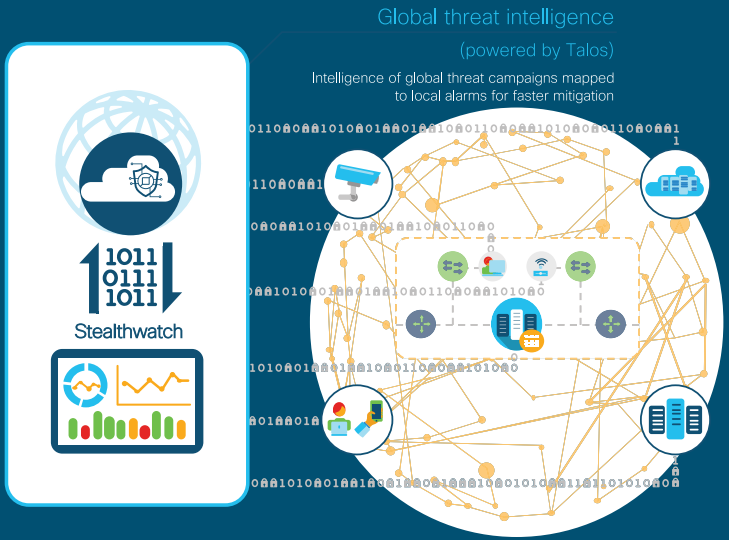
Cisco Stealthwatch Threat Intelligence License

One of the advantages that attackers have is that they can apply the same attack on multiple targets, and the odds are that they'll be successful across them all because these victims are all constrained to their local view of the threat activity. But what if you had information about malicious IPs and domains, or a new strain of malware used in a campaign, and could map the alerts to this global threat intelligence? You would greatly reduce the time to detection as well as increase the fidelity of detection.

Cisco Stealthwatch® Threat Intelligence (TI) License

Cisco Stealthwatch® Threat Intelligence (TI) License gives Stealthwatch customers access to a global threat intelligence feed powered by the Cisco Talos™ intelligence platform. It provides an additional layer of protection against botnets and other sophisticated attacks by monitoring connections from the local network environment to the internet using data on thousands of known command-and-control servers, unallocated or bogon IP address spaces, and Tor entry and exit nodes. This leads to high-fidelity detections and faster threat response.



What is Stealthwatch?

Cisco® Stealthwatch is the industry-leading security analytics solution that collects rich telemetry from existing network infrastructure to provide comprehensive threat visibility into the extended network, including data center, branch, endpoints, and cloud. Stealthwatch can detect and respond to advanced threats, and help simplify network segmentation using a combination of behavioral modeling, multilayered machine learning, and global threat intelligence. Because attackers aren't employing just one method to breach your network, Stealthwatch employs multiple analytical techniques to detect threats early and helps ensure that the eviction is complete. Stealthwatch is the first and only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analytics.

Benefits of the Cisco Stealthwatch Threat Intelligence (TI) feed:

- Real-time detection of attacks by immediately detecting malicious connections from the local environment to the internet
- High-fidelity alerts and rapid threat response with the knowledge of known bad hosts across the world
- Cost-effective solution requiring no management as threat info is pulled in automatically, frequently, and securely

Note: A TI License is required for each Stealthwatch Flow Collector.

Advanced botnet detection

The Stealthwatch TI feed offers advanced botnet detection capabilities, continuously monitoring customer networks for thousands of known command-and-control (C&C) servers, bogon IP address spaces, and Tor entry and exit nodes, and automatically adding new botnets to its radar as they are identified in the wild. From there, Stealthwatch generates alarms and Concern Index™ events to flag these communications for administrators so they can be swiftly mitigated.

Stealthwatch botnet detection functionality includes:

- Detection of either attempted or successful C&C communications
- Reporting on the specific botnet name responsible for the infection
- Detection of C&C servers operating within a network
- In-depth traffic reporting and analysis of the C&C communications
- Accelerated priority of other suspicious network activity from infected hosts
- Real-time information of malicious hosts across the world
- Correlation of user and device information for the infected hosts to add context
- Utilization of application metadata such as HTTP URLs from the Stealthwatch Flow Sensor to increase accuracy of detection
- Connections to bogon IP address spaces (A bogon is a bogus IP address from the bogon space, which is a set of IP addresses not yet officially assigned to any entity)
- Connections to Tor entry and exit Nodes

About Cisco Talos

Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers. These teams are supported by unrivaled telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence for Cisco customers, products and services. Cisco Talos sees upto 1.5 million unique malware samples and blocks as many as 20 billion threats per day.

Learn more

Next steps

To learn more, visit https://www.cisco.com/go/stealthwatch or contact your local Cisco account representative.

To see what threats might be lurking in your network, sign up for a free visibility assessment.

Sign Up

How it works

Today's threat landscape and growing network complexity has rendered conventional solutions such as antivirus, firewalls and IDS/IPS far less effective. In order to remain ahead in the cybercrime arms race, organizations must now obtain end-to-end situational awareness into everything happening across their networks. Stealthwatch provides a comprehensive picture of network activity for combating a robust range of security and performance issues – including unknown attacks and advanced persistent threats (APTs) – across both physical and virtual environments. Unlike many conventional security technologies, the system does not rely on signature updates to detect anomalous behaviors that could signify risks.

The Stealthwatch TI feed provides an added layer of protection against the spread of malware by incorporating in-depth intelligence on known bad hosts on the Internet into Stealthwatch, eliminating the need for costly point solutions. Using their existing Stealthwatch appliances, customers can choose to add the TI license to their deployment to automatically pull in updated threat information on an hourly basis. Customers do not have to worry about collecting their own threat intelligence and inputting it into Stealthwatch. Instead, the threat feed is continuously delivered via a compressed, encrypted communication channel for optimal security and efficiency. (Figure 1)

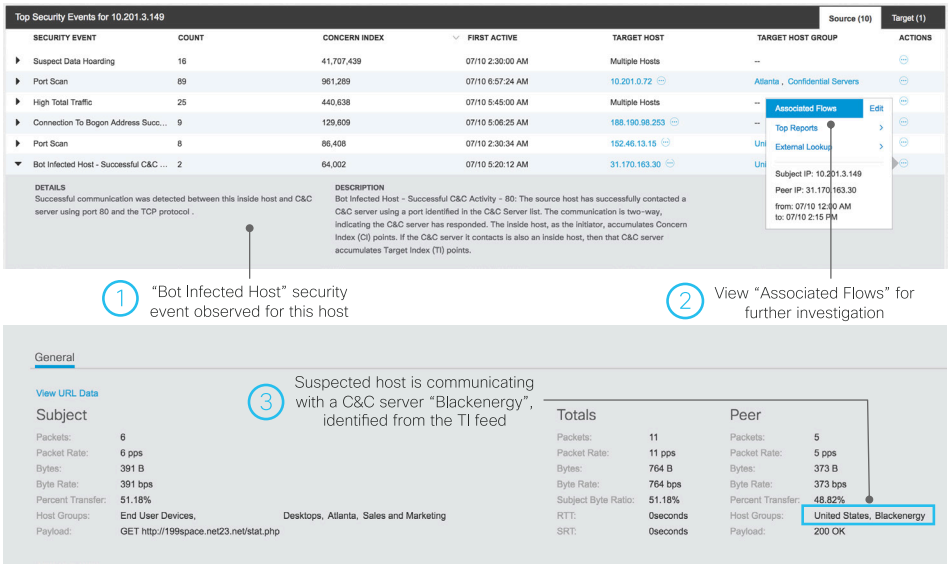


Figure 1: Command-and-Control (C&C) activity detection using the Stealthwatch Threat Intelligence (TI) feed