Encrypted Traffic Analytics Q&A

Q

What is the official name of this solution?

A

Cisco® Encrypted Traffic Analytics.

Q

What is Encrypted Traffic Analytics?

A

Encrypted Traffic Analytics is a solution that provides visibility into encrypted traffic in order to detect malware within encrypted communications.

Q

What are the components of the Encrypted Traffic Analytics solution?

A

Encrypted Traffic Analytics is enabled by new features within the Cisco Stealthwatch® portfolio and Cisco's newest switching and routing infrastructure. Participating products include:

- New metadata transported over NetFlow with Encrypted Traffic Analytics from the new Cisco IOS® XE Software based Cisco Catalyst® 9000 switching family and routers such as the Cisco 4000 Series Integrated Services Routers, ASR 1000 Series Aggregation Services Routers, Cloud Services Router 1000V Series, and Integrated Services Virtual Router, including Enterprise Network Compute System.
- Cloud-based machine learning classifier algorithm from Cognitive Analytics, which is a feature of Stealthwatch version 6.9.2.
- New cryptographic compliance capabilities in Stealthwatch.

Q

What is Cognitive Threat Analytics?

A

Cognitive Threat Analytics is a cloud-based threat enrichment and intelligence capability that uses supervised machine learning classifier algorithms and is a feature of Stealthwatch in versions 6.9 and later. Cognitive Threat Analytics is also a feature of Cisco Advanced Malware Protection (AMP) and Web Security Appliance.

Q

What types of hidden malware can be detected?

A

Network devices with Encrypted Traffic Analytics capabilities enabled are able to derive new metadata from Secure Sockets Layer (SSL) and Transport Layer Security (TLS) sessions that transit the configured device.

Q

Does Encrypted Traffic Analytics require any special license on a network device?

A

Encrypted Traffic Analytics is enabled as part of the Security features license (or k9 license) or the Cisco DNA Advantage or Cisco ONE™ license bundles.

Q

How is this new Encrypted Traffic Analytics metadata transported?

A

Encrypted Traffic Analytics data is exported from a configured network device to a capable flow collector. At this time, the only NetFlow collector capable of processing Encrypted Traffic Analytics metadata is the Cisco Stealthwatch Flow Collector for NetFlow version 6.9.2 or later.

C67-740080-00 12/17