

Enterprise Brand Surveillance: The Power of Precise Threat Intelligence

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 seeks to collect relevant information wherever it can be found, analyzing and synthesizing it into meaningful knowledge upon which you can act, at times even before a threat has reached your organization.

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 help you identify actors who may be targeting your organization or its executives, providing the insights to help you prepare or take action.

Creating threat intelligence that is meaningful and actionable requires specialized expertise, knowledge and tools that go well beyond simple alerts and content searches. 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.

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.

Enterprise Brand Surveillance

Enterprise Brand Surveillance 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.

Client Benefits

- 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

Solution Features

- Understand which attack scenarios are most likely to be launched against your company and why
- Assess the potential impact of publicly available data to your security posture
- Minimize attack surface and restrict potentially damaging information from greater public disclosure
- Running Tabletop exercises simulating scenarios outlined in the info brief and determine a clients' level of preparedness

Enterprise Brand Surveillance

Gain insight with tailored intelligence

Secureworks' Enterprise Brand Surveillance service gives you the actionable security intelligence and expert security consultation needed to monitor for threats beyond the edges of your organization. Enterprise Brand Surveillance service is offered as an ongoing service subscription or point-in-time service based on your needs.

Focus

- **Annual Subscription:** Get real-time visibility into threat actors targeting your organization or key personnel
- **Point-in-Time Services:** Understand which attack scenarios are most likely to be launched against your company and why

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.

Identify Threat Actors Targeting Your Organization

The Enterprise Brand Surveillance service provides realtime 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.

This 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

“Boards, company management and CISOs cannot eliminate all cybersecurity risk, but by learning to ask the right questions and prompting a productive dialogue, board members can ensure security staff and employees at large are doing their part to minimize and mitigate risk to the greatest extent possible.”

Barry Hensley

Chief Threat Intelligence Officer, Secureworks

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 helps you:

- Understand which attack scenarios are most likely to be launched against your company and why
- Assess the potential impact of publicly 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 clients' existing policies in limiting inadvertent disclosure by employees and former employees
- Run tabletop exercises simulating scenarios outlined in the Info Brief and determine the clients' level of preparedness

About Secureworks

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.™

Annual Subscription

As part of the annual subscription for Enterprise Brand Surveillance, you will receive a year of alerting and monitoring service. We work with you to understand your needs and then craft queries that incorporate any keywords the you provide to us. We have a variety of tools that send us an automate notification on a ongoing basis. We review the alerts, determine if they are true/false positives, and then decide if there is additional research that needs to be done based on the information we received to further enrich the alert and report it to the you. As part of the Enterprise Brand Surveillance service, you will receive:

- Daily alerts
- Monthly report that contains a summary of alerts emails over the past 30 days
- Monthly call to walkthrough the report and go over the findings
- Enterprise Threat Profile reports:
A comprehensive report of the your digital footprint

Threat Assessment – Are there indicators of threat actors targeting you? Are there any indications that you may already been breached?

Risk Assessment – Looking for information that is currently available out there that if an attacker was able to get their hands on it, they can use it to target you.

Threat Scenarios – Based on our findings, we construct 2 or 3 scenarios that an attacker can use against you today.



For more information, call **1800 737 817** to speak to a Secureworks security specialist.

secureworks.com.au