Secureworks®

SERVICE DESCRIPTION

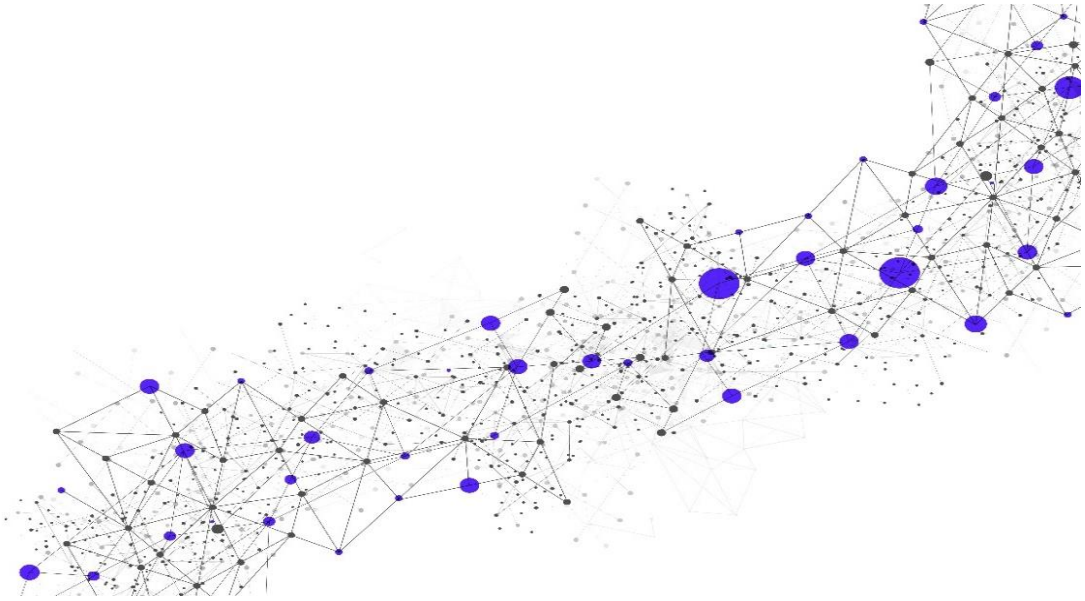
# Global Threat Intelligence

Release Date

**December 14, 2022**

Version

**31.1**




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 Global Threat Intelligence 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.

## 1.1 Overview

Secureworks® will make available to Customer through the Secureworks Client Portal ("**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 threat intelligence ("**TI**") provides Customer with analysis of emerging threats, and deliver early warnings and actionable global TI. A monthly TI webinar that Secureworks hosts will be available to Customer. The Service is provided through four tiers, as indicated in Section 2.2.9. If Customer purchases the Advanced or Enterprise tier, then Customer will have access to TI Support. The Service is provided in English only.

The Service includes the following components:

- Threat Analysis Reports
- Advisory Reports
- Monthly TI Webinar
- Weekly TI Summary *
- Emerging Threat Bulletins: Counter Threat Unit® ("**CTU**") TIPS *
- Bi-Weekly Cybersecurity News Roundup *
- Data Feed in XML Format *
- TI Support *
- Attacker Database ("**AttackerDB**") Data Feed *

* These components are only available for specific tiers as specified in Section 2.2.9.

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 Application Program Interface ("API") Integration

Some vendors provide APIs to interact with their systems. Any script or code creation for, usage of, maintenance of, or integration with other third-party tools are not included in this Service; Customer will be responsible for all API integration, and related activities and licenses. Secureworks will not install any third-party software applications that use the API directly on the appliance.

### 1.2.2 Communications

Customer will communicate with the Secureworks Security Operations Center ("**SOC**") through telephone (Customer-authorized representative will be authenticated). For this Service, SOC provides limited support such as resolving issues with a Customer's account in the Portal. It is Customer's responsibility to ensure that its list of authorized users is up to date with the Secureworks SOC. Additional support is available for an additional charge, as described in Section 2.2.8.1.

### 1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Service Order ("**SO**") 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

This section contains information about how the Service will be implemented.

### 2.1 Service Implementation

The standard service implementation period begins after Secureworks reviews and approves Customer's signed SO, and ends after the initial configuration and setup of Customer-designated authorized users for the Portal.

Customer will provide list of authorized users who will have access to the TI reports in the Portal. Secureworks will configure the authorized users in the Portal and their access to the TI reports.

Secureworks performs the following activities:

- Create implementation ticket in Portal (for ongoing tracked communication between Customer and Secureworks during implementation)
- Schedule initial meeting (remote) with Customer and review SO (or on-site meeting for Customers in Japan, if needed) *(**Note:** Receipt of a Customer-executed SO is required prior to scheduling initial meeting.)*
- Provide Customer with access to the Portal
- Collect Customer information that is necessary for implementation
- Provide any new Secureworks Customer with opportunity to participate in foundational training (see Section 2.5)

### 2.2 Service Components

The subsections below contain information about the components of the Service. The information and reports described in these subsections (excluding the webinar, the data feed in XML format, and TI Support) are made available to Customer-designated authorized users through the Portal, and through email.

***Note:*** With the Enterprise tier, customers can export a data feed in XML format, which contains the information and reports described in subsections 2.2.1 and 2.2.2. See Section 2.2.7 for information about the data feed.

#### 2.2.1 Threat Analysis Reports

Customer will be provided with decompositions of selected current malware and threats twice a month. The reports contain the following:

- Detailed technical analysis to illustrate popular hacker attack vectors and techniques
- Cross-referencing of threats to countermeasures and indicators of compromise where applicable

### 2.2.2 Advisory Reports

Customer will be provided with Advisory reports that contain strategic security information pertinent to the current threat landscape. Because threats are unpredictable, the Advisory reports are published as threats become known. The reports also contain the following:

- Secureworks-identified threats that target multiple customers
- High-profile threats (e.g., WannaCry and NotPetya)
- High-criticality threats (e.g., Internet Explorer zero-day vulnerability)

### 2.2.3 Monthly TI Webinar

The Research Team will host a TI webinar security briefing each month. They will discuss current security threats and advisories, and review current security concerns and hacker activities. This webinar is available to all TI customers.

### 2.2.4 Weekly TI Summary

Customer will be provided with a Weekly TI Summary report that contains threats and advisories across a 7-day period. The report is provided in .pdf format. This report also contains the daily CTU® Cyber Security Index ("**CSI**") across the entire week. The Weekly TI Summary is:

- Sent the first business day of the week
- Comprised of summary reports containing a review of emerging threat bulletins and alert summaries from monitored security devices when applicable

### 2.2.5 Emerging Threat Bulletins: CTU TIPS

Customer will be provided with real-time, emerging threat bulletins up to five (5) times per week. Bulletins include Research Team comments on emerging threats under investigation, curated security news relevant to customers, and updates on security concerns currently being investigated by the Research Team. Topics are often not verified and may not result in a security advisory or vulnerability posting. Since these bulletins are provided real-time, the information in the bulletins is not verified prior to publication (i.e., the information is researched after publication, and a determination is made whether to publish an Advisory or vulnerability).

### 2.2.6 Bi-Weekly Cybersecurity News Roundup

Customer will be provided with a report that highlights recent major issues and trends, as determined by the Research Team. The report is published every two weeks, and highlights stories from public news sources with a focus on issues impacting critical infrastructure sectors.

### 2.2.7 Data Feed in XML Format

Customers with the Enterprise tier will have access to a data feed in XML format in the Portal. The data feed contains CTU TI Data (threats and threat analysis, advisories, and other data provided to Customer as part of this Service), and Customer can export the CTU TI Data systematically into one or more of Customer's ticketing systems. Typically, a Customer using the data feed will configure its ticketing system(s) or threat intelligence platform(s) to extract the data every few hours.

### 2.2.8 Add-on Services

Based on the Service tier purchased (see table in Section 2.2.9), Customer can also purchase one or both add-on services described in the subsections below.

#### 2.2.8.1 TI Support

The TI Support Service provides Customer with a direct escalation path to the Research Team to complement our Advanced and Enterprise TI subscriptions. Customer can submit

TI-specific questions, issues, and telephone call-back requests directly to the Research Team as service request tickets in the Portal or call the SOC to initiate TI-specific tickets. A researcher will respond in the ticket in the Portal within one (1) business day of ticket creation. Requests not submitted in the Portal will be addressed on a best-effort basis and are outside the scope of the TI Support SLA.

TI Support is an **annual subscription** that is purchased in increments of five (5) hours per month for one year. For example, if Customer needs 20 hours of TI support per month, then Customer will purchase a quantity of four (4) for TI Support (5x4=20 hours of support per month for one year). Unused hours at the end of each month are forfeited and cannot be used in any future month. Customer can request a summary of hours used at any time by submitting a service request in the Portal. The Research Team will respond with the number of TI Support service requests and total hours of TI Support used for the requested time period. This request-driven, transactional support enables Customer 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 analysis, or TI sourced from internal Customer operations or third-party sources (***Note:*** Custom reports, recurring deliverables, and reoccurring deliverables are not in scope for TI Support.)

Upon commencement of the Service, the Research Team will conduct an initial onboarding session to explain TI Support to Customer, discuss best practices and use cases for TI support service requests, and answer Customer questions. Additional sessions can be conducted if or when a Service refresh is deemed appropriate, or when Customer experiences changes in personnel (new Customer POCs for the Service).

For malware analysis requests, Customer will provide sample file(s) for analysis via the Portal ticket in a password-protected .ZIP file along with related context / questions. A researcher will provide an initial assessment within one (1) business day of receipt of the ticket in response to the ticket. Customer may request additional analysis based on initial assessment within limits of the active TI Support Service. The Research Team will negotiate further delivery with Customer based on complexity of analysis.

For telephone call-back requests, Customer will include point of contact name, telephone number, and the nature of the research topic or issue in the TI Support service request, and a researcher will respond within one (1) business day to Customer contact provided.

Secureworks reserves the right to decline TI Support service requests that: (a) are beyond the scope of TI Support as defined in this SD; (b) are beyond the capability to deliver within contracted service levels; or (c) may violate legal or regulatory requirements. Requests for bespoke, recurring deliverables are beyond the scope of the TI Support service.

#### 2.2.8.2 Attacker Database Data Feed

AttackerDB contains lists of malicious internet protocol ("**IP**") addresses and domains identified by the Research Team. Secureworks correlates attacks (any malicious attempts to subvert, gain control, or otherwise cause damage to Customer's environment or equipment) across monitored security devices daily. These attacks are processed into an AttackerDB.

### 2.2.9 Summary of Tier-based Service Components

The table below explains the four tiers that are available for the Service, and the above-described components that are included in each tier.

| Service Components | Standard | Standard Plus | Advanced | Enterprise |
|---|---|---|---|---|
| **Number of Authorized Users** | 1 | 3 | 5 | 50 |
| Portal Access * | • | • | • | • |
| | • | • | • | • |
| Threat Analysis Reports | • | • | • | • |
| Advisory Reports | • | • | • | • |
| Monthly Security Intelligence Webinar | 48-Hour Availability | 48-Hour Availability | 30-Day Availability | 30-Day Availability |
| Weekly Security Intelligence Summary | | • | • | • |
| Emerging Threat Bulletins (CTU TIPS) | | • | • | • |
| Bi-Weekly Cybersecurity News Roundup | | | | • |
| Data Feed in XML Format | | | | • |
| **Add-on Services** | | | | |
| Threat Intelligence Support | | | • | • |
| AttackerDB Data Feed | • | • | • | • |

* ***Note:*** The Portal provides on-demand access to all threats and advisories, through searchable reports. Customer can map software applications to assets and assign a criticality to facilitate risk reporting and customize the TI data.

## 2.3 Service Delivery

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

### 2.3.1 Security Operations Centers (“SOCs”)

Secureworks maintains SOCs in the United States and internationally. For this Service, SOCs are available to Customer for Portal access issues only. Contact information for SOCs will be provided to Customer.

### 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, except in Japan where support is provided in both English and Japanese.

## 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.

| Threat Intelligence Service | | | |
|---|---|---|---|
| **Activity** | **Task** | **Customer** | **Secureworks** |
| **Service Preparation** | Provide contact information for authorized contacts regarding Customer's account | R, A | I |
| | Provide information for authorized users who need access to the Portal (Customer will modify as needed at any time through the Portal, and add / remove users as needed) | 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 initial Portal access for Customer's authorized users | C, I | R, A |
| | Provide training (remotely) to Customer for Portal | I | R, A |
| | Configure asset and application mapping | R, A | |
| **General** | Ensure Secureworks has current contact information for authorized Customer contacts | R, A | I |
| | Ensure threat intelligence asset and software profiles are kept current for accurate and effective use of Secureworks security services | R, A | |
| | Download CTU TI data feeds from Portal, or use the Create a URL feature (only for Customers with Enterprise tier and AttackerDB) | R, A | |
| | Integrate CTU TI data feeds with Customer's devices and systems (only for Customers with Enterprise tier and AttackerDB) | R, A | |

## 2.5 Training and Documentation

Each new Secureworks Customer can participate in foundational training (primarily webinar-based). The training is scheduled during the service implementation process, and is delivered through live, interactive training sessions. Foundational training includes the following topics, as applicable to the Service:

- Portal Training
- Portal User Roles and Audit

Secureworks will provide Service-related documentation to Customer. Documentation is generally provided through the Portal.

## 2.6 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. For example, custom

reports and/or reoccurring deliverables are not in scope. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate SO or Statement of Work ("**SOW**").

# 3 Service Fees and Related Information

Service Fees are based on a fixed fee that is billed to Customer monthly. 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.

- **Enterprise Brand Surveillance:** Secureworks will leverage proprietary Open-Source Intelligence ("**OSINT**") collection capabilities, research methods, and Research Team analysis to report and alert on security threats that are specific to Customer. Customer will receive an Enterprise Threat Profile, monthly monitoring reports and updating meetings, monitoring and alerting, and direct access to the Secureworks Surveillance Team for guidance and recommendations as questions or threatening situations arise.
- **CTU Countermeasures:** Secureworks will provide Customer with software for internal security purposes to act against threats.

# 5 Service Level Agreements ("SLAs")

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

| SLA | Definition | Credit |
|---|---|---|
| Threat Analysis Reports | At least two (2) threat analyses will be provided each month. | 1/30th of the monthly Service fee for each business day that the SLA is not met |
| Monthly TI Webinar | One (1) TI webinar will be delivered each month. | 1/30th of the monthly Service fee for each business day that the SLA is not met |
| Weekly TI Summary | One (1) TI summary will be provided each week. | 1/30th of the monthly Service fee for each business day that the SLA is not met |
| Emerging Threat Bulletins | A minimum of five (5) bulletins will be provided each week. | 1/30th of the monthly Service fee for each business day |

<table>
<tr><th>SLA</th><th>Definition</th><th>Credit</th></tr>
<tr><td>(CTU TIPS)</td><td></td><td>that the SLA is not met</td></tr>
<tr><td>Bi-Weekly Cybersecurity News Roundup</td><td>Two (2) news roundup reports will be provided each month.</td><td>1/30th of the monthly Service fee for each business day that the SLA is not met</td></tr>
<tr><td>TI Support (all responses are provided in tickets in Portal except telephone call-back requests)</td><td><table>
<tr><td>TI malware analysis requests</td><td>Respond in Portal ticket with an initial assessment within one (1) business day of ticket creation</td></tr>
<tr><td>TI telephone call-back requests</td><td>Respond through telephone call-back within one (1) business day to Customer contact provided</td></tr>
<tr><td>TI summary of hours used requests</td><td>Respond in Portal ticket with the total number of TI Support service request tickets and total number of hours used for the requested time period</td></tr>
<tr><td>Other TI requests</td><td>Respond in Portal ticket within one (1) business day of ticket creation</td></tr>
</table></td><td>1/30th of the monthly Service fee for each business day that the SLA is not met</td></tr>
<tr><td>AttackerDB Data<br>Feed</td><td>The AttackerDB data feed will be accessible on a daily basis through the Portal in CSV, XML, STIX, and PAN formats.</td><td>1/30th of the monthly Service fee for each business day that the SLA is not met</td></tr>
</table>

**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, or 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.

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 | Definition |
|---|---|
| Advisory | Announcements that inform customers about current threats that the Secureworks Counter Threat Unit research team deems critical. |
| Attacker Database (“**AttackerDB**”) | A database of known malicious attackers determined by analyzing Secureworks security device data. |
| Counter Threat Unit (“**CTU**”) | Internal team of security experts that research and 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. |
| Customer Device(s) | One or more devices that are owned by Customer and were not purchased from Secureworks. |
| Cyber Security Index (“**CSI**”) | The threat-based, color-coded indicator used in the Weekly TI Summary, based on emerging threats, active and developing exploits, and observed threat activity. |
| Service Level Agreement (“**SLA**”) | A legally-binding arrangement to meet defined standards for the Service. |