At-a-Glance

Benefits

- **Identify threats** occurring right now in your environment, including botnets and malware
- **Eliminate the exfiltration** of sensitive data
- **Seamlessly integrate** with your existing security infrastructure
- **Eliminate unnecessary investigations** by seeing only confirmed threats and no false-positive alerts

Cisco Cognitive Threat Analytics

Enhance Web Security with Breach Detection and Analytics to Stop Threats in the Network

Attackers are no longer motivated by notoriety but, more typically, economic or political gain. With significant financial incentives for successful attacks, cybercriminals today have become more sophisticated and clandestine. They are more proficient at discreetly exploiting gaps in security and using new techniques to conceal malicious activity. Researchers on our Cognitive Threat Analytics team have found that when attackers have established a foothold within an organization, more than 90 percent of them use the web for command-and-control communications and to exfiltrate sensitive information.

Cisco® Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before. A cloud-based service, Cognitive Threat Analytics analyses the information generated by your existing web security solutions without the need for any additional hardware or software. It's simple, powerful, and highly effective.

Turn Your Web Proxy into a Security Sensor with Cloud-Based Breach Detection and Analytics

Cognitive Threat Analytics automatically analyzes more than 10 billion web requests daily. It zeroes in on malicious activity that has bypassed security controls and is using web-based communications. This includes standard, encrypted, and anonymous channels that can be used to attack your organization.

Using machine learning and a statistical modeling of networks, Cognitive Threat Analytics creates a baseline of normal activity and identifies anomalous traffic occurring within your network. It analyzes device behavior and web traffic to pinpoint command-and-control communications and data exfiltration.

"[Cognitive Threat Analytics] allows our team to work on the projects that they need to be working on instead of trying to remediate threats."

Scott Engle
Director of IT, Transplace

Detection and Analytics Engines

Detection and analytics features provided in Cognitive Threat Analytics are shown in Table 1.

Table 1. Features of Cisco Cognitive Threat Analytics

Engine	What It Does
Data exfiltration	Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content.
Domain-generation algorithm (DGA)	Attackers generate an arbitrary number of domain names to avoid the detection and blacklisting of hosts that provide malware. Cognitive Threat Analytics recognizes malicious and obfuscated domain names generated from words, analyzes the frequency of communication, the information content of the headers, and hundreds of other features on each HTTP or HTTPS request.
Exploit kit	Analyzing web requests allows Cognitive Threat Analytics to uncover infections by exploit kits from (1) visits to an infected webpage, (2) redirects of web requests to a domain-hosting exploit kit, (3) unknowing downloads by users, (4) successful exploitations, and (5) downloads of malicious payloads.
Tunneling through HTTP and HTTPS requests	Attackers often try to exfiltrate sensitive data, including credentials, using HTTP and HTTPS requests themselves. Cognitive Threat Analytics uses multiple indications of compromise (IOCs), including global statistics and local anomaly scores, to reliably distinguish malicious tunneling from benign use of the technique.
Command-and-control (C2) communication	Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPS-encoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats.

Cisco Cognitive Threat Analytics serves up information through an intuitive web-based portal, so users can quickly:

- Assess the severity and scope of intrusions
- Understand the mission of the threat and how it works
- Take immediate action

Learning from what it sees, Cognitive Threat Analytics adapts to provide continuous breach identification, reducing the risk of repeat attacks or continued infection.

Next Steps

For more information on Cisco Cognitive Threat Analytics, visit www.cisco.com/go/cognitive to watch customer testimonials and download detailed data sheets.

C45-736555-00 01/16