Secureworks®

WHITE PAPER

Which Secureworks Threat Intelligence Service is Right for Me?

Enhance your visibility across the threat landscape

Threat Intelligence Overview

For security leaders and professionals, threat intelligence is the information that extends your visibility into cyber threats beyond the physical edge of your network. Threat intelligence means combining data with expert analysis to provide predictive information about the adversary. Using this knowledge, you can take action in confidence, sometimes even before a threat has reached your organization. Therefore, Threat Intelligence can be summarized as 'information that can be acted upon to change outcomes'.

In today's cyber threat landscape, intelligence can alert you to new and emerging global threats that may affect your operations, impact your financial performance, expose customer data, and damage your brand and reputation. Threat intelligence can also identify actors who may be targeting your organization or its executives, and provide the insights that prepare you to take the right action to reduce risk.

Creating actionable threat intelligence requires an understanding of your current threat model, your risk appetite, specialized expertise, knowledge and tools that go beyond simple alerts and content searches. Your organization's threat model will help define your organizations major threats and how to mitigate them. Are you the sort of organization that needs to protect themselves against advanced nation state actors or are you looking to defend against the majority of e-crime activity? Once you have determined your threat model, your risk appetite will guide the amount of investment you want to make in threat intelligence, and the sort of sources you want to come to. From here you can determine, where you have the right skills and tools to create threat intelligence based on your threat model and risk appetite? Experts must know where to look for information that may be tucked away in the dimmer areas of the Internet, including within hacker communities, to construct the "big picture" from a thousand disparate puzzle pieces of data.

So how do you determine the right threat intelligence provider? What are some questions you might want to ask a provider? You might want to talk about the sources threat intelligence data they consume that will have a big impact on what they'll be able to help you with and what they'll be able to tell you. What unique intelligence data does that provider possess and analyze in order to give you the intelligence that they're providing? Do they have stuff you won't be able to get elsewhere? And that's something you have to factor in when comparing a number of different vendors? The vertical and sector visibility and then perhaps geographical region visibility that those vendors provide, is that aligned with your business model or operations? Will that provider or even set of providers be able to assist you with the areas that you operate in? You can talk about the type of intelligence they provide and how that is delivered. And additionally, what other technical capabilities that provider might be able to give you?

Secureworks researchers and security consultants are highly versed in the practices and nuances of intelligence formulation. With diverse and extensive backgrounds encompassing private industry, military and intelligence experience combined with the understanding of how your business works, our security experts deliver visibility into threats and the actors behind them, which you need to protect your organization and its leaders.

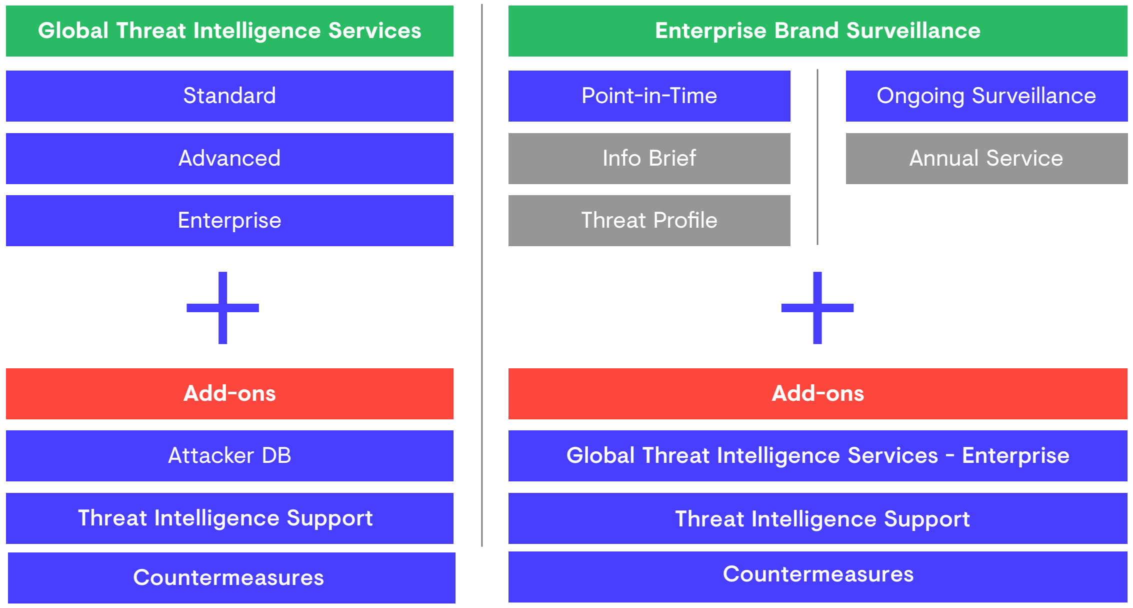
Secureworks Threat Intelligence Services Portfolio

Global Threat Intelligence

Global threat intelligence is generalized or non-targeted threat intelligence our expert security researchers develop based on data from threats collected and analyzed across our global client base of 4,100+ managed security clients. This intelligence provides a globalized view of emerging threats, evolving Tactics, Techniques and Procedures (TTP) of threat actors, known threat infrastructure and newly identified vulnerabilities, and provides clear actionable guidance for clients to enhance their security profiles.

Enterprise Brand Surveillance

Targeted threat intelligence is intelligence our security researchers and security consultants develop that is specific to the environments, organizations and executives of our clients. This intelligence is tailored to the requirements of the client to identify potential threats and threat actors that represent a direct and credible risk. The threat intelligence may be based on client brand and company affiliation information, IP/domain information, executive profiles and other attributes of interest to the client.



Global Threat Intelligence Services

Standard

Advanced

Enterprise

+

Add-ons

Attacker DB

Threat Intelligence Support

Countermeasures

Enterprise Brand Surveillance

Point-in-Time

Info Brief

Threat Profile

Ongoing Surveillance

Annual Service

+

Add-ons

Global Threat Intelligence Services - Enterprise

Threat Intelligence Support

Countermeasures

Global Threat Intelligence Service

Secureworks Global Threat Intelligence service delivers early warnings and actionable security intelligence, enabling you to quickly protect against emerging threats and vulnerabilities before they can impact your organization. Leveraging Secureworks' global threat visibility across thousands of client networks, along with our proprietary toolsets and unmatched research expertise, the service enables you to enhance the security capabilities of your team and reduce risk by addressing potential vulnerabilities more quickly and effectively.

Global Threat Intelligence Deliverables

Vulnerability Analysis

The Vulnerability analysis provides clients with detailed descriptions and recommendations to address current vulnerabilities. Secureworks Counter Threat Unit™ (CTU™) researchers gather and process vulnerability data from numerous public feeds, enriching the data with expert analysis and recommendations. Vulnerabilities are mapped to assets and applications in your environment, and you can easily query the vulnerability database and run reports across vulnerability data relevant to your organization.

Vulnerability analysis features:

- Comprehensive vulnerability analysis with expert recommendations
- Threat-level evaluation of each vulnerability
- Mapping of vulnerability data to specific assets and applications
- Delivery via the Client Portal, XML analysis and email

Threat Analysis

The Threat analysis provides clients with in-depth analyses of emerging threats, including detailed decompositions through malware analysis of Trojan horses, worms, rootkits and other forms of malware. Detailed threat reports investigate the core functions and operations of malware and are published to the Secureworks Client Portal, where they are mapped to the profile of your environment and cross-referenced with relevant vulnerability entries.

Threat analysis features:

- In-depth analyses of malware samples representing emerging threats
- Detailed decompositions that illustrate popular attack vectors and techniques
- Cross-referencing of threats with vulnerability data
- Delivery via the Secureworks Portal, XML analysis and email

Security Advisory

The Advisory analysis includes strategic security reports that focus on significant events and trends across the current threat landscape. Using security data collected from monitoring security activity across thousands of client networks, CTU researchers regularly publish Advisory Reports that include analysis of aggregate attack data and emerging trends.

Advisory analysis features:

- Detailed analysis of high impact, widespread threats
- Actionable recommendations for protecting assets
- Cross-referencing with applicable threat and vulnerability data
- Delivery via the Client Portal, XML analysis and email

> ***"Organizations can be faced with the challenge of acting on data that lacks proper analysis and curation, and if not fully vetted, may lead to poor conclusions based on faulty assumptions and waste resources on ineffectual outcomes.”***
>
> ***Barry Hensley,***
> ***Senior Vice President***
> ***Chief Threat Intel Officer***

Weekly Intelligence Summary

The Weekly Intelligence Summary provides a recap of worldwide cyber security issues from new activity and research performed during the previous week, and summarizes the last seven days of threats, vulnerabilities, advisories and CTU TIPS.

Weekly Intelligence Summary features:

- Quickly review CTU research activity from the previous week
- High-level report helps demonstrate value to management
- Links make it easy to drill into the recent activity

Emerging Threat Bulletins (CTU TIPS)

CTU researchers are constantly investigating new threats and cybercriminal activities. Emerging Threat Bulletins give you a window into the analysis of threats currently being investigated by our experts. Emerging Threat Bulletins are based on real-time security information and are designed to keep clients informed of security issues as they are being investigated.

Emerging Threat Bulletin features:

- Insight into current threats as they are investigated by our team
- Real-time information on active tools, tactics and procedures seen in the wild
- Expert commentary and opinion on emerging threats and security issues
- Minimum of five bulletins per week

Threat Intelligence Briefing

On a monthly basis, CTU researchers host a Threat Intelligence Briefing that encompasses the current threats, vulnerabilities and advisories. During this session, our researchers review aggregate attack data from across our client base and provide their analysis of the latest news and trends in information security.

Microsoft Update Analysis

Published within 24 hours of regular and out-of-cycle Microsoft patch releases, the Microsoft Update Analysis report provides a thorough examination of the patch content and the vulnerabilities addressed. The criticality of each vulnerability is reviewed by researchers with expertise in emerging threats and attack techniques. The report provides an assessment of the circumstances that must be present for successful exploitation and anticipated exploit activity is discussed. The CTU team uses this additional context to provide expert recommendations on which patches should be the highest priority for your organization.

Microsoft Update Analysis features:

- In-depth analysis of monthly or out-of-cycle Microsoft Updates within 24 hours
- Criticality assessments of each vulnerability addressed by the update
- Delivery via the Secureworks Portal, XML feed and email

CTU Cybersecurity News Roundup

Delivered twice per month, this report highlights the previous 2 weeks of major issues and trends in information security. The report contains stories from public news sources and media outlets, with a focus on security issues affecting major industries. These stories help inform executive leadership of the issues shaping the future of information security and underscore the importance of a strong information security program.

Additional Service Offerings

Threat Intelligence Support

CTU Support provides subscribers with direct access to CTU researchers for information regarding threats, vulnerabilities and advisories. When a request is submitted, a CTU researcher will respond within one business day. Direct access to this team enhances clients' internal security capabilities by providing expert guidance and consultation as needed.

Attacker Database

Secureworks' technology and security experts correlate and analyze attack data from tens of thousands of monitored security devices and critical information assets worldwide, processing more than 15 billion events every day. From this visibility, as well as numerous public and private sources, Secureworks' Attacker Database contains IP addresses and domain names of servers hosting exploits and malware, botnet Command and Control (C&C) servers and other known malicious activity. XML feeds are updated daily, giving valuable context to your security team.

Malware Analysis and Reverse Engineering

To determine the purpose and methods used by specific malware, clients may obtain Malware Analysis and reverse engineering services from our experts. Upon receiving a sample of the malware in question, a CTU researcher will analyze the malware using proprietary and public toolsets. Within one business day, they will provide a customized report detailing the composition of the malware and addressing additional client information needs.

Automatic event alerts are delivered when threat data is found related to your Threat Profile. These alerts contain your Threat Profile identifier, indicators and information about the identified threat. This allows you to manage the threat in a timely fashion or initiate additional support from the CTU at your discretion.

The service delivers:

- Indicators from collected malware and processed by a three-stage automation process designed to extract network and host indicators
- Indicators from our Advanced Persistent Threat (APT) research to include network and host indicators from known APT infrastructure and associated tradecraft
- Indicators from botnets monitored by the Secureworks CTU research team

Available Service Options

Global Threat Intelligence is available in the following service options.

Service Deliverables	Standard	Standard Plus	Advanced	Enterprise
Authorized Users	1	3	5	50
Secureworks Client Portal Access	✓	✓	✓	✓
SOC Analyst Support	✓	✓	✓	✓
Threat Analysis	✓	✓	✓	✓
Vulnerability Analysis	✓	✓	✓	✓
Security Advisory	✓	✓	✓	✓
Monthly Intelligence Webinar	48-Hour Availability	48-Hour Availability	30-Day Availability	30-Day Availability
Weekly Intelligence Summary		✓	✓	✓
Emerging Threat Bulletins (CTU TIPS)		✓	✓	✓
Microsoft Update Summary		✓	✓	✓
Microsoft Update Analysis				✓
Bi-Weekly Cybersecurity News Roundup				✓
XML Data Feed				✓
Available Add-on Services for Advanced and Enterprise Offerings				
Threat Intelligence Support			✓	✓
Attacker Database	✓	✓	✓	✓

Enterprise Brand Surveillance

Targeted cyber security threats represent the greatest challenge to information security and the financial well being of your enterprise. The stakes are high and involve the potential for intellectual property theft, financial loss, the compromise of customer information, public embarrassment and, ultimately, the health and longevity of your organization. Because a targeted threat actor will select their target and marshal the resources needed to launch a sustained campaign against your organization, security leaders and security analysts must have greater visibility than ever before to threats beyond the edges of their networks.

Secureworks Enterprise Brand Surveillance services give you the actionable security intelligence and expert security consultation needed to monitor for threats beyond the edges of your network. Identify and assess targeted cyber threats and the actors behind them, gain insight into ongoing exploits at a detailed level and take proactive steps to defend against them. Get access to elite threat intelligence research identifying new tools, tactics and procedures, and discuss your concerns directly with expert resources, when you need them.

The Enterprise Brand Surveillance service provides real-time monitoring of information outlets to identify threat actors targeting your organization, so you can quickly and effectively prepare countermeasures to protect networks, systems, executives, assets and your brand reputation. The Enterprise Brand Surveillance service delivers compelling, actionable intelligence on threats specific to your enterprise. Enterprise Brand Surveillance provides direct consultative support to keep your security team apprised of activities by actors that may pose a threat to your organization.

Enterprise Brand Surveillance services allow organizations to identify and assess advanced threats and the actors behind them, gain insight into ongoing exploits at a detailed level and take proactive steps to defend against them.

The service helps you:

- Get real-time visibility into threat actors targeting your organization or key personnel
- Preserve your organization's financial and reputational integrity
- Receive notifications about public data leaks that may compromise your security or introduce new risk

Point-in-Time Services

Info Briefs and Threat Profiles are standalone engagements that a client can leverage for a specific point in time. Both of these services provide a one-time report compiled of research that will help you understand what information an attacker could compile on your organization or key individuals. Determining how in-depth of a report your organization will need will drive which point-in-time engagement will best fit your needs. Info Briefs are a more concise report, while Threat Profiles are more comprehensive and require more research hours to complete.

Point-in-Time services help you:

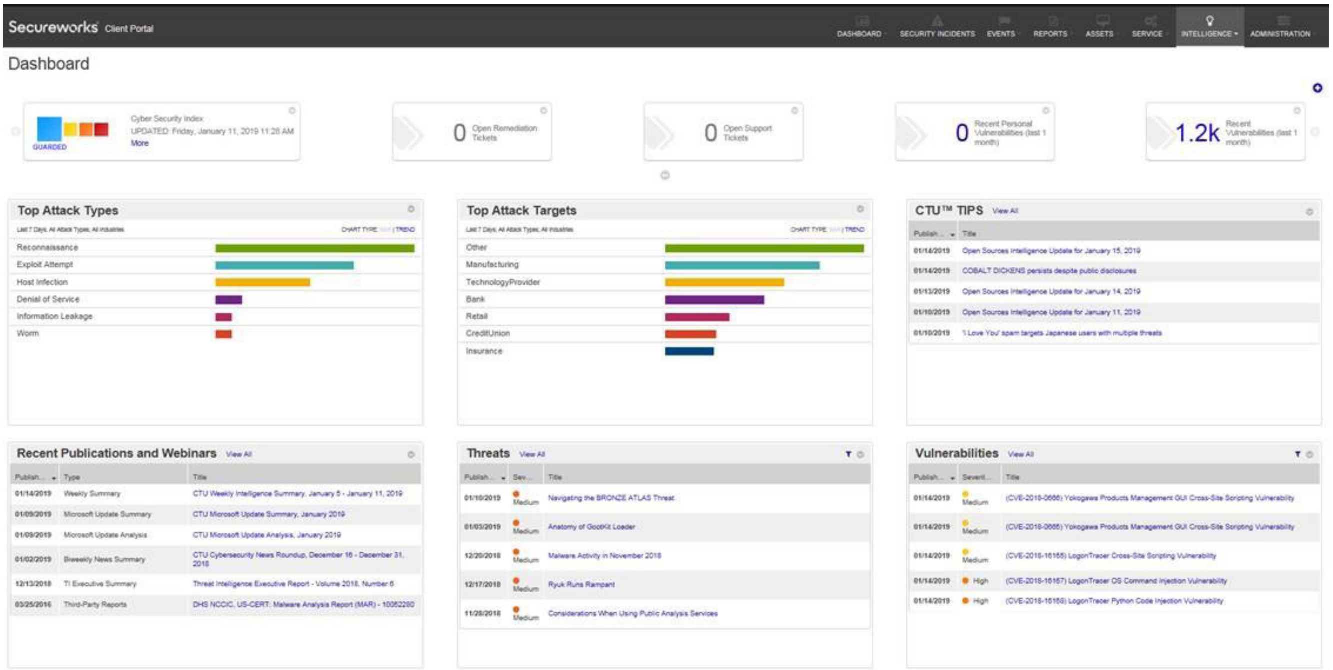
- Understand which attack scenarios are most likely to be launched against your company and why
- Assess the potential impact of publically available data to your security posture
- Better understand the threats posed by public information sources
- Minimize attack surface and restrict potentially damaging information from greater public disclosure

- Determine the effectiveness of customers' existing policies in limiting inadvertent disclosure by employees and former employees
- Run tabletop exercises simulating scenarios outlined in the Info Brief and determine the customers' level of preparedness

Client Portal

The Secureworks Client Portal is widely recognized as one of the premier security portals in the industry. Clients can create custom profiles so that intelligence information is tailored to their environment, providing actionable security intelligence that is relevant to different roles and technologies found in the enterprise. The Threat Intelligence Summary Dashboard, seen below, provides visibility into current threats, advisories and vulnerabilities relevant to your environment, as well as aggregate attack data detected across vertical markets.

Threat Intelligence Summary Dashboard



Cyber Security Index
UPDATED: Friday, January 11, 2019 11:28 AM

0 Open Remediation Tickets

0 Open Support Tickets

0 Recent Personal Vulnerabilities (last 1 month)

1.2k Recent Vulnerabilities (last 1 month)

CTU™ TIPS View All

Publish...	Title
01/14/2019	Open Sources Intelligence Update for January 15, 2019
01/14/2019	COBALT DICKENS persists despite public disclosures
01/13/2019	Open Sources Intelligence Update for January 14, 2019
01/10/2019	Open Sources Intelligence Update for January 11, 2019
01/10/2019	'I Love You' spam targets Japanese users with multiple threats

Recent Publications and Webinars View All

Publish...	Type	Title
01/14/2019	Weekly Summary	CTU Weekly Intelligence Summary, January 5 - January 11, 2019
01/09/2019	Microsoft Update Summary	CTU Microsoft Update Summary, January 2019
01/09/2019	Microsoft Update Analysis	CTU Microsoft Update Analysis, January 2019
01/02/2019	Biweekly News Summary	CTU Cybersecurity News Roundup, December 16 - December 31, 2018
12/13/2018	TI Executive Summary	Threat Intelligence Executive Report - Volume 2018, Number 6
03/25/2016	Third-Party Reports	DHS NCCIC, US-CERT: Malware Analysis Report (MAR) - 10052280

Threats View All

Publish...	Sev...	Title
01/10/2019	● Medium	Navigating the BRONZE ATLAS Threat
01/03/2019	● Medium	Anatomy of GootKit Loader
12/20/2018	● Medium	Malware Activity in November 2018
12/17/2018	● Medium	Ryuk Runs Rampant
11/28/2018	● Medium	Considerations When Using Public Analysis Services

Vulnerabilities View All

Publish...	Severit...	Title
01/14/2019	● Medium	(CVE-2018-0666) Yokogawa Products Management GUI Cross-Site Scripting Vulnerability
01/14/2019	● Medium	(CVE-2018-0666) Yokogawa Products Management GUI Cross-Site Scripting Vulnerability
01/14/2019	● Medium	(CVE-2018-16165) LogonTracer Cross-Site Scripting Vulnerability
01/14/2019	● High	(CVE-2018-16167) LogonTracer OS Command Injection Vulnerability
01/14/2019	● High	(CVE-2018-16166) LogonTracer Python Code Injection Vulnerability

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States

1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France

8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany

Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom

One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates

Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan

Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp