**Three Important Security Analytics Attributes.**

**Hint: Machine Learning is Just One**

Yes, with the growth in security vendors claiming to do **Artificial Intelligence and Machine Learning**, one might think it’s the ultimate answer to keeping organizations secure! It is definitely a rapidly evolving technology with many benefits. But while evaluating a security solution, it’s important to understand the context in which machine learning is applied. Actually, first, it is important to understand what AI and machine learning even is.

**Network visibility and security analytics** is increasingly becoming an essential component of an organization’s security strategy. These solutions are also referred to as network behavioral monitoring, network traffic analysis (NTA), network behavior anomaly detection (NBAD), etc.

The growth of the attack surface is real! Employees demand access from multiple locations and devices, and workloads are increasingly moving to the cloud. And the bad guys aren’t always hacking in, they’re logging in as well. So you need visibility everywhere, including data center, branch, endpoints, and cloud. Applying security analytics to network traffic provides one of the only ways to, for example, discover data exfiltration from your cloud instance or illicit cryptomining activity within compromised IoT devices. According to research, **92%** of the security professionals admitted that they see value in deploying such tools.

Cisco’s network security analytics solution, [Cisco Stealthwatch](https://www.cisco.com/go/stealthwatch), offers threat detection and threat hunting capabilities leveraging your network infrastructure. It uses a combination of analytical techniques to find threats hiding within your network, including encrypted traffic, and provides the necessary information for a rapid incident response.

Here’s three things you should demand from a network visibility and security analytics solution.

1. **Comprehensive data collection**

Before we even get into the “analytics” part of this, it’s important to begin with the right data set. First, most security analytics solutions rely on agents or sensors to provide visibility into the network traffic, but it’s not feasible as the network continues to expand rapidly with the growing business needs. With a **single, agentless** appliance, Stealthwatch provides visibility into the extended network, [including hybrid- and multi-cloud environments](https://blogs.cisco.com/security/no-one-can-detect-threats-in-your-public-cloud-like-cisco), data center, and branch. Secondly, with the rise in encrypted traffic, you can struggle with dark spots in the network even if you are consuming the enterprise telemetry. Stealthwatch, using [Encrypted Traffic Analytics](https://www.cisco.com/go/eta), is able to analyze the enhanced telemetry from encrypted traffic, without decryption. And lastly, Stealthwatch is a well-integrated solution that derives **context** from multiple sources for advanced threat detection and response. For example, it gets user contextual data from [Cisco Identity Services Engine (ISE)](https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html). Stealthwatch also ingests proxy, web, and endpoint data to provide a complete picture.

1. **Layered analytical techniques, working together**

The next step is to apply advanced security analytics to the rich network telemetry and other contextual data, to catch threats lurking in your environment in real-time.

* **Behavioral modeling**

Stealthwatch closely monitors the activity of every device on the network and is able to create a baseline of normal behavior. In addition, it also has a deep understanding of known bad behavior. It applies close to 100 different security events or heuristics that look at various types of traffic behavior, such as scanning, beaconing host, brute force login, suspect data hoarding, suspect data loss, etc. Think about a physician examining a patient’s symptoms. The physician doesn’t determine a diagnosis based on just one symptom. Similarly, Stealthwatch doesn’t look at one incident in isolation to trigger an alarm.

* **Multilayered machine learning**

Stealthwatch also applies machine learning, both supervised and unsupervised, to discover the full spectrum of bad communications. It also integrates with a multistage machine learning analytics engine, which correlates threat behaviors seen **locally** within the enterprise with those seen **globally**. There are multiple layers of processing to gradually build a notion of “what is anomalous”, then classify actual individual pieces of “threat activity” (because what is anomalous might not necessarily be malicious), which would culminate with a final conviction of whether or not a device or user is in fact compromised.

* **Global threat intelligence**

A global threat intelligence feed powered by the [Cisco Talos](https://www.talosintelligence.com/)™ intelligence platform provides an additional layer of protection against botnets and other sophisticated attacks. With Talos, adversaries have nowhere to hide. The platform sees 1.5 million daily malware samples, 16 billion daily web requests, and has multiple researchers and partners round the world keeping an eye on emerging threats.

How does this unique analytics pipeline benefit Stealthwatch customers?

* **High-fidelity threat detections** – Customers consistently rate upwards of 90% Stealthwatch alerts as helpful. The machine learning engine classifies incidents as either **“confirmed”**or “**detected”.** A confirmed incident carries with it a 99 to 100 percent confidence. And detected incidents are unique to you and part of a very targeted campaign
* **Detection of unknown threats** – Stealthwatch also monitors the behavior of suspicious servers across the world to create a Global Risk Map. And there are multiple other events that Stealthwatch is constantly observing. So even if an attacker is using a new or unique malware strain, Stealthwatch would still be able to detect it
* **Autonomous noise reduction** – Stealthwatch gathers vast amounts of telemetry from the network and applies analytics to boil down thousands of alerts to a few actionable critical incidents. [At a recent global conference](https://blogs.cisco.com/security/cisco-catches-thousands-of-hidden-threats-on-a-massive-public-network), Stealthwatch detected more than 32,000 security events and drastically reduced them to 350 significant security detections
* **Real-time threat detections** – Stealthwatch analytics looks at early indicators of an attack such as port scanning, communication to suspicious domains, etc. to pinpoint threats before they are able to create havoc

*“With Cisco Stealthwatch, false positives are almost none whenever we are alerted for spikes which is very useful.”*

— Security Manager, Medium Enterprise Banking Company

1. **Rapid incident response**

Your security analytics tool detected a threat, now what? Stealthwatch provides the contextual information to pinpoint the source of the threat easily. And it integrates with your existing workflows to provide information to other tools such as a SIEM. Through the integration with ISE, you can **quarantine** the suspicious host instantly, continue investigating the threat, and determine where it might have propagated. Stealthwatch also has the capability to store enterprise telemetry for a certain period of time and serves as a valuable forensic tool.

So it’s a combination of all these features and capabilities that makes Cisco Stealthwatch a strong contender for your network visibility and security analytics solution.

Assignment:

* 1. List & elaborate on the three things you should demand from a network visibility and security analytics solution
  2. Explain how [Cisco Talos](https://www.talosintelligence.com/)™ intelligence platform serves as global intelligence for threats.