TL

TODD LAMMLE

Advanced Network Training

1.0: Cisco Secure Endpoint Hands-On-Course

About
Michael O’Connell

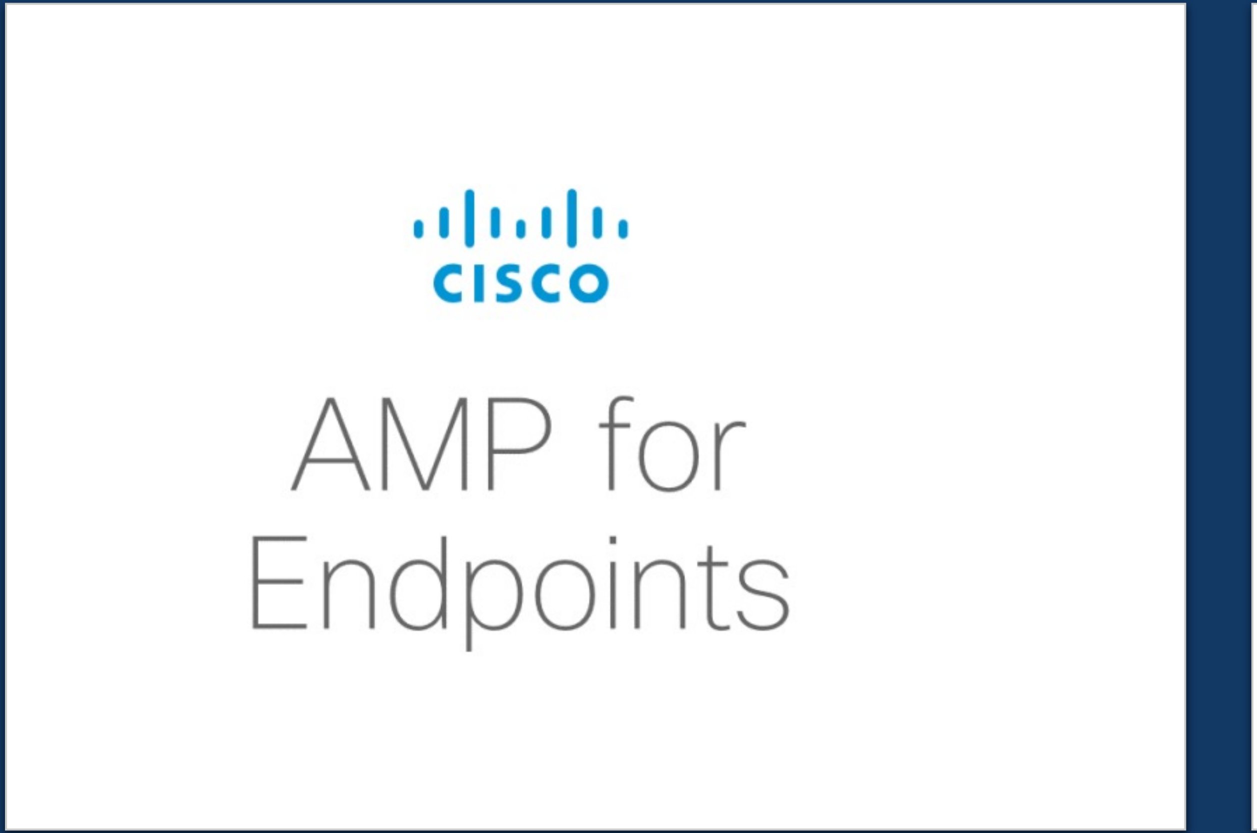
Twitter: @MichaelOConn

Linkedin: michaeloconnell1984

Email: mike@lammle.com

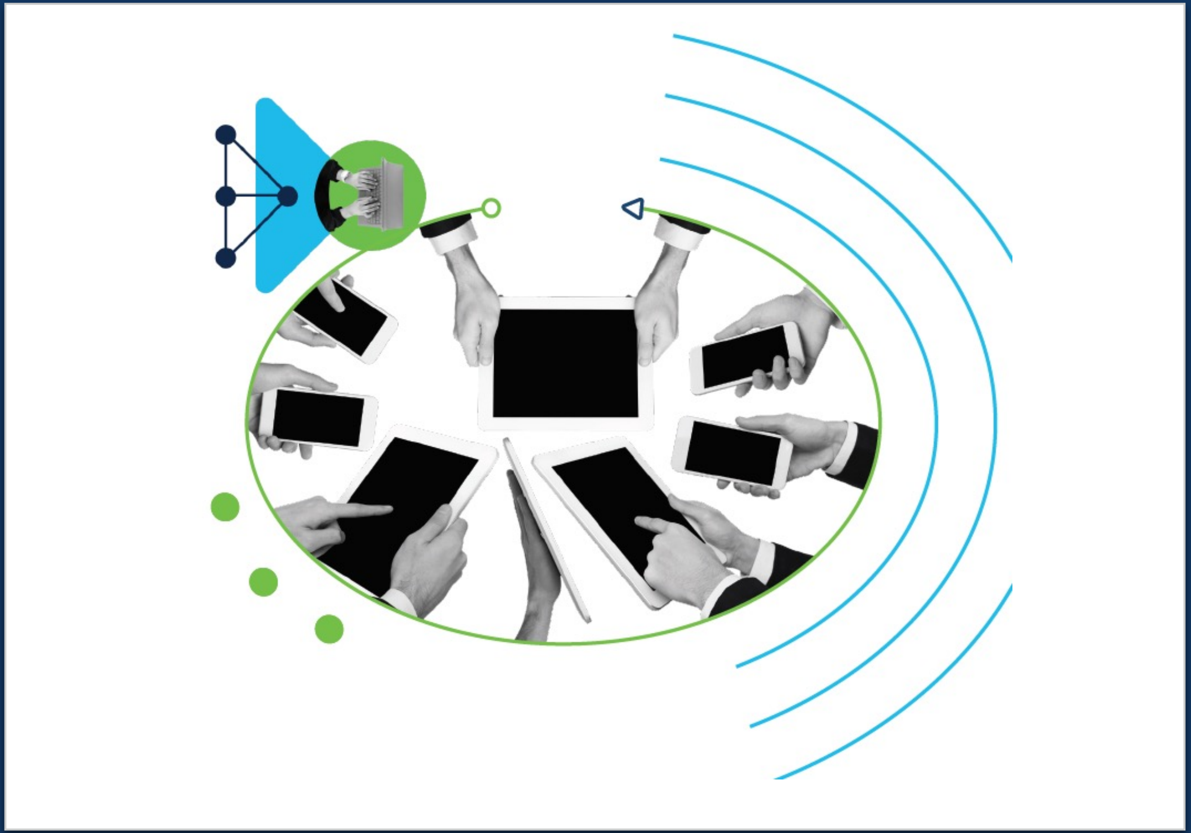
www.lammle.com/AMP

Cisco Secure Endpoint



cisco

AMP for Endpoints



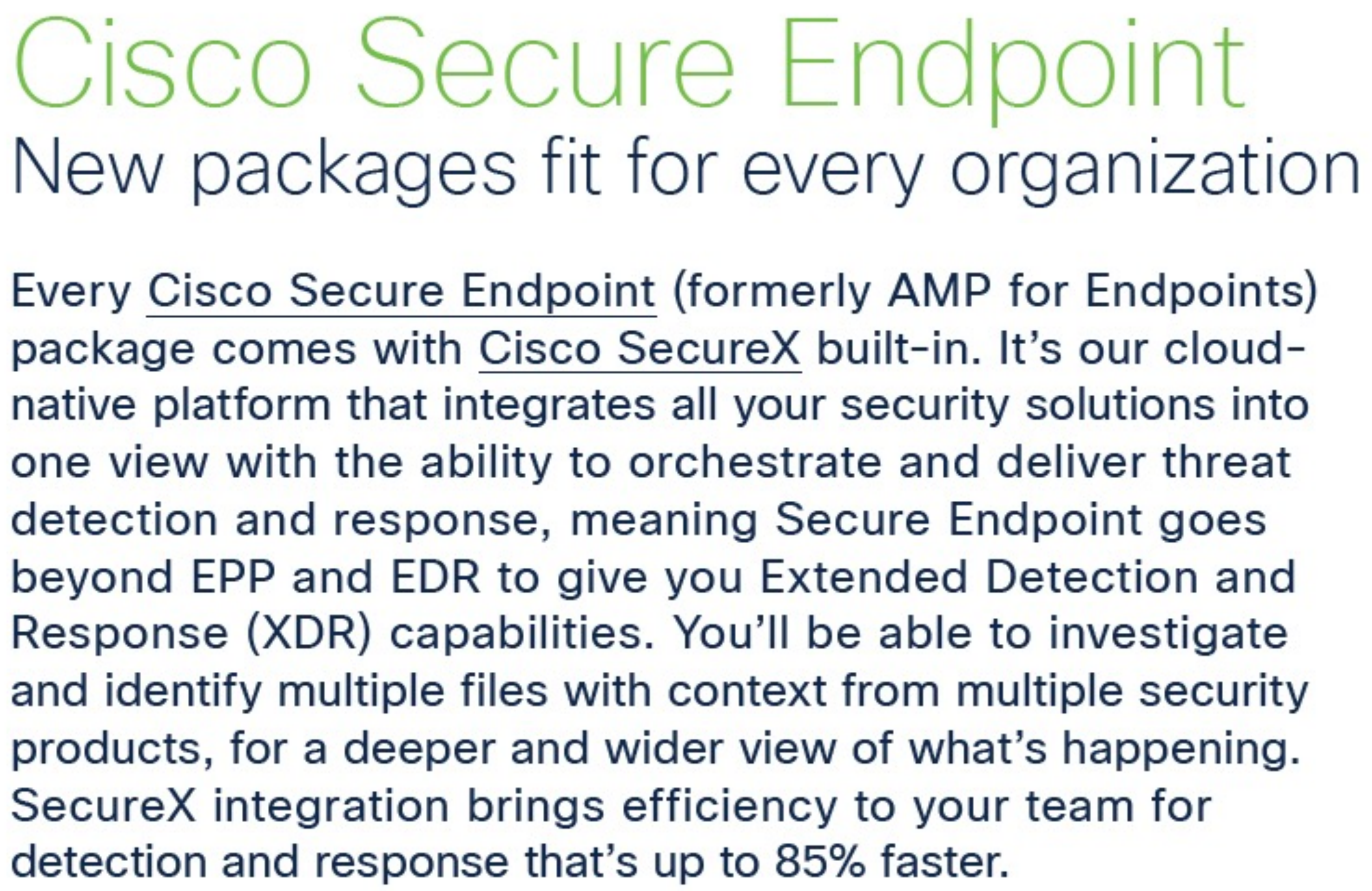
Cisco Secure Endpoint Background:

Secure Endpoint Statistics:

20 billion threats blocked daily with Cisco Secure Endpoint.

1.5 million unique malware samples analyzed daily by Cisco Talos.

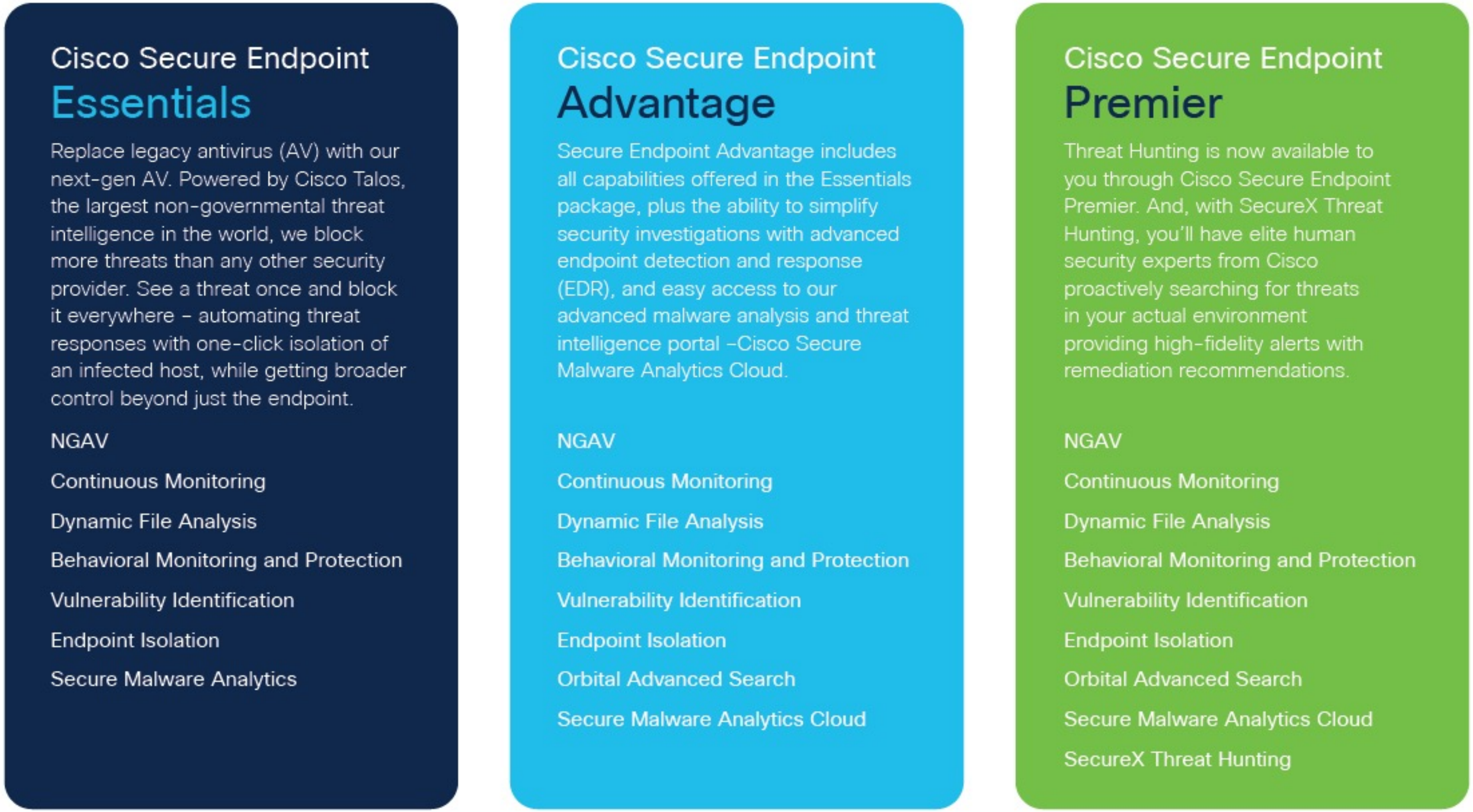
14 integrated detection techniques compared to 4 in competing products.



Cisco Secure Endpoint

New packages fit for every organization

Every Cisco Secure Endpoint (formerly AMP for Endpoints) package comes with Cisco SecureX built-in. It's our cloud-native platform that integrates all your security solutions into one view with the ability to orchestrate and deliver threat detection and response, meaning Secure Endpoint goes beyond EPP and EDR to give you Extended Detection and Response (XDR) capabilities. You'll be able to investigate and identify multiple files with context from multiple security products, for a deeper and wider view of what's happening. SecureX integration brings efficiency to your team for detection and response that's up to 85% faster.



Cisco Secure Endpoint Essentials

Replace legacy antivirus (AV) with our next-gen AV. Powered by Cisco Talos, the largest non-governmental threat intelligence in the world, we block more threats than any other security provider. See a threat once and block it everywhere – automating threat responses with one-click isolation of an infected host, while getting broader control beyond just the endpoint.

NGAV

Continuous Monitoring

Dynamic File Analysis

Behavioral Monitoring and Protection

Vulnerability Identification

Endpoint Isolation

Secure Malware Analytics

Cisco Secure Endpoint Advantage

Secure Endpoint Advantage includes all capabilities offered in the Essentials package, plus the ability to simplify security investigations with advanced endpoint detection and response (EDR), and easy access to our advanced malware analysis and threat intelligence portal –Cisco Secure Malware Analytics Cloud.

NGAV

Continuous Monitoring

Dynamic File Analysis

Behavioral Monitoring and Protection

Vulnerability Identification

Endpoint Isolation

Orbital Advanced Search

Secure Malware Analytics Cloud

Cisco Secure Endpoint Premier

Threat Hunting is now available to you through Cisco Secure Endpoint Premier. And, with SecureX Threat Hunting, you'll have elite human security experts from Cisco proactively searching for threats in your actual environment providing high-fidelity alerts with remediation recommendations.

NGAV

Continuous Monitoring

Dynamic File Analysis

Behavioral Monitoring and Protection

Vulnerability Identification

Endpoint Isolation

Orbital Advanced Search

Secure Malware Analytics Cloud

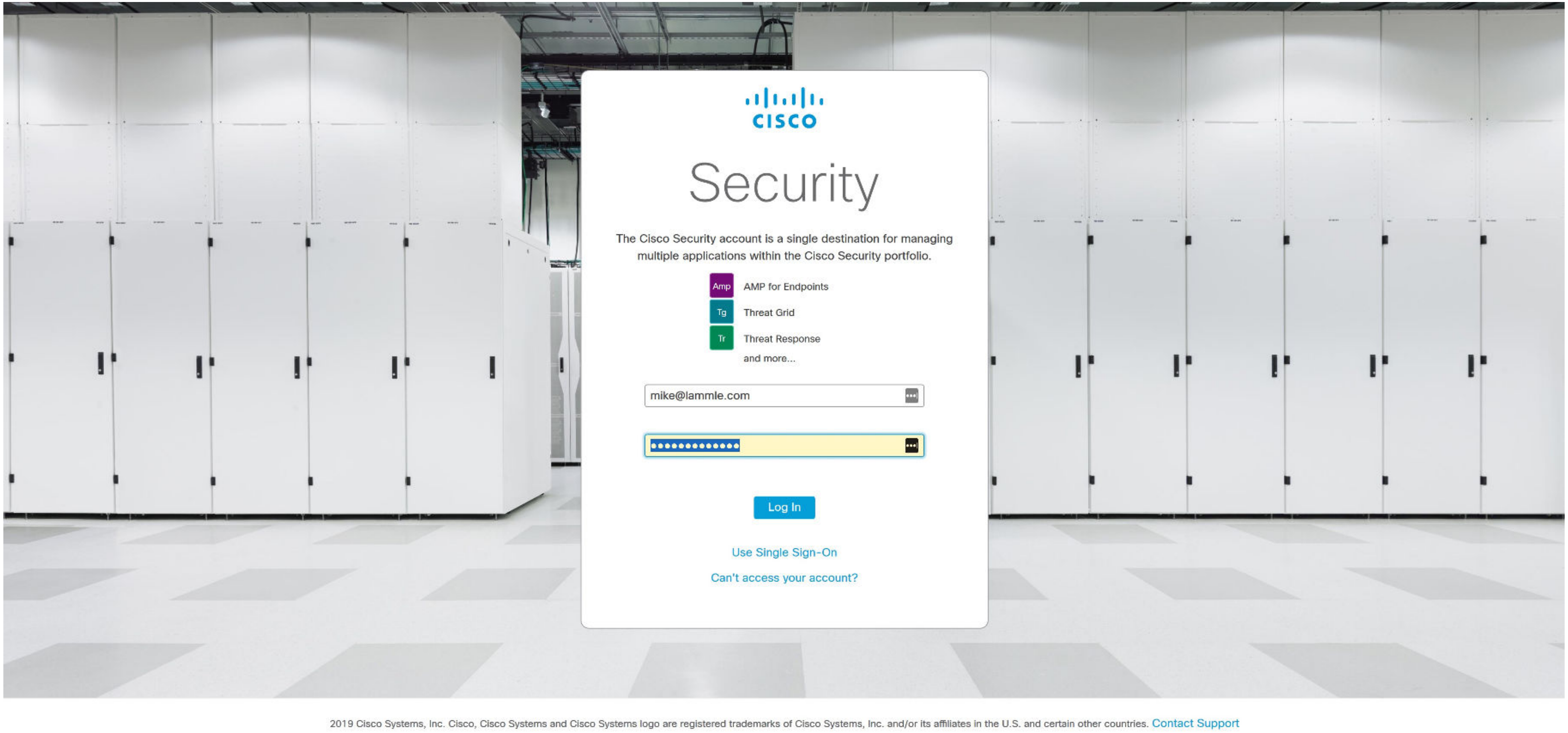
SecureX Threat Hunting

TODD LAMMLE

Cisco Secure Endpoint Course Overview

- Introduction to Cisco Secure Endpoint Technologies
- Console Interface and Navigation
- Using Secure Endpoint Best Practices.
- Debug Policies
- Group Creation.
- Simple and Custom Detections.
- Whitelist Hashing.
- Indications of Compromise.
- Connect / Performance Troubleshooting.
- Orbital Advanced Search.
- Upgrading and Operations.
- Endpoint Isolation.
- Cisco Secure X and API Integration.

Logging into your Portal



cisco

Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

- Amp AMP for Endpoints
- Tg Threat Grid
- Tr Threat Response
- and more...

mike@lammle.com

●●●●●●●●●●●●●

2019 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Contact Support