Threat Intelligence

Enriched by intelligence from our Counter Threat Unit™ (CTU™) research team, Dell SecureWorks Information Security Services help organizations predict threats, proactively fortify defenses, continuously detect and stop cyber-attacks, and recover faster from security breaches.

Dell SecureWorks protects thousands of organizations worldwide.

Threat actors are upping the ante in their methods to penetrate your environment. Actors who specifically target an organization are waging sustained campaigns that are purposeful, resourceful and sophisticated. As a result, traditional detection technologies and methods are proving insufficient to effectively combat the threat posed by targeted threat actors.

At Dell SecureWorks, intelligence plays a vital role in addressing the risk posed by targeted and broad-based or “commodity” threats.

The Dell SecureWorks Counter Threat Unit research team seeks to collect relevant information wherever it may be found; analyzing and synthesizing it into meaningful knowledge on which you can act, at times before a threat has even reached your organization. Intelligence can alert you to new and 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. Threat intelligence can also help you identify actors who may be targeting your organization, or its executives, and provide actionable guidance to effectively resist an attack.

Services backed by elite cyber threat intelligence

Threat intelligence supports all aspects of our services portfolio. With global threat visibility, intelligence formulated by the Dell SecureWorks Counter Threat Unit (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.

Threat intelligence backs all aspects of the Dell SecureWorks services portfolio. Our services enhance the intelligence capabilities for security organizations worldwide.
Threat Intelligence

We know the threats you face

The CTU gathers billions of threat data points from diverse sources worldwide to formulate the intelligence backing the Dell SecureWorks services portfolio:

Elite cyber threat intelligence driven by world-class talent

Consisting of some of the most highly regarded security researchers in the world with diverse experience and backgrounds in private security, military and intelligence communities, Counter Threat Unit researchers specialize in tracking, investigating and anticipating the most well-resourced and sophisticated threat actors, ranging from nation-state actors to top cybercrime organizations.

CTU researchers are among the most proficient in the industry, with exceptional talent for malware analysis, reverse engineering, counterintelligence, forensics and cybercrime investigation.

Their expertise is often specifically sought by government agencies, media outlets and enterprises.

CTU mission and capabilities

The CTU’s mission is to protect Dell SecureWorks’ clients, embrace innovation in security and promote new service development. The CTU 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
- Threat Intelligence
- Vulnerability Analysis and Management
Threat Intelligence

**Applied Intelligence**

The CTU applies intelligence across the Dell SecureWorks services portfolio to provide our analysts, security consultants and incident responders with deeper insight and enriched context into attacker Tactics, Techniques and Procedures (TTP).

This applied intelligence enables faster, more precise and effective service delivery for our clients.

---

**Security innovation and “Big Data”**

Dell SecureWorks is constantly innovating to introduce new capabilities that allow our security researchers to collect, analyze and apply vast amounts of threat data we see as a result of our global visibility across thousands of client environments and other data sources.

Central to this innovation is the Threat intelligence Management System (TIMS) platform which we use to centralize, query, analyze and correlate billions of threat indicators and event data.

Intelligence derived from TIMS is applied across our Managed Security operations and better informs our analysts, consultants, incident responders in their daily operations.

---

**Cyber Security Index**

The CTU Cyber Security Index (CSI) is a threat-based, color-coded system provided to notify clients about threats that might require protective measures.

The CSI is evaluated daily by CTU researchers and published online at Secureworks.com. Statuses are Guarded, Elevated, High and Critical.

**Status: Guarded**

---

**Enhanced service options**

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

**Global Threat Intelligence**

Global threat intelligence is generalized or non-targeted threat intelligence our expert security researchers develop based on data on threats collected and analyzed across our client base of 3,700-plus 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.

**Malware Analysis and Reverse Engineering**

Dell SecureWorks has unmatched malware analysis and reverse engineering expertise, powered by the Counter Threat Unit 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 offer an opinion on the malware code’s potential impact to your networks, systems and information assets, and suggest recommendations for the malware’s removal.

**Targeted Threat Intelligence**

Targeted Threat Intelligence is intelligence our security researchers and top security consultants develop that
Threat Intelligence

is specific to the environments, organizations and executives of our clients. Dell 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 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.

Available services include:

- Enterprise Brand Surveillance
- Executive Threat Surveillance
- Targeted Threat Surveillance

Visit www.secureworks.com to learn more about our information security services.

Email info@secureworks.com or phone 877-838-7947 to speak to a Dell SecureWorks Security Specialist.

About Dell SecureWorks

Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Dell SecureWorks’ Information Security Services help organizations proactively fortify defenses, continuously detect and stop cyber-attacks, and recover faster from security breaches.

Availability varies by country. ©2014 Dell Inc. All rights reserved. Dell and the Dell logo, SecureWorks, Counter Threat Unit (CTU), and iSensor are either registered trademarks or service marks, or other trademarks or service marks of Dell Inc. in the United States and in other countries. All other products and services mentioned. March 2014