped, defined, and charged per the original Transaction Document. In some cases, an amended or additional Transaction Document may be required to provide the services in the original Transaction Document.

- Customer will designate authorized contacts for reports, meetings, and other activities related to the Service

- **Prepare:** Baseline the project schedule, and obtain all information from Customer that is necessary for the Service
  - Customer will provide information specific to Customer's organization (using the EBS onboarding document that Secureworks will provide to Customer) that will facilitate implementation of the Service, including up to 250 keywords that Secureworks will use to create queries. Customer can submit the following information for use as keywords within identified limits:
    - Domains – Up to five (5) critical domains for permutation monitoring and/or 100 total domains for keyword monitoring
    - General Keywords – Up to 50 total key brands, products, trademarks, subsidiaries, accounts, and data classifiers for keyword monitoring
    - Employees – Up to five (5) key executives for monitoring and profiling in the Enterprise Threat Profile (see further below), along with up to 10 additional executives/employees for keyword monitoring
    - Network ranges and ASN numbers – Up to five (5) key networks for monitoring
    - Other – Any other keywords, terms, or context the EBS team should be aware of in addition to the keywords listed above and up to a total of 250

    Note: Keywords related to third parties, including but not limited to vendors and suppliers, are not within the scope of the EBS service.

- **Execute:** Perform all activities necessary to ensure proper delivery of Service (e.g., testing the search queries)
  - 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.
- **Rationalize:** Confirm Customer's ability to participate in management of the Service; ensure alert quality and tuning of the queries for the Service
- **Accept:** Confirm recipients for alerts and EBS reports, and confirm plans for Monthly Update Meetings

2.1.2 Service Activities

Secureworks performs the following activities:

- Schedule initial meeting (remote) with Customer and review Transaction Document (or on-site meeting for Customers in Japan, if needed) *(**Note:** Receipt of a Customer-executed Transaction Document is required prior to scheduling initial meeting.)*
- Collect Customer information that is necessary for implementation
- Benchmark the delivery timelines for EBS reports according to the date Secureworks receives necessary information (per the Prepare phase in Section 2.1.1) from Customer
- Complete other implementation tasks listed in Section 2.4

2.2 Service Components

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

2.2.1 Enterprise Threat Profile

Within six (6) months of Customer returning to Secureworks the information described in Section 2.1.1, Secureworks will send to Customer the Enterprise Threat Profile ("**ETP**"). The ETP contains a point-in-time snapshot of the information available about Customer across open sources on the Internet. The ETP will contain an executive summary with key findings and

recommendations, and detail about threat scenarios and information collected that is based on discovered exposure points. Suggested analysis and mitigations focus on identifying areas where security controls will limit the impact of publicly available information and highlighting Customer's most significant risks.

2.2.2 Monthly Monitoring Report

Customer will receive a Monthly Monitoring Report, which summarizes alerts sent during the previous 30 days, along with any threat/risk trends identified through the course of alerting. The Monthly Monitoring Reports will commence one (1) month after Customer returns the information described in Section 2.1.1. The Monthly Monitoring Report provides Customer with metrics on incidence of alerts observed by the Surveillance Team in relation to Customer's organization. The Monthly Monitoring Reports are delivered to Customer through email and are discussed during the Monthly Update Meeting (hereinafter defined), which will also cover topics related to ongoing monitoring efforts.

2.2.3 Monthly Update Meeting

The Monthly Update Meeting is designed to ensure the Service is iterative, and that the delivery team's focus evolves in response to Customer's dynamic EBS needs. The purpose of this meeting is to review the Monthly Monitoring Report, discuss proximate research and service delivery goals, and discuss keywords and Priority Intelligence Requirements ("**PIR**"). This meeting will also ensure that baseline assessments established for Customer during ETP collection are refined through more recent research findings. Assigned Secureworks researchers and Customer personnel, as designated by Customer, will participate in the Monthly Update Meeting. This meeting will typically occur within five (5) Business Days following distribution of the Monthly Monitoring Report, on a mutually agreed-upon day and time, which can be modified as needed.

2.2.4 Monitoring and Alerting

Ongoing monitoring and alerting will be provided as part of the Service. If activity is detected that poses potential risk to Customer, then Customer's authorized contacts will receive an alert in accordance with the criteria defined during implementation. When relevant intelligence is collected and alerted upon, as much context as possible will be provided to Customer in an ongoing manner to ensure Customer remains informed about the situation and enable Customer to make informed decisions based on the real risk to Customer. The Surveillance Team will also provide monitoring and alerting of registered and dropped domains related to potentially fraudulent website creation (i.e., typosquatting) that targets Customer. Alerts will be sent to Customer's authorized contacts through email during Secureworks normal Business Hours (see Section 2.3.2 for Business Hours).

Customer is entitled to a maximum of 20 domain takedown requests for each year of Service purchased. If more than 20 are needed, then Customer must purchase an Incident Management Retainer ("**IMR**"). Any unused domain takedown requests at the end of the Services Term will be forfeited. Secureworks cannot guarantee a domain takedown request will lead to an actual removal of content; each domain takedown request from Customer will count towards the 20-per-year total regardless of whether the domain takedown is successful. Secureworks will provide Customer with domain takedown assistance for websites, domains, and IP addresses used for phishing campaigns and other malicious purposes that have a direct impact on Customer's cybersecurity posture, not to exceed one (1) threat indicator per domain takedown request and not to exceed 14 calendar days of Secureworks' best efforts per domain takedown request. Secureworks will pursue domain takedown assistance on Customer's behalf from the appropriate internet service providers, hosting providers, and domain registrars. Digital Millennium Copyright Act ("**DMCA**") and brand infringement takedown requests are out of scope.

Note: Monitoring and alerting 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 escalated to Customer.

2.2.5 Access to the Surveillance Team

During Secureworks Business Hours, Customer will have direct access to the Surveillance Team for guidance and recommendations as questions or situations arise.

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 delivers the Service, and this specialized team is part of the Secureworks CTU research team. The Surveillance Team is dedicated to performing surveillance activities, and they will conduct the activities described herein.

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.

The Secureworks SOC is available 24 hours a day, 7 days a week, for questions and support. During non-Business Days and Hours, some SOC inquires may be sent to other support groups to address during Business Days and Hours.

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) are provided in English only. Additionally, Secureworks requires that inputs and interfaces to the Service, including but not limited to logs, Application Programming Interfaces ("**APIs**"), and Command Line Interfaces ("**CLIs**"), be provided in English. Service options and availability may vary by country; contact Secureworks sales representative for details.

2.4 Customer and Secureworks Responsibilities

The following responsibility assignment matrix 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 the 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. For any individual task, there could be multiple roles responsible.
- 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.

Enterprise Brand Surveillance Service			
Activity	**Task**	**Customer**	**Secureworks**

Enterprise Brand Surveillance Service			
Activity	**Task**	**Customer**	**Secureworks**
Service Preparation	Provide contact information for authorized contacts regarding Customer's account	R, A	I
	Provide up to 250 keywords to be monitored *(**Note:** See Section 2.1.1, Implementation Methodology, for details.)*	R, A	C, I
	Complete and return the required forms and requested information (including the EBS onboarding document)	R, A	I
	Provide email address for one or more users who will receive reports and updates that are emailed to Customer	R, A	I
Service Implementation	Configure EBS for keyword monitoring	I	R, A
	Provide implementation guidelines for service implementation	I	R, A
	Configure implementation rules	I	R, A
General	Ensure Secureworks has current contact information for authorized Customer contacts	R, A	I
	Submit change requests for keywords to the Secureworks Surveillance Team through email to direct Surveillance Team POC and/or the team's email address	R, A	I
	Conduct daily monitoring activities to include review, triage, and forwarding of Customer-related validated alerts for next steps	I	R, A
	Collect, analyze, and produce Enterprise Threat Profile report, and deliver report to Customer (Customer completes and returns EBS onboarding document to Secureworks, and then the 10-week data collection period begins)	I	R, A

2.5 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. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document.

Providing this Service, including all of the individual service components listed in Section 2.2, 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.

3 Service Fees and Related Information

Service Fees are based on a fixed fee that is billed to Customer monthly. Customers purchase an annual subscription for the Service. See Customer's Transaction Document for details, including the following:

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

3.1 Invoice Commencement

See the Service-specific Addendum or Transaction Document 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**
  - **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.
    - **TI Support:** Customers with Advanced or Enterprise tier Service will have direct access to the CTU research team for escalation support. These customers can escalate TI questions or issues directly to the CTU research team through the Portal. This request-driven, transactional support enables these customers to leverage the expertise and threat visibility of the team for:
      - Questions, issues, and clarification on TI information received through the Advanced or Enterprise tiers and associated add-on services
      - Transactional requests for researchers to add enriched context to Customer-provided threat indicators, threat context, malware samples, or TI sourced from internal Customer operations or third-party sources
  - **CTU Countermeasures:** Secureworks will provide Customer with software for internal security purposes to act against threats.
- **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.

5 Service Level Agreements ("SLAs")

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

SLA	Definition	Credit
Enterprise Threat Profile	Within six (6) months after Customer returns to Secureworks the information described in Section 2.1.1, Secureworks will send to Customer the ETP report.	1/30th of the monthly Service fee for each business day that the SLA is not met
Monthly Monitoring Report	Customer will receive a Monthly Monitoring Report, which summarizes alerts sent during the previous 30 days. The Monthly Monitoring Reports will commence one (1) month after Customer returns the information described in Section 2.1.1.	1/30th of the monthly Service fee for each business day that the SLA is not met
Monitoring and Alerting	If an activity that poses potential risk to Customer is detected, then Customer's authorized contacts will receive an alert. Alerts will be sent through email within one (1) business day during Business Hours, and within seventy-two (72) hours during weekends and holidays.	1/30th of the monthly Service fee for each business day that the SLA is not met
Access to Surveillance Team	Customers will have direct access to the delivery team for guidance and recommendations as questions or situations arise. Secureworks will respond to all Customer inquiries with one (1) business day, and within seventy-two (72) hours during US weekends and holidays.	1/30th of the monthly Service fee for each business day that 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 SLAs 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 SLAs shall not apply during scheduled maintenance outages, and no SLA credit shall apply during a maintenance outage.
- The SLAs shall not apply if any act or omission by Customer prohibits or otherwise limits Secureworks from providing the Service or meeting the SLAs, including but not limited to misconduct, negligence, provision of inaccurate or incomplete information, modifications to the Service.
- The SLAs shall not apply to the extent Customer does not fulfill and comply with the obligations and responsibilities set forth within this SD.
- The SLAs 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.

6 Glossary

Term	Description
Counter Threat Unit ("**CTU**")	Internal team of security research experts that analyze threat data across Secureworks global Customer base and actively monitors the threat landscape. Provides threat intelligence that extends visibility into cyber threats beyond the edges of the networks of our Customers. The threat intelligence, applied to technology and our suite of services, enables Customers to expand visibility and reduce the time it takes to see and respond to them, 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.
Priority Intelligence Requirement ("**PIR**")	Directs the focus, nature, content, and format of technical, tactical, and strategic intelligence. In the context of the Service, the Surveillance Team, in conjunction with Customer, will create and enumerate PIRs, providing direction for information collection and objectives for intelligence outputs.
Service Level Agreement ("**SLA**")	A legally-binding arrangement to meet defined standards for the Service.