Secureworks

SOLUTION BRIEF

Threat Intelligence Services

The Challenge

Threat actors who specifically target an organization or use commodity attacks are waging sustained campaigns that are purposeful, resourceful and sophisticated. As a result, traditional detection technologies and methods are proving insufficient to effectively combat this threat.

The Solution

At Secureworks, intelligence plays a vital role in addressing the risk posed by targeted and broad-based or "commodity" threats. Combining human and supervised machine learning intelligence gives The Secureworks Counter Threat Unit™ (CTU™) Research Team unparalleled insight into the threat landscape, across any technology and environment.

Threat actors are constantly developing new methods to penetrate your environment. Threat Intelligence can alert you to emerging global threats that may affect your organization's operations, impact its financial performance, expose customer data, and damage your organization's brand and reputation.

Services Backed by Elite Cyber Threat Intelligence

Threat intelligence supports all aspects of our services portfolio. With global threat visibility, intelligence formulated by the Secureworks CTU Research Team is applied to security device signatures and policies, attacker black lists and event correlation. Intelligence on threat actors and their tradecraft is actively shared across our security analysts, consultants and incident responders through an open feedback loop, providing further context for every engagement. As a result, clients receive sharper, more effective support across our entire services portfolio.

We Know the Threats You Face

Our CTU Research Team gathers billions of threat data points from diverse sources worldwide to formulate the intelligence backing the Secureworks services portfolio:

Elite Cyber Threat Intelligence Driven by World-Class Talent

Drawing from a diverse background in private security, military and intelligence communities, CTU researchers specialize in tracking, investigating and anticipating resourceful and sophisticated adversaries.

Our elite team regularly advises global government agencies, law enforcement, and the media on the latest trends in malware analysis, counterintelligence, forensics, and cybercrime.

"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

The CTU Research Team Mission and Capabilities

The CTU Research Team's mission is to protect our clients, embrace innovation and promote new service development. Our team achieves this mission by maintaining premier capabilities in the following:

- Countermeasure development and testing
- Advisories and support
- Knowledge sharing
- Liaison to law enforcement, military and intelligence communities
- Malware analysis
- Security innovation
- Specialized threat research
- Global Threat Intelligence
- Vulnerability analysis and management

Applied Intelligence

The CTU Research Team provides our analysts, security consultants and incident responders with deeper insight and enriched context into attacker Tactics, Techniques and Procedures (TTP).

Security Innovation and 'Big Data'

Our team collects and analyzes vast amounts of threat data as a result of our global visibility across thousands of client environments and other data sources. We refine this data into intelligence applied across our managed security operations, and actionable enterprise defense strategies.

Enhanced Service Options

Secureworks offers the following services for those security teams wishing to further enhance the intelligence function within their organizations:

Global Threat Intelligence

Our expert security researchers develop global Threat Intelligence based on threat data collected and analyzed across our client base of 4,400 managed security clients. This intelligence provides a globalized view of emerging threats, evolving Tactics, Techniques and Procedures of threat actors, known threat infrastructure and newly identified vulnerabilities, and provides clear actionable guidance for clients to enhance their security profiles.

Malware Analysis and Reverse Engineering

Secureworks has unmatched malware analysis and reverse engineering expertise, powered by the CTU Research Team. Using advanced tools and techniques, our world-class researchers thoroughly dissect malware to determine its functionality, purpose, composition and source.

Our experts will advise you of the malware code's potential impact to your networks, systems and information assets, and make recommendations for the malware's removal.

Enterprise Brand Surveillance

Enterprise Brand Surveillance is specific to the environments, organizations and executives of our clients. Secureworks researchers and security consultants are highly versed in the practices and nuances of intelligence formulation.

This intelligence is tailored to the requirements of the client to identify potential threats and adversaries that represent a direct, credible risk. The Threat Intelligence may be based on client brand and company affiliation information, IP or domain information, executive profiles and other attributes of interest to the client.

Threat Intelligence Support

Threat Intelligence Support provides you 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 your internal security capabilities by providing expert guidance and consultation as needed.

Attacker Database

Technology and security experts at Secureworks correlate and analyze attack data from tens of thousands of monitored security devices and critical information assets worldwide, processing billions of events every day.

From this visibility, as well as private sources, our 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.

Countermeasures

Secureworks leverages the intelligence provided by our global visibility and expert research, and converts it into countermeasures – creating a continuously improving technology that adapts with the changing security landscape.

When anomalous activity is detected, our CTU researchers perform thorough analysis to discover new attack techniques and threats. This process, which is unique to Secureworks, enables our CTU research team to identify real threats “in the wild” and develop countermeasures that protect our clients before damage is done.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com

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.™

Secureworks®