Cisco Encrypted Traffic Analytics
Security Performance Validation

March 2018

DR180222D

Miercom.com

www.miercom.com

Contents

1.0 Executive Summary 3
2.0 About the Product Tested 5
3.0 How We Did It 6
4.0 Encrypted Traffic Analytics Malware Detection 7
4.1 Progressive Detection of Malicious Flows 7
4.2 Time to Detect Encrypted Malware with and without ETA 8
4.3 Role of Flows in Detection of Encrypted Malware with and without ETA 9
4.4 Detection Efficacy 10
5.0 Crypto Analytics 14
5.1 Corporate Cryptographic Compliance 14
About Miercom 15
Customer Use and Evaluation 15
Use of This Report 15

1.0 Executive Summary

Enterprises seeking privacy and security rely on applications that use Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption for in-transit messaging where data is hidden and protected from unauthorized users. Communications, transactions and applications depend on encryption to shield its sensitive content from listening attackers.

It would seem this private communication method was foolproof for avoiding threats, but users have a false sense of protection. Encrypted traffic is now just another means of transporting malware, undetected in its encapsulated form. This can have catastrophic effects, and with each passing minute data is compromised. Average breach detection takes over six months and containment requires about two months – costing an organization upwards of $3 million.

Most enterprises examine encrypted traffic by decrypting it first, using techniques such as Man-in-the-Middle (MITM) proxy and security products like a firewall or intrusion prevention system. But this is time consuming and drains network performance and resources. Additionally, decrypted data is now vulnerable to attacks and complicates compliance due to its storage in unencrypted form.

To prove the capabilities of a solution that doesn't require decryption to discover threats in encrypted traffic, Cisco Systems engaged Miercom to perform an independent security efficacy and performance assessment of its Encrypted Traffic Analytics (ETA) solution for their line of new Catalyst 9000 switches, ISR/ASR/CSR routers in an enterprise network. Cisco ETA is a novel approach that uses metadata of encrypted traffic exported by the switches and routers in a NetFlow v9 record to identify behavioral anomalies which may indicate suspicious events. These flows are pushed to Cisco Stealthwatch Enterprise and its Global Threat Analytics, a cloud-based function of Stealthwatch Enterprise, for further analysis, risk assessment and action.

We evaluated the Cisco ETA feature for functionality and cohesion with the Cisco Catalyst switches, ASR1K routers, and Stealthwatch Enterprise enhancements in a large enterprise test environment of two systems - with and without Cisco ETA. By running a range of malware threats through each system, we determined the detection time and efficacy. From this we compared results to further deduce the positive impact of Cisco ETA deployment.

Key Findings and Conclusions

- Using the power of multi-layer machine learning, Stealthwatch creates a baseline of normal web and network activity for a host, and applies context-aware analysis to automatically detect anomalous behaviors. ETA further enhances this solution by dramatically improving speed and accuracy over time.

- Cisco ETA showed as much as 36 percent higher rates of detection than the non-ETA system, finding 100 percent of threats within three hours.
- In under five minutes, ETA detected nearly two-thirds of all malicious flows – almost double that of the non-ETA path.
- For increased flows, ETA threat detection grew more accurate and identified 100 percent of threats after 2000 flows, outperforming the non-ETA path by 8 percent.
- With only 0 to 20 flows, ETA discovered over 9 times the amount of threats than the system without it.
- After the Fast Detections stage was completed, threats were ranked by severity and readily displayed with detailed information and remediating action once confirmed.
- Stealthwatch Enterprise with Cisco ETA displays a detailed view of detected threats for additional intelligence on threat sources and similar threats in the network infrastructure.
- Crypto Standard and Revision Levels of traffic can be monitored, assessed and displayed using the additional fields available in Stealthwatch Enterprise "Flow Search" capability to ensure Corporate Cryptographic Compliance and to assist in policy actions.

The test results confirm that Cisco's Encrypted Traffic Analytics delivers impressively fast, efficient and intelligent threat detection for high-performing enterprise security. We proudly award the Cisco Encrypted Traffic Analytics the **Miercom Performance Verified** certification.

Robert Smithers

CEO

Miercom

2.0 About the Product Tested

Encrypted Traffic Analytics (ETA)

ETA is an IOS-XE feature that includes Enhanced NetFlow and uses advanced behavioral algorithms to identify malicious traffic patterns hiding in encrypted traffic. Through the analysis of message metadata and telemetry, ETA'S analysis does not require message decryption.

As additional flows are examined, patterns of metadata form a baseline of normal traffic. Any irregularities which contrast with this baseline are called out. By using metadata instead of decrypted processing as other security solutions do, ETA focuses on relevant elements rather than every single message. This dramatically reduces the negative impact of security on performance, time and resources.

ETA Components

- **NetFlow** – Identifies each flow using packet information (IP addresses, Layer 4 port numbers, timestamps, packet statistics)
- **Stealthwatch Enterprise**– Collects information from proxy servers, endpoint telemetry, policy and access engines, traffic segmentation to establish baseline behavior across the network to correlate traffic with threat behavior. Stealthwatch Enterprise also uses machine learning via its Global Threat Analytics to create a history of normal traffic, identify anomalies in flow sequences, build a behavior baseline for each host or category and update its cloud-based intelligence with malware sources and signatures

With all these components, ETA creates a contextual map to detect inbound and outbound threats, as well as discover malware activity already operating on hosts within the protected network. Detected threats are assessed for risk severity and confirmed with detailed information.

An enterprise no longer has to wait months to discover encrypted breaches. Cisco ETA can deliver detection and remediation in just a few hours.

System Versions

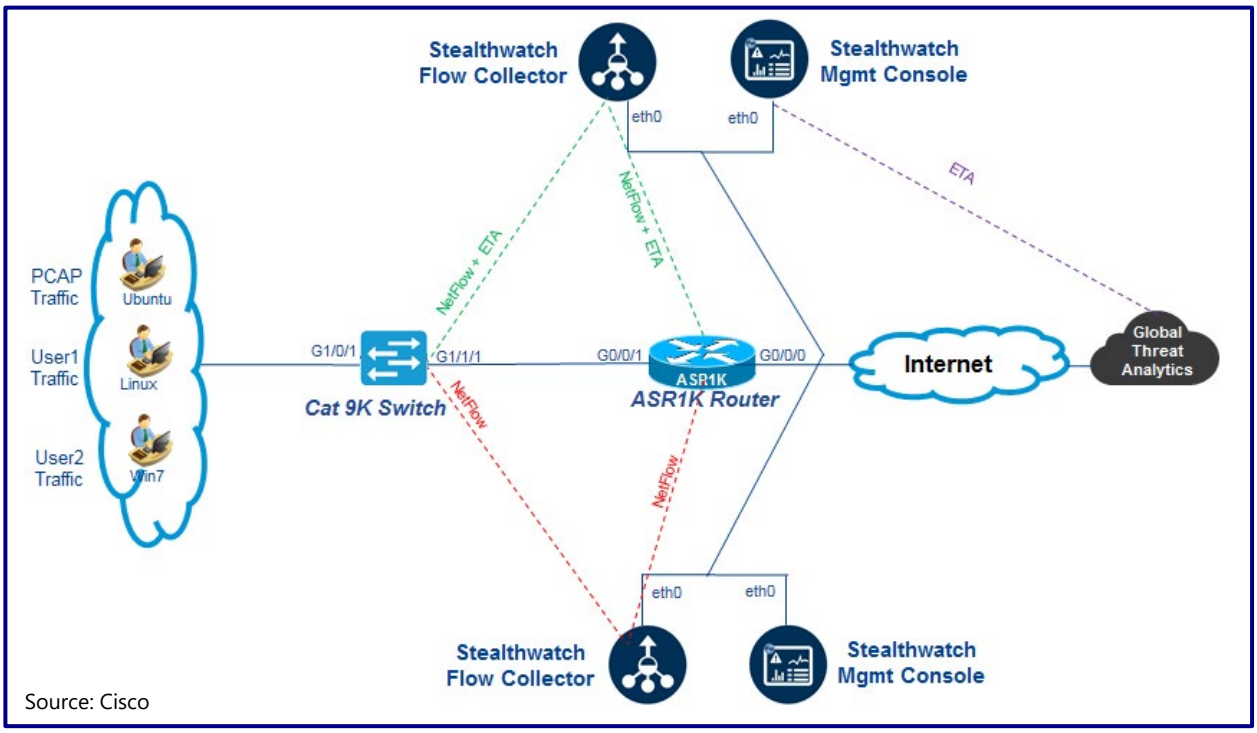
ASR1001-X router: IOS XE 16.6.2 release with an enterprise license **Cisco Catalyst 9300 switch (C9300-24P):** IOSXE 16.6.2, Network Advantage & DNA Advantage licenses	**Stealthwatch Enterprise (Flow Collector & Management Console) virtual appliances:** release with 6.9.2-01 ROLLUP patch installed on a Cisco UCS C200 M2 **PCAP PC:** Ubuntu 16.04.3 LTS installed on a Cisco UCS C200 M2

3.0 How We Did It

We tested the ability of Cisco ETA to identify and mitigate malware and exploits using a combination of generated and live malware. Threats were publicly available and privately captured, with some being unencrypted and others encrypted. Threats covered in our testing include exploits such as Trojans, Botnets, Ransomware and keyloggers. Additionally, we used malware samples that used TOR relay networks to evade detection. At least two-thirds of these threats used encrypted communications.

These samples were used to determine how quickly these known threats could be discovered. Threat flows were run at a normal traffic speed and lasted from a few minutes to several hours. The time of detection was measured with ETA on and off, for each flow routed through two separate systems.

Test Bed Setup



Source: Cisco

A set of laptops served as the source of different types of generated malware traffic. Timing was set to be as close to that of traffic configurations connected to the public internet. A selection of live generated and recorded traffic was used to emulate a variety of attack modes. Traffic was routed through a Cisco Catalyst 9300 switch and Cisco ASR1001-X router along two paths. On one path, ETA was enabled. On the other, ETA was disabled. Both paths had streams of NetFlow and Stealthwatch Enterprise data passed onto Stealthwatch Enterprise cloud-based Global Threat Analytics to demonstrate these machine learning abilities with and without ETA enabled.

4.0 Encrypted Traffic Analytics Malware Detection

4.1 Progressive Detection of Malicious Flows

Testing primarily consisted of encrypted flows sent in two directions – with and without ETA. Without ETA, encrypted malware is detected using non-encrypted portions of the messages. With ETA, flow telemetry gathers information on initial data packet exchange before an encryption session establishes, message size, direction and timing within each flow to sense irregularities in encrypted traffic that may contain malware.

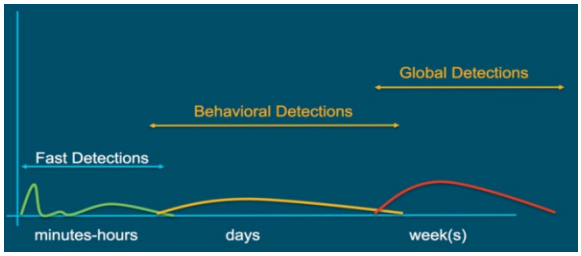
With Stealthwatch Enterprise, as more messages enter on a flow. Telemetry is gathered and stored in the cloud and is analyzed by a multi-layer machine-learning system to provide increasingly observant feedback about abnormal traffic. This includes information an operator can use to adjust the threat level of the traffic. With time, these updates provide an increasingly accurate categorization of old and new threats.

Results

The machine learning curves shown below are built on multiple stages of detection which include a feedback loop. New malware is detected and information about these threats is fed back into the system to further identify attacks earlier in this cycle.

Figure 1: Time Properties of Stealthwatch Enterprise Malware Detection and Confirmation

Phase 1 & 2: Fast Detections



Phase 3 & 4: Behavioral & Global Detections

Testing covered Phase 1 and 2 of the full ETA Detection and Confirmation process. This "Fast Detections" portion, shown above in green, uses message headers and telemetry of bidirectional traffic flows captured by ETA to identify suspicious behavior. The remaining phases continue to detect, confirm and revise flow threat levels for new and legacy malware, as well as input from system operators on new potential threats. This feedback improves detection and remediation for real threats and identifies any false positives.

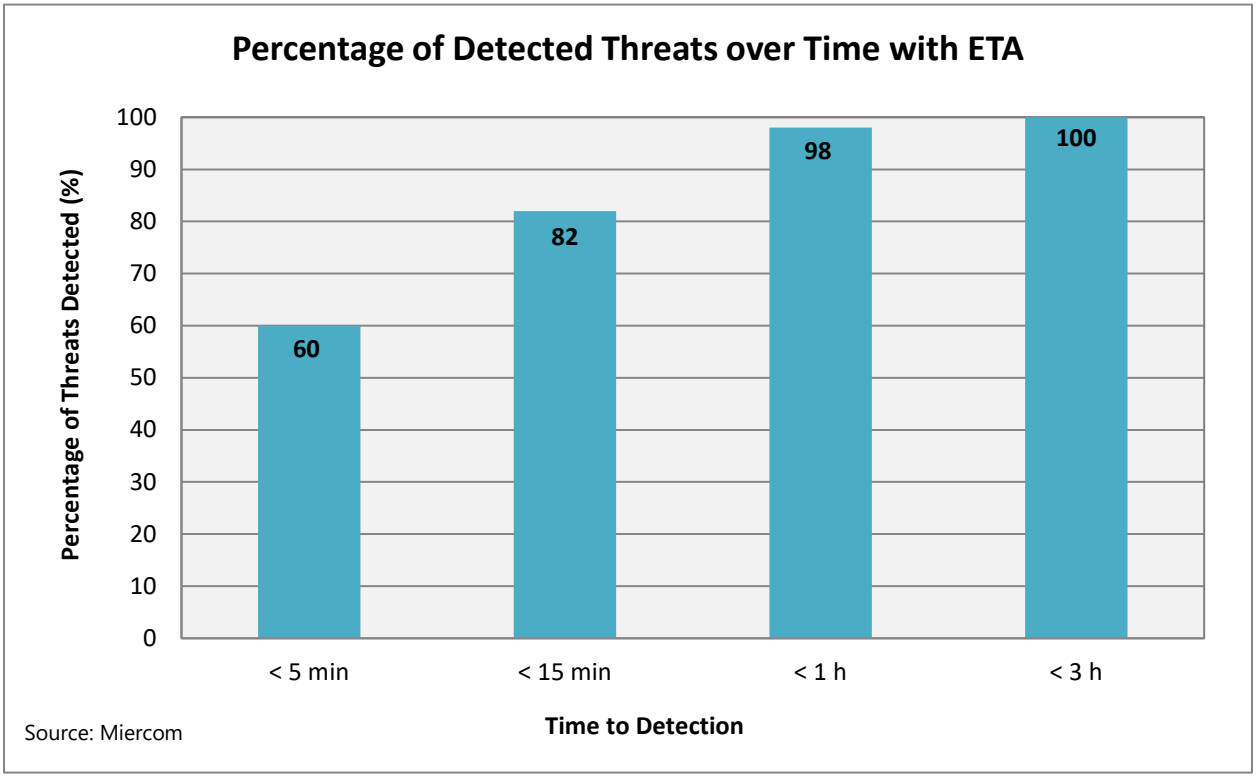
Summary

Testing observed Fast Detections made by cloud-based, machine learning malware detection using information gathered by ETA.

4.2 Time to Detect Encrypted Malware with and without ETA

The system measured the time it takes to identify flows that are known malware threats. On the ETA path, threats were detected faster than the same flow detected on the non-ETA path as shown below.

Results



The percentages of malicious flows detected over a three hour test period were recorded. The ETA path showed substantially higher detection rates than the non-ETA path, by as much as 36 percent. Within three hours, the ETA path detected all malicious flows. Without it, less than two-thirds were identified in the same timeframe. Immediate detection (under five minutes) and learning capabilities (over the course of three hours) of ETA showed impressive performance.

Summary

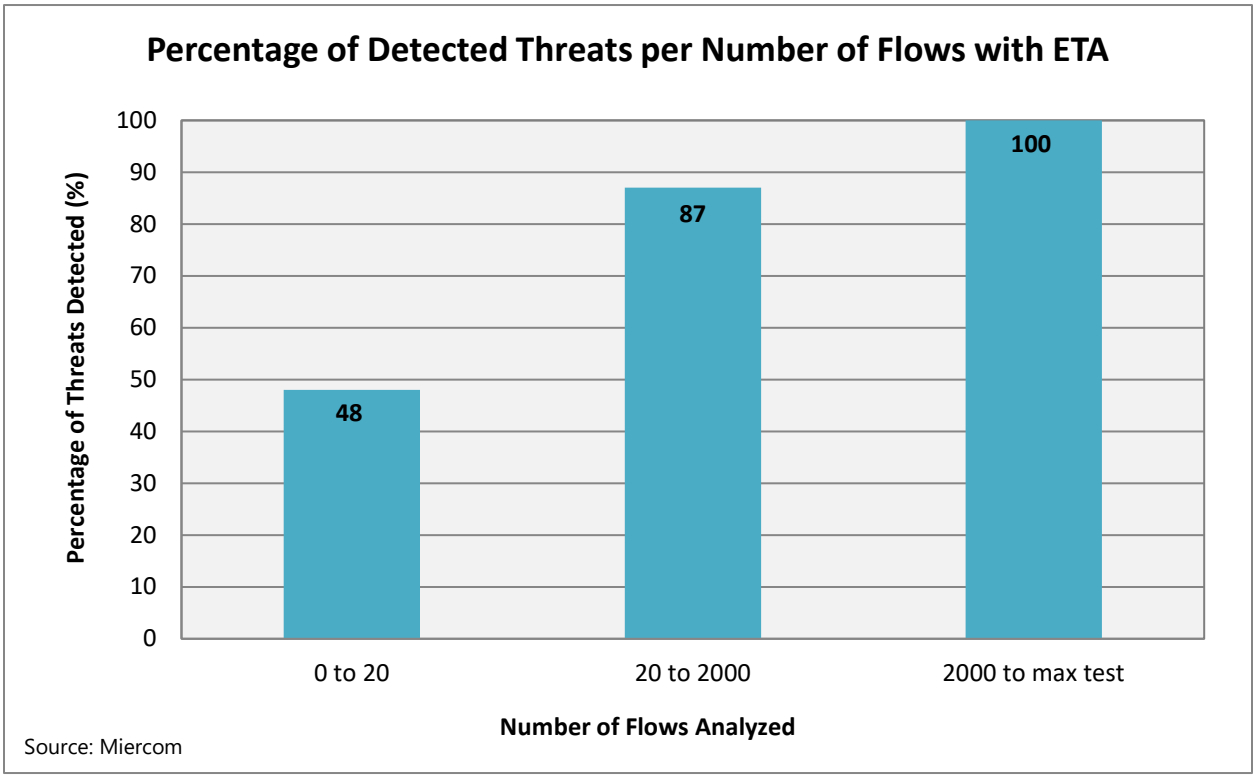
With ETA enabled, malicious flows are detected with speed and increased accuracy over time.

4.3 Role of Flows in Detection of Encrypted Malware with and without ETA

Detection accuracy was expected to improve as the number of flows increased. Flows with malicious messages contributed to the rise in accuracy by utilizing the feedback system of Phase 1 and 2 of Global Threat Analytics processing – known as Fast Detections.

The following two phases make use of the machine learning and operator feedback, allowing Detection and Confirmation of new incoming malware. These are discussed in the next section.

Results



Source: Miercom

With ETA, the first two hours of malware detection uses flow telemetry. Flows familiar to already detected flows are identified quickly. As flows increase, telemetry uses pattern anomalies to detect larger amounts of malicious flows over the course of 1-2 hours. For the first 20 flows, ETA found over 9 times the amount of threats as the path without ETA enabled. From 20 to 2000 flows, the non-ETA path is able to detect more threats, but its efficacy still falls 26 percent behind the ETA protected path. For 2000 flows or more, ETA found all threats and had an 8 percent higher rate of detection than its non-ETA counterpart.

Summary

More flows yield greater detection efficacy. ETA allows substantially higher detection rates even with just 0 to 20 flows. By 2000+ flows, it can find all threats while the non-ETA path cannot.

4.4 Detection Efficacy

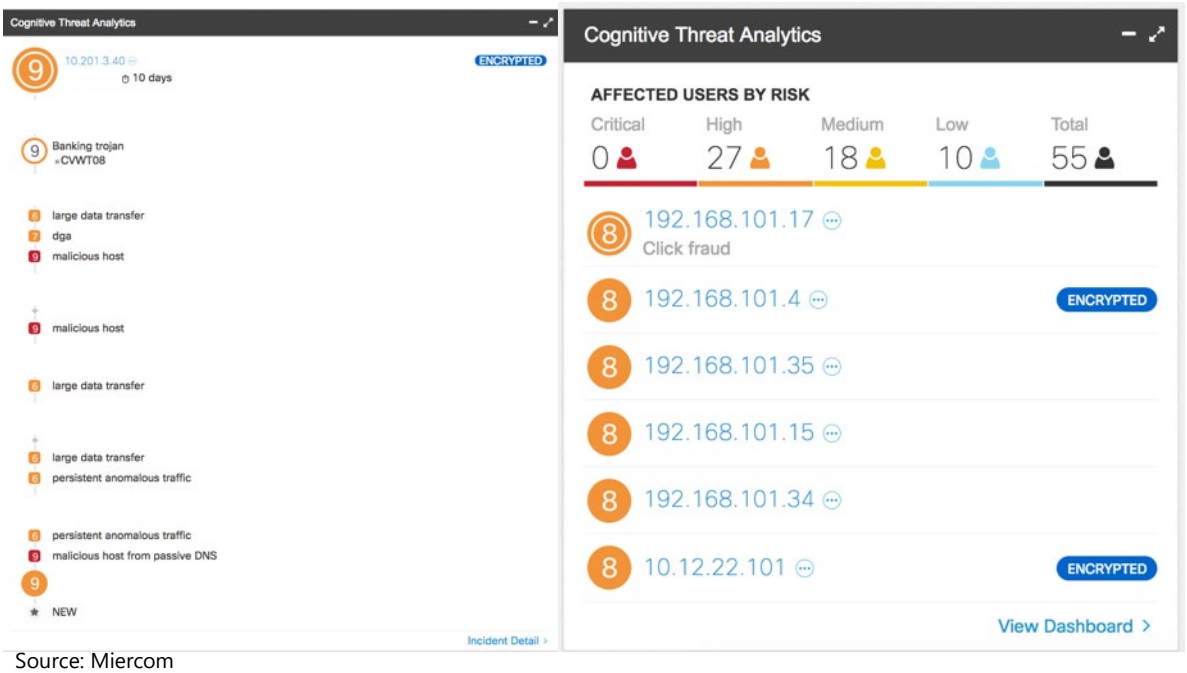
Stealthwatch Enterprise's Global Threat Analytics is the core of ETA malware detection. While it discovers harmful activity already operating on protected network hosts, it is not designed to detect and block malware infection steps or executables in transit. Using a machine-learning system, a behavioral baseline is built for each host or category to determine changes and operator input. Any contrasting information is sent to the cloud for further analysis.

With more exposure to normal traffic, threats become increasingly apparent – as discussed in the previous section. This feedback loop continually updates the context of these threats, allowing Stealthwatch Enterprise create a ranking system of severity. Risk is rated 1 through 10, 10 being the most severe.

Low-level malware flows may go through an initial detection process, as shown below (left). As additional information is collected, this level may rise as pictured below (right). A confirmed threat is indicated by an encircled number.

Results

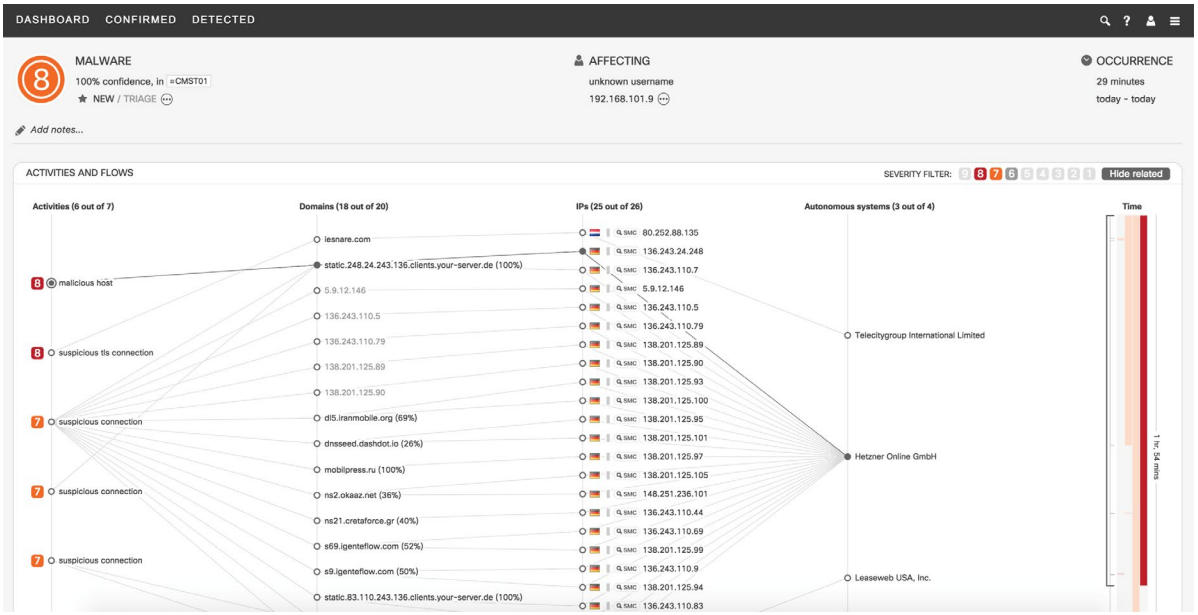
Figure 2: Stealthwatch Enterprise Detection and Confirmation



Source: Miercom

Threat severity reached the highest level of 10 where it was determined to be a ransomware attack. The number 10 risk-level was circled once confirmed as fitting all identifying characteristics of this type of attack.

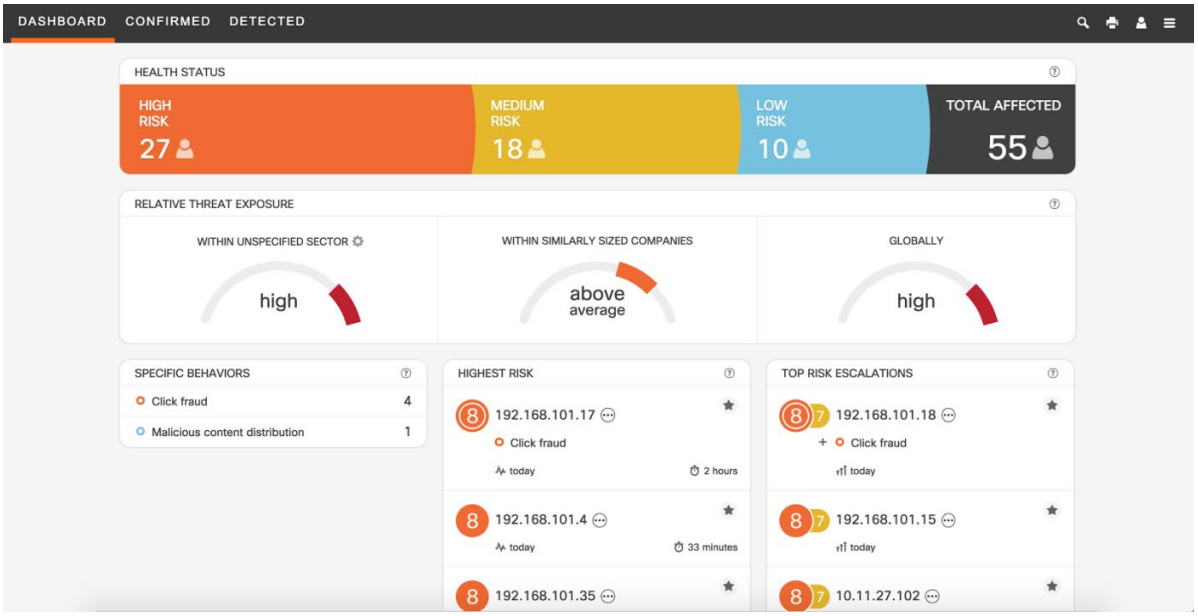
Figure 3: Related Flows of a Detected Threat



Source: Miercom

Further detail can be found on each particular threat, showing where the flow originates and how it connects to known vulnerable systems used as sources for similar previous attacks.

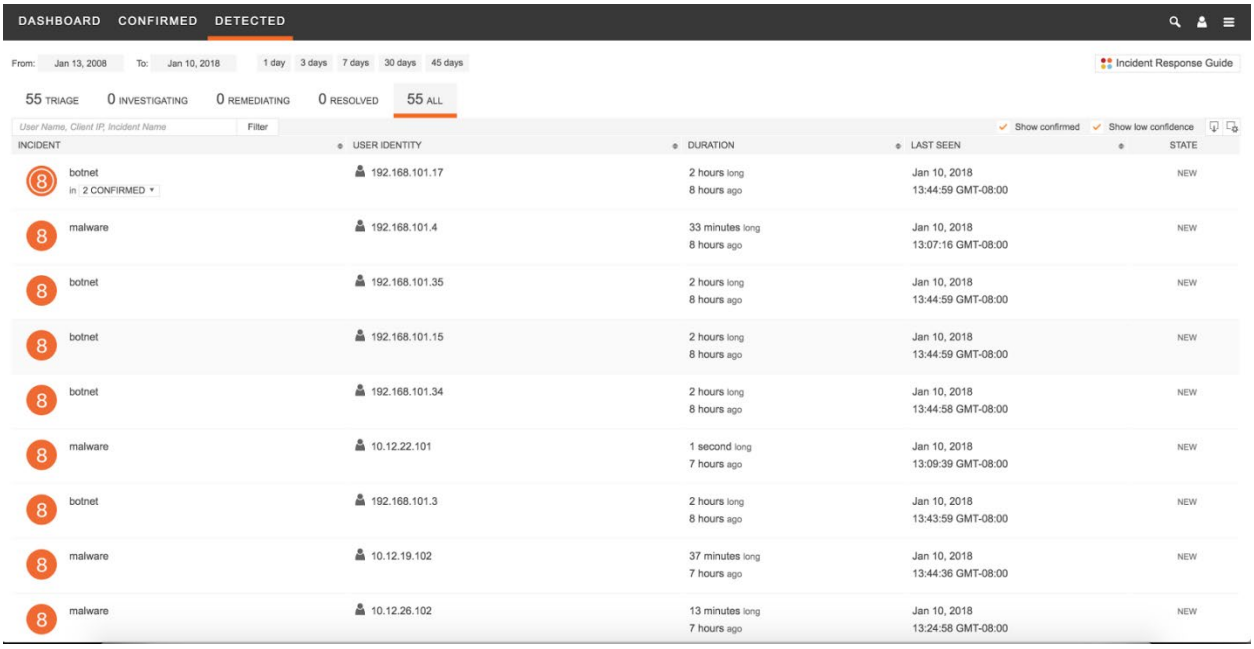
Figure 4: Actionable Confirmed Attribution



Source: Miercom

Over time, Stealthwatch Enterprise connects early detection with other related flows to reveal threat sources and similar threats. Possible events are displayed on a dashboard, separated as Detected and Confirmed. Events are further categorized by Threat Level. The interface continually informs operators of risk severity progression.

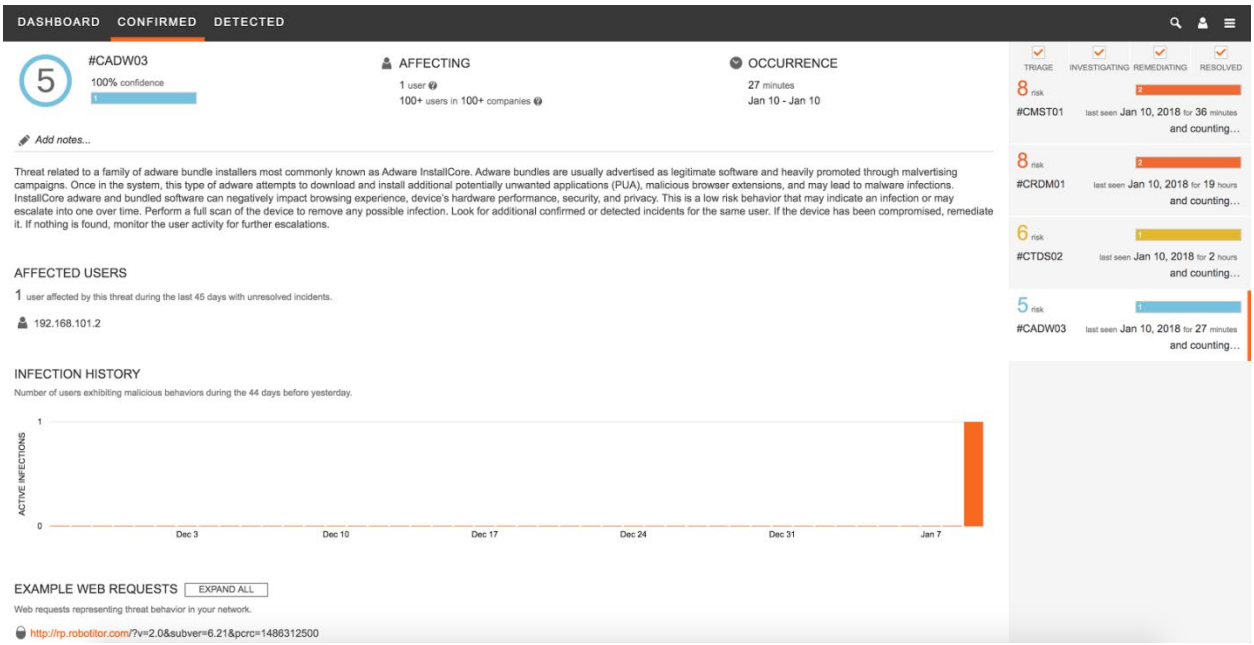
Figure 5: Detected Events List



Source: Miercom

Threats are sorted by incident, identity (e.g. IP address), attack duration, time last seen and state.

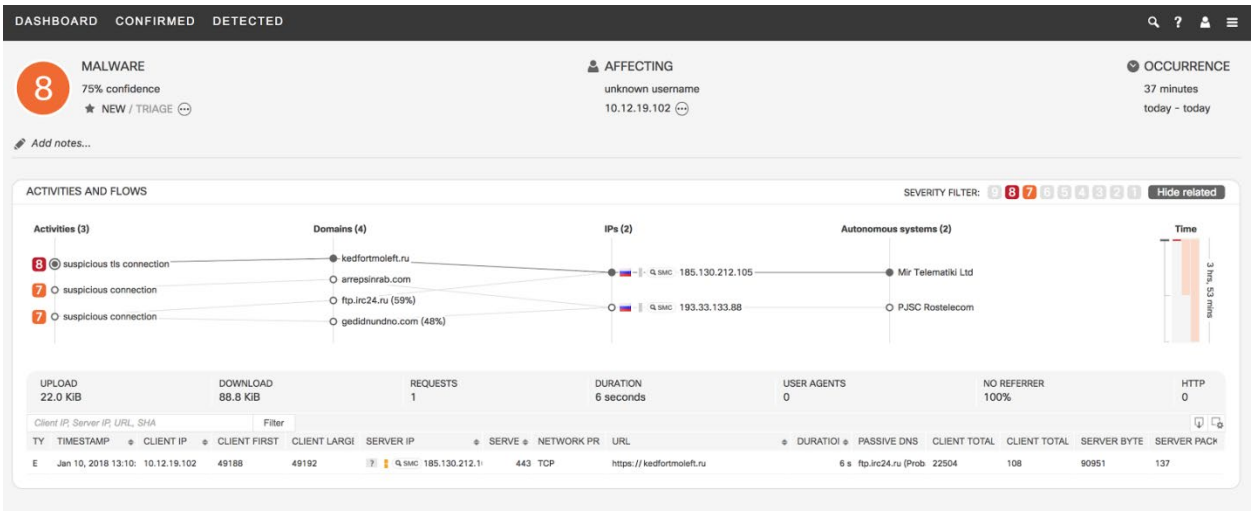
Figure 6: Confirmed Threat Detail



Source: Miercom

Confirmed threats give more detail about the attack, showing a complete description of the threat, affected users, infection history, examples, and last occurrence.

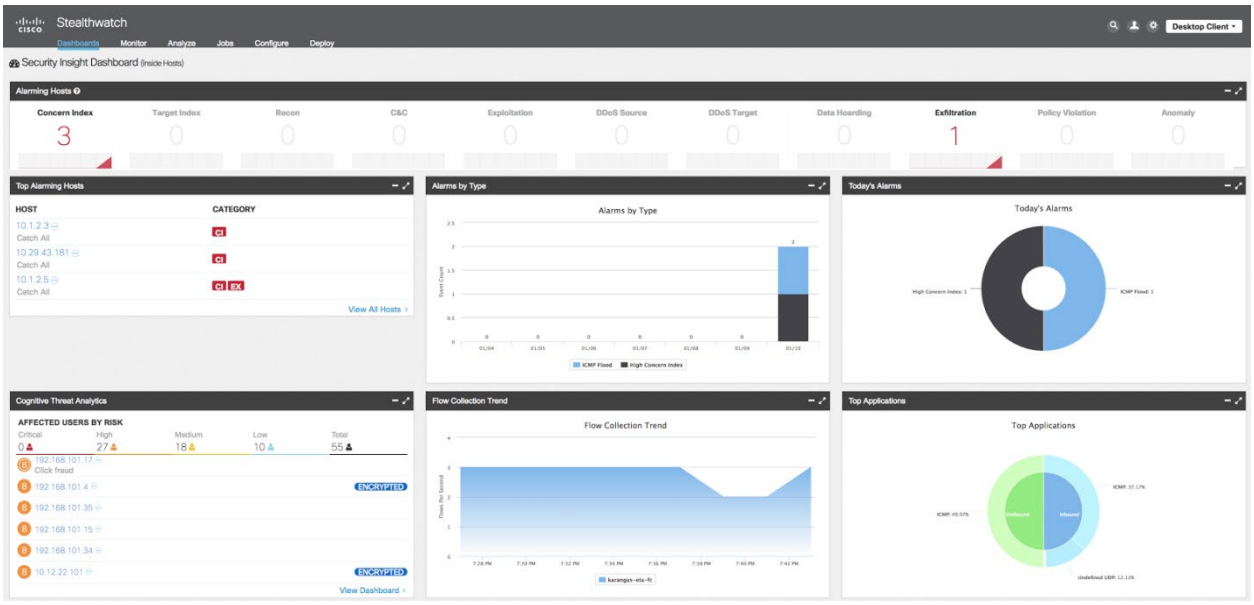
Figure 7: Attack Source Information



Source: Miercom

This view shows more detail on the attack source by activity, domains, IP addresses and systems as well as the affected user, by username and/or IP address.

Figure 8: Stealthwatch Enterprise Dashboard: Full View



Source: Miercom

The processing is completed using its Security Insight Dashboard where additional information can be found for Detection and Confirmation.

Summary

Threats are detected, ranked by risk based on growing information gathered by flows and confirmed with complete background on source, history, examples, timestamps and associated hosts or systems. The Stealthwatch Enterprise dashboard gives a full view using visual widgets.

5.0 Crypto Analytics

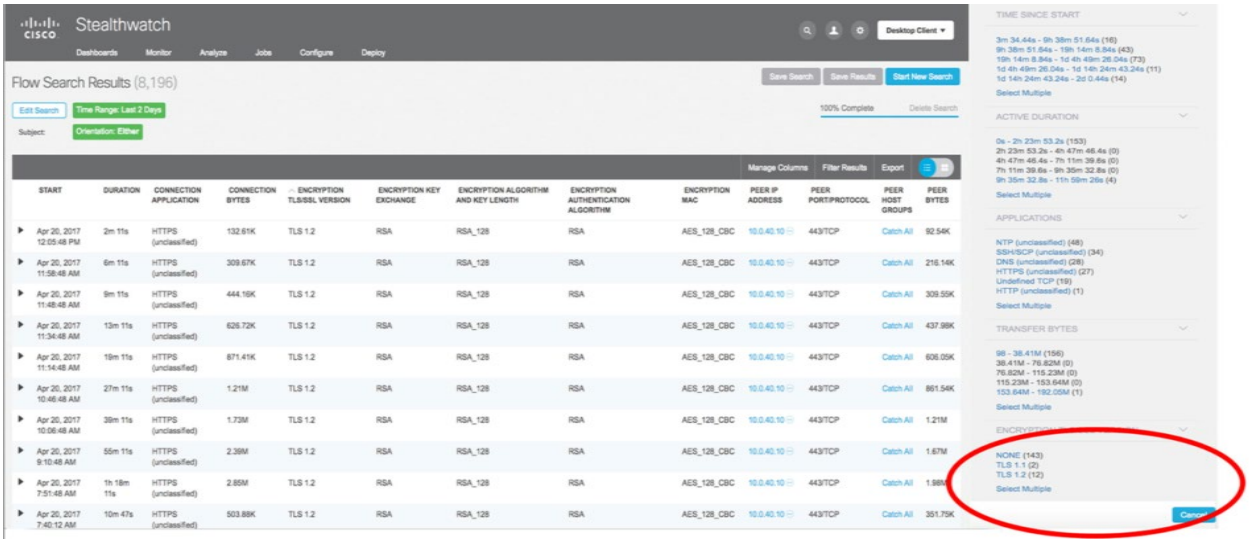
In corporate situations where there are cryptographic standards to be followed such as for PCI Compliance or Corporate IT governance to eliminate vulnerable applications, Stealthwatch Enterprise with ETA provides the data to determine if vulnerable applications are actually being used by corporate network users. This display shows the cryptographic protocol, and its version, so that corporate managers can see if users are up to date on their corporate standards.

In the magnified view, the "Encryption TLS/SSL Version" being used is "TLS 1.2". This may show other versions, such as "TLS 1.1" which may not be the approved version for corporate use, in which case the source and destination of such traffic can be identified and the Corporate standard enforced.

5.1 Corporate Cryptographic Compliance

This cryptographic assessment is displayed in Stealthwatch Enterprise and can be exported to third-party tools for monitoring and auditing of encryption compliance. It includes the encryption standard and revision level used. It is then up to the corporate policies to determine what actions to take.

Results



Source: Miercom

The red circle indicates where to find the summary of all crypto standards with revision levels and instance count for each.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.