AMP for Endpoints – Premier

SecureX Threat Hunting FAQ

What is Cisco announcing?

We are announcing the introduction of a Premier tier of AMP for Endpoints that includes all of the functionality in AMP for Endpoints Advantage and on top of that our new SecureX Threat Hunting capability.

Q **What is SecureX Threat Hunting?**

A SecureX Threat Hunting is an analyst-centric process that enables organizations to uncover hidden advanced threats. Once threats are detected, customers are notified within their AMP Console, so they can begin remediation. Threat Hunting is a proactive approach to threat detection, which tells the incident responders a narrative of how an attack was spotted and how it evolved. The purpose is to discover and thwart attacks before they cause any damage. As a side-effect of leveraging a regular and continuous Threat Hunting, an organization increases their knowledge of vulnerabilities and risks which further allows the hardening of their security environment.

Q **What makes SecureX Threat Hunting different than other solutions?**

A SecureX Threat Hunting is not a managed service, it is a feature embedded tightly inside the AMP for Endpoints product and along-side all of its other detection mechanisms. As such it is designed to produce additional net new high-impact findings.

Q **When will SecureX Threat Hunting be released?**

A General availability is scheduled for June 30, 2020.

Q A

What are the major features of SecureX Threat Hunting?

The AMP Console features a Threat Hunting report that shows the new findings with all of the relevant context and events mapped to MITRE ATT&CK TTP's, together with recommendations for customer incident responders on what to do next in terms of further investigation or remediation of the findings.

Q A

How does SecureX Threat Hunting complement other Cisco products and services?

SecureX Threat Hunting is specific to the AMP for Endpoints product initially and it does complement its existing capability with new hypothesis-driven detections continuously executed and maintained by Cisco experts.

Q A

Is SecureX Threat Hunting an MDR offering?

SecureX Threat Hunting is not a managed service per se. It does not replace a customer analyst in front of the AMP Console. It instead focuses on delivering and highlighting high-impact findings that should receive priority from the customer analysts in terms of response.

Q A

How is SecureX Threat Hunting deployed and managed?

SaaS-based delivery just like all of AMP for Endpoints. Customers are encouraged to deploy Orbital so that the SecureX Threat Hunting can tap into richer telemetry.

Q A

With SecureX Threat Hunting is any endpoint data captured and if so, what type?

The endpoint data captured is from the AMP and Orbital telemetry data sets.

Q A

Where is the data stored that SecureX collects stored?

All data used for hunting is stored in a private AWS data store in North America, that is only accessible by SecureX Threat Hunters.

Q A

What operating systems are supported?

All OSes currently supported by AMP for Endpoints.

Q A

How will existing customers upgrade if they have Essentials? Advantage?

Upgrades depend on the PID's used during their original order. SBP (Software Buying Program) customers can use SBP to update and effectively upgrade the tier in their orders. TnC customers can be dealt with as rebooking.

Q A

Will customers need to redeploy agents?

No – but customers encouraged to deploy Orbital across their environment.

Q A

In what regions and supported languages will this be available

Same as AMP for Endpoints. However, Data Centers for SecureX Threat Hunting are initially located only in North America. Threat Hunting information will only be in English, however, menus and titles will be localized.

Q
A

What is the pricing and packaging model? New customers and existing customers?

Packaging and pricing are available in the standard AMP for Endpoints Ordering Guide. SecureX Threat Hunting is available within the AMP for Endpoints Premier tier.

Q
A

How do I engage with analysts?

There is no direct engagement with SecureX Threat Hunters. Should the customer need assistance, they can engage TAC, CX or Talos IR depending on the need.

Q
A

What if I don't see any alerts?

There will be individual statistics for each hunt based on the entire data set of AMP to showcase how many businesses and hosts are affected by the threat. This is confirmation that your organization hasn't experienced this specific threat. SecureX Threat Hunting metrics reports will also be available.

Q
A

How are threat hunts executed on the backend?

All threat hunts executed are based on intelligence, TTP, anomaly, machine learning, and manual research, along with the data sources available (i.e. AMP, Orbital, Umbrella).

Q
A

Who is behind the threat hunts (human-driven vs machine-driven detections vs combined)?

Cisco delivers highly automated human-driven hunts based on playbooks producing high fidelity alerts. The process uniquely combines the new Orbital Advanced Search technology with expertise from elite threat hunters, with 20 years of industry experience, to proactively find more sophisticated threats. The entire process is highly automated and that does also include algorithmic machine-driven detections.

50+ daily hunts are scheduled and automated, the results are investigating by analysts.

Researchers develop various engines to perform data stacking, masquerading detection, and process analytics. Results are investigated by analysts.

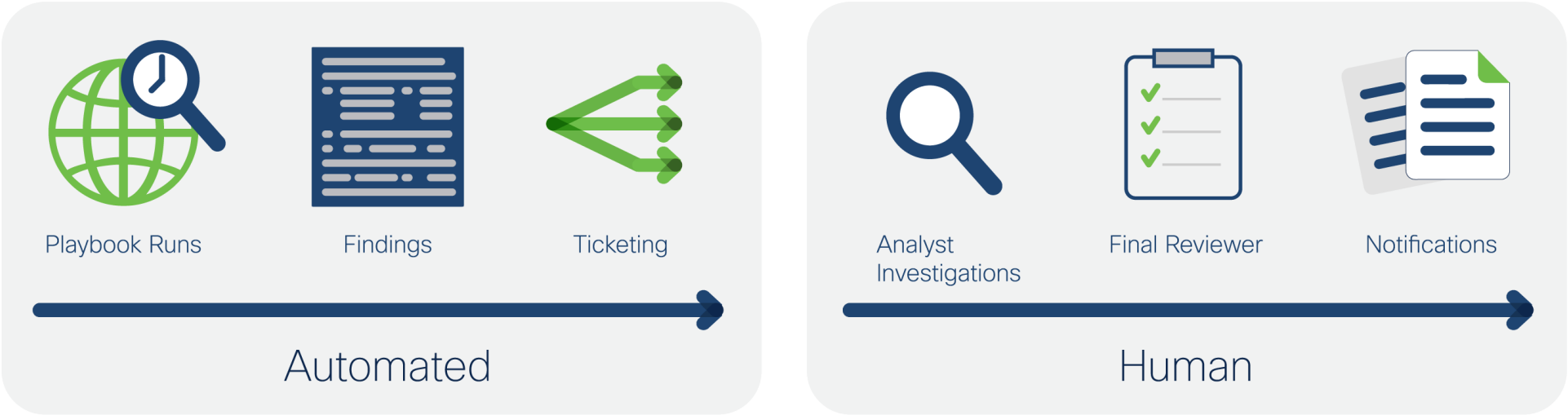
Q
A

Is the team behind the service a part of Talos or does it include Talos team members, what's the interaction with Talos?

Threat Hunting within AMP for Endpoints is managed by Cisco a nd leverages the expertise of both Talos and the Cisco Research and Efficacy Team to help identify threats found within the customer environment.

Example workflows for executing threat hunts

(playbook driven, scheduled, triggered, etc.)



Q A

How does SecureX Threat Hunting Compare with services such as MDR/MSSP?

SecureX Threat Hunting is deeply embedded with AMP for Endpoints, as a feature. The feature delivers continuous hunts. It is not a managed service and it does not provide direct interaction with Cisco analysts.

Q A

What data sources used for threat hunts (which Cisco products if not just AMP)?

Currently, the data sources used for SecureX Threat Hunting are AMP and Orbital.

Q A

What is in scope for the service (incident notification only, recommendations, actions, etc.)?

Customers get notified of an incident that does include a summary of what type of threat or behavior has been observed and what that means for the customer in terms of the possible impact. If there are events associated with the incident, they will be shown on a timeline. Finally, there are additional references such as mapping to MITRE ATT&CK and a clear set of recommendations on what to do next in terms of investigation and remediation of the threat.

Q **Can customers have bi-directional communications with threat hunters?**

A Not at this time.

Q **What regions will this be available (APJC specifically, if not immediately, timelines for APJC availability)?**

A Same as AMP for Endpoints. However, Data Centers for SecureX Threat Hunting are initially located only in North America. Threat Hunting information will only be in English, however, menus and titles will be localized.

Q **Is the service for increasing net new detections or improving and providing additional context for existing detections, or both?**

A Net new detections.

Q **Are there any SLAs for the feature and how are they managed?**

A There are no SLAs for this feature.

Q **How is data privacy guaranteed for the service?**

A Read the Privacy Data Sheet.

Q **What is the escalation process for the service, how to file disputes / provide feedback?**

A Same as AMP for Endpoints.

Q **Is SecureX Threat Hunting available for AMP Private Cloud?**

A No, SecureX Threat Hunting will not be available for AMP Private Cloud.