Advanced Threat Services

The first and only comprehensive suite of services designed specifically to combat targeted attacks

Dell SecureWorks’ Advanced Threat Services elevate your defenses with key capabilities needed to effectively resist targeted threats. Addressing the entire attack cycle, the Targeted Threat Services portfolio is the first and only comprehensive suite of services available designed specifically to combat targeted attacks.

Fueled by Dell SecureWorks Counter Threat Unit (CTU) intelligence, Advanced Threat Services help you anticipate your attackers, detect their tradecraft, disrupt the kill chain and eradicate their presence in your environment.

Targeted Threat Services include:
- Targeted Threat Intelligence
- Red Team Testing
- Managed Advanced Malware Protection
- Enterprise iSensor
- Targeted Threat Hunting
- Targeted Threat Response

Benefits
- Understand your adversaries and how to counter them
- Proactively reduce your exposure to advanced threats and fortify your defenses
- Detect and mitigate attacks before major compromise
- Minimize the extent of data loss
- Access specialized targeted threat expertise and support
- Increase confidence in system integrity and data confidentiality
Successful defense against advanced threats requires integrated threat intelligence, security operations and incident response:

**Advanced Endpoint Threat Detection**

**Advanced visibility into endpoints**

Employing proprietary CTU Endpoint Intelligence technology, the Dell SecureWorks Advanced Endpoint Threat Detection service gives you the earliest possible warning that your endpoints may be hosting an advanced adversary.

The service heightens your security situational awareness by warning you when endpoints may have been compromised and accelerates remediation efforts by pinpointing exactly which systems are compromised, how they were compromised, and how you can repair them.

**Benefits**

- Improves situational awareness by detecting signs of endpoint compromise
- Accelerates response times by pinpointing affected systems quickly
- Reduces costs by allowing patching of systems versus reimaging
- Reduces exposure to targeted threats and fortifies defenses
- Minimizes the extent of data loss
- Increases confidence in system integrity and data confidentiality
Enterprise iSensor
IPS network intrusion protection from harmful traffic that evades your firewall

The Dell SecureWorks Enterprise iSensor IPS service helps you eliminate malicious inbound and outbound traffic around the clock, without the burden of device or signature management, and without increasing in-house headcount.

The service performs in-line deep packet inspection of inbound and outbound network traffic using multiple integrated defensive technologies to identify and block real security events that require attention. The subscription includes hardware, support, managed and monitored service, and thousands of unique countermeasures developed by our CTU research team.

Benefits
- Reduces management and monitoring costs
- Protects systems and data 24x7 without increasing in-house headcount
- Defends your network with real-time threat intelligence
- Guards against the new and emerging threats
- Filters out “noise” and manage real attacks that require attention
- Satisfies compliance regulations

Managed Advanced Malware Protection (MAMP) detects and blocks advanced malware delivered via email and web content, often used by Advanced Threat Actors.

Benefits
- Detects and prevents the deployment of advanced malware 24x7
- Disrupts attack process earlier in the “kill chain”
- Defends against spear phishing and “drive-by-download” attacks
- Integrates Advanced Malware Protection systems into holistic security management, monitoring and reporting
  Maximizes Advanced Malware Protection system performance, uptime and availability

Managed Security Awareness Programs
Managed program to build a culture of security awareness and change employee behavior

The Dell SecureWorks Managed Security Awareness Programs service helps leaders build a culture of security awareness by designing and fully managing a comprehensive Security Awareness Program for your organization.

Led by the same experts who protect Dell SecureWorks’ own employees and infrastructure, the service provides a comprehensive application of impactful content, testing, reward and remediation, combined with clear metrics and reporting to help leaders change employee behavior.
Benefits

- Increases employee vigilance while reducing risk to your organization
- Trains employees on hazards presented by phishing, social engineering and weak security behaviors
- Measures improvement in employee security awareness and vigilance
- Reduces employee clicks on malicious emails
- Reduces cyber security incidents caused by employee behavior

Red Team Testing

Targeted attack simulation using real-world tactics, techniques and procedures

Red Team Testing simulates a real-world attack against your organization using blended threat scenarios that test the effectiveness of your security defenses, policies and staff.

Benefits

- Improves organizational readiness
- Inspects current performance levels
- Improves training for defenders
- Evaluates the effectiveness of your defenses and controls
- Provides objective insights into vulnerabilities that may exist

Targeted Threat Hunting

Deep inspection of networks and endpoints for indications of attacker presence

The Dell SecureWorks Targeted Threat Hunting service searches your networks and endpoints to identify the presence of compromises and entrenched threat actors operating in your environment.

Powered by CTU Special Operations, the Targeted Threat Hunting service leverages elite cyber threat intelligence and decades of combined experience countering targeted adversary tradecraft. Our highly experienced security experts, armed with CTU proprietary hunting technology, perform a deep inspection of your environment to identify indicators of attacker presence.

Benefits

- Determines if your environment has been compromised by a sophisticated attacker
- Increases your confidence in system integrity and data confidentiality
- Gives you recommendations on security architecture, instrumentation and controls to make your environment more resilient
- Provides actionable guidance on next steps to respond to and eradicate the threat

Targeted Threat Intelligence

"Over-the-horizon" intelligence and context on threat actors and their tradecraft

Targeted Threat Intelligence services allow organizations to identify and assess targeted threats and the actors behind them, gain insight into ongoing exploits at a detailed level, and take proactive steps to defend against them.

Services include:

- The Targeted Threat Surveillance service proactively provides contextual,
researched, actionable host and network threat indicators specific to your organization to inform your protection and response processes.

- The **Enterprise Brand Surveillance** service provides real-time monitoring of information outlets and communications to identify threat actors targeting your organization, so you can quickly and effectively prepare countermeasures to protect your networks, systems, data and brand reputation.

- The **Executive Threat Surveillance** service monitors and assesses risk posed to your executives, specific personnel, and organization.

**Benefits**

- Provides advanced warning of plans by targeted actors to attack your organization
- Determines if your network and systems are connected to known and suspected threat infrastructure
- Expands your visibility into the threats that concern you most before they strike your network

**Targeted Threat Response**

*Containment and removal of attacker presence and advanced tradecraft with surgical precision*

The Targeted Threat Response service provides rapid containment and eradication of threats, minimizing the duration and impact of a security breach. Leveraging elite cyber threat intelligence and global visibility, the CTU Special Operations team helps you respond to and recover from even the most complex and large-scale security incidents involving targeted actor tradecraft.

**Benefits**

- Minimizes the duration and impact of a security breach
- Provides rapid engagement by Incident Response experts when a security breach is detected
- Provides for seamless engagement by CTU Special Operations team after a hunting engagement

---

**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. For more information, visit [http://www.secureworks.com](http://www.secureworks.com).

For more information, phone 877.838.7947 to speak to a Dell SecureWorks security specialist.

Availability varies by country. © 2014 Dell Inc. All rights reserved.

Dell and the Dell logo, SecureWorks, Counter Threat Unit (CTU) 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 are trademarks of their respective companies. This document is for illustration or marketing purposes only and is not intended to modify or supplement any Dell specifications or warranties relating to these products or services. April 2014