Automating Cisco Endpoint Security Solutions Using APIs

PROTECTING USERS WITH CISCO AMP FOR ENDPOINTS

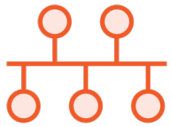
Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

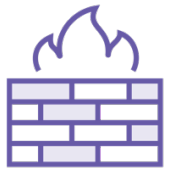
Suggested Prerequisite Courses

Getting Started with Software Development Using Cisco DevNet

Consuming Cisco APIs and Understanding Application DevOps



Managing Cisco Networks via Infrastructure as Code



Automating Cisco ASA and Firepower Policies Using APIs

Agenda

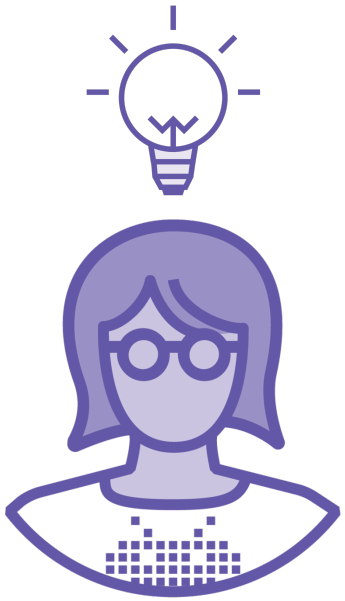
Introducing Globomantics

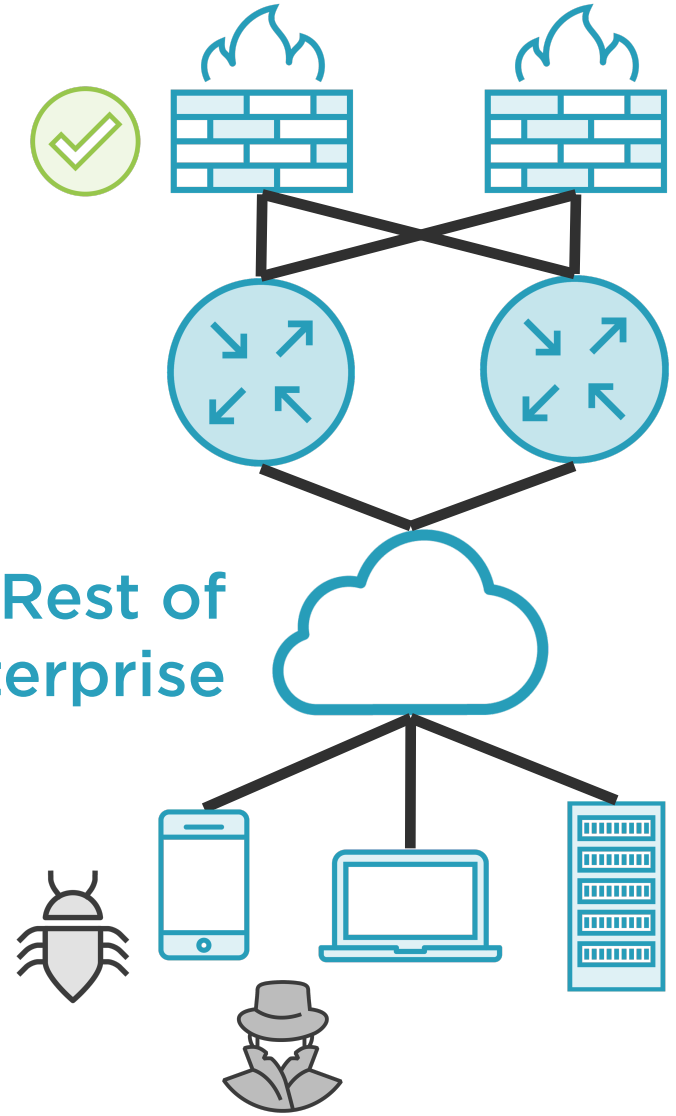
AMP architecture and deployments

Tons of demos:

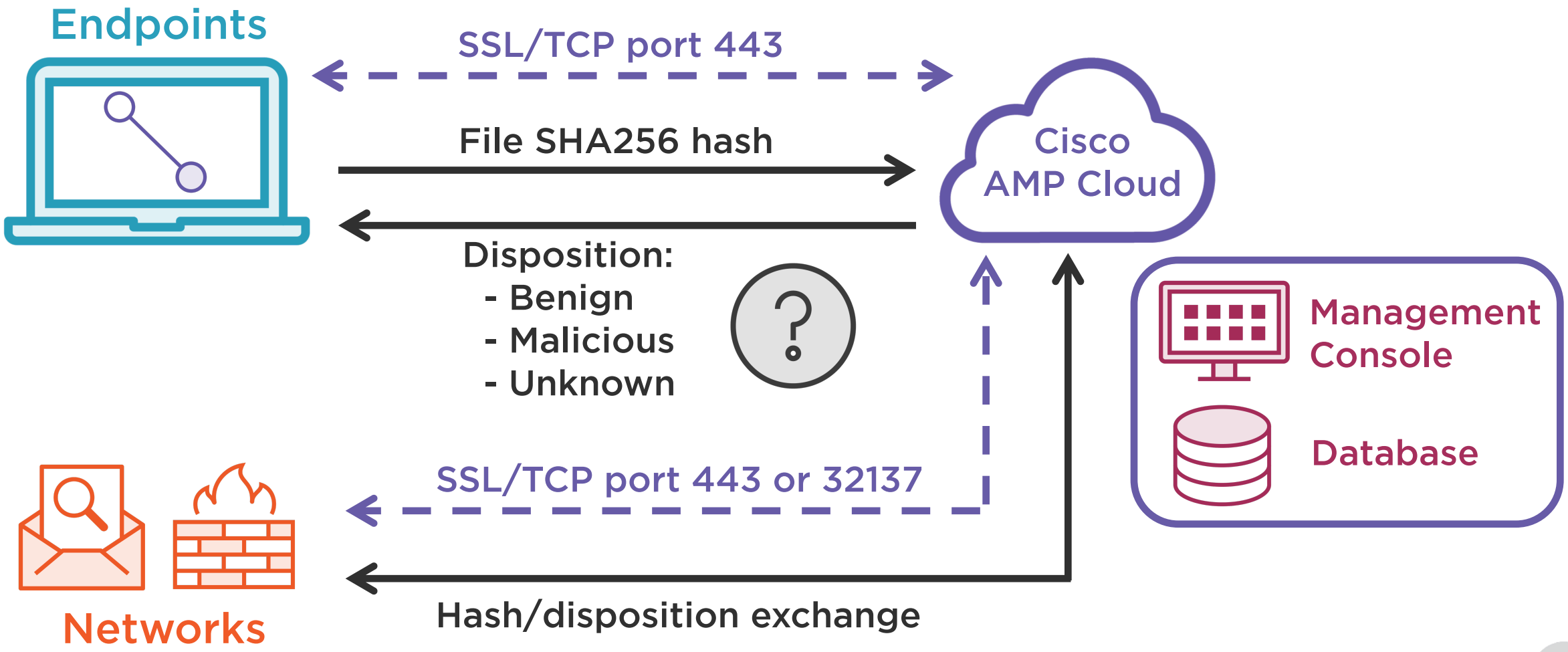
- Installation
- Developer resources
- Detecting malware
- Reconfiguring computers
- Blocking custom apps

Introducing Globomantics

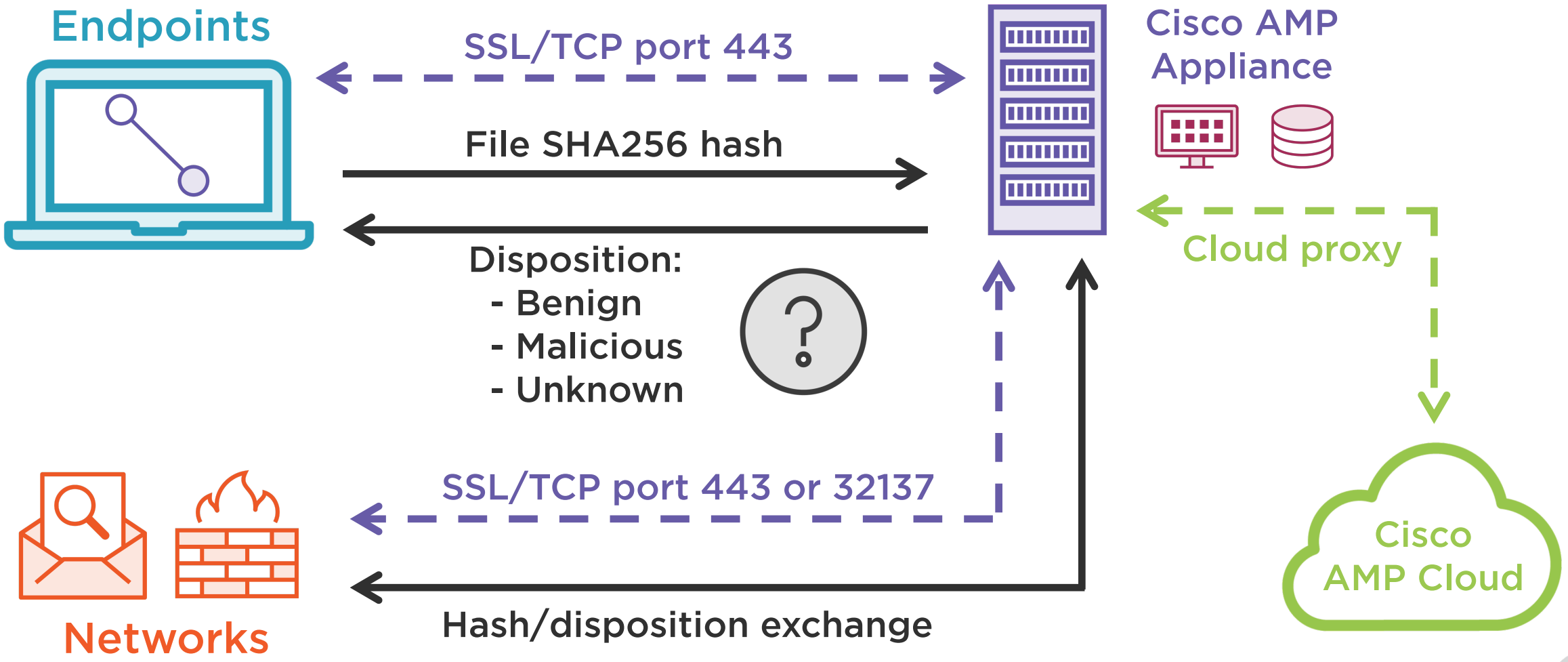




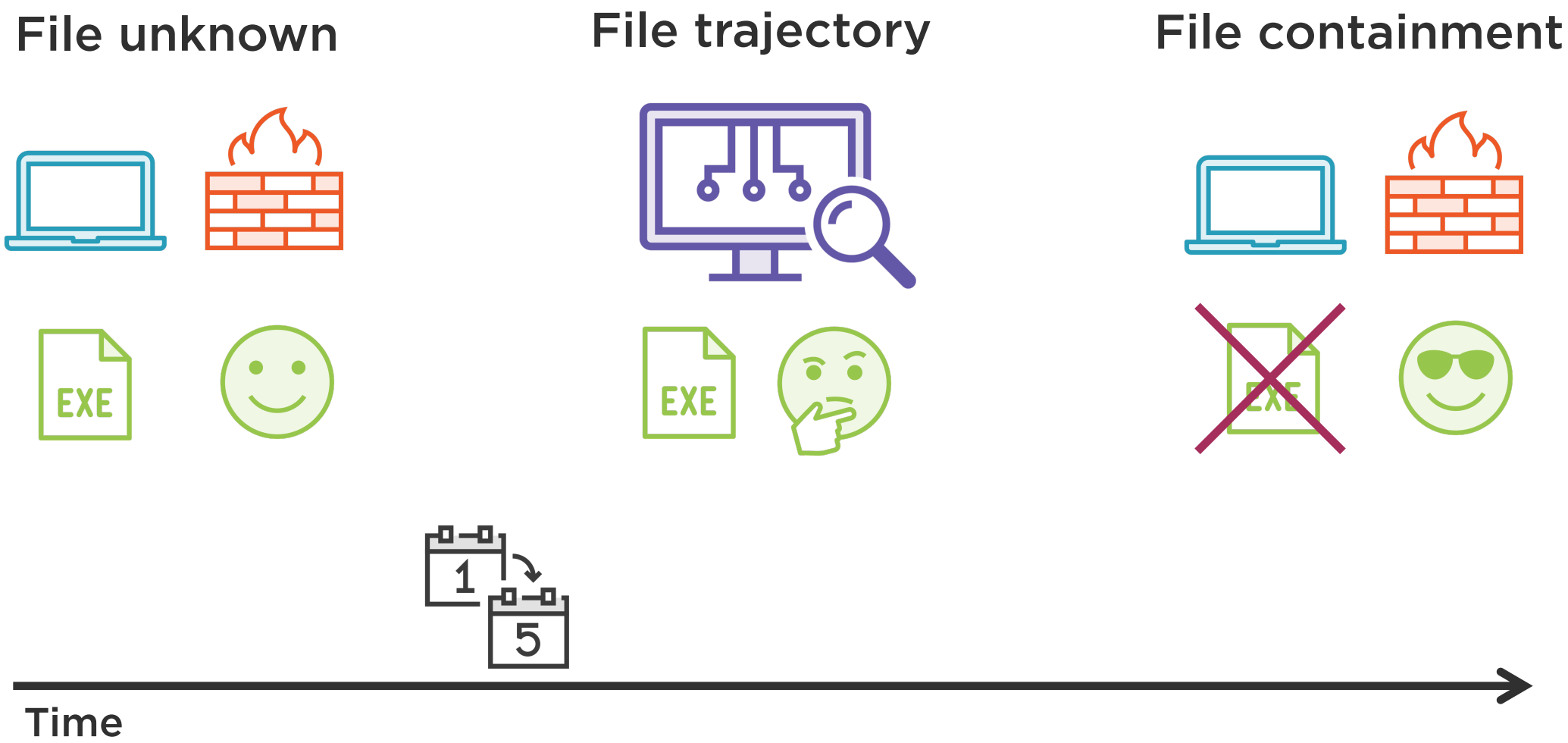
Cisco AMP in the Cloud



Cisco AMP in Private Deployments



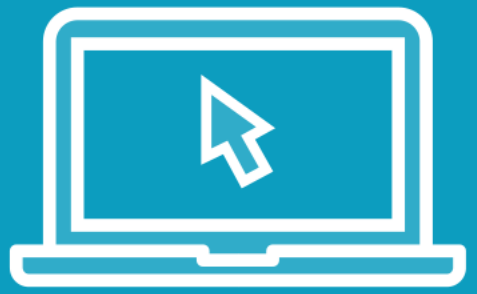
Cisco AMP Retrospection



Demo

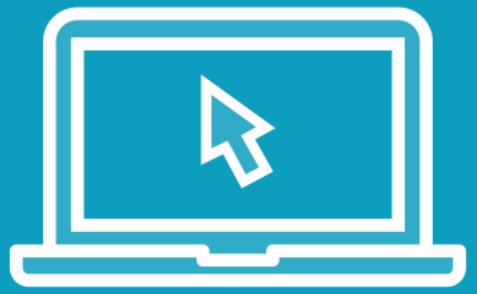
Initial AMP setup

Demo



AMP developer resources

Demo



A solid foundation: SDK framework

Demo

Detecting malware using AMP

Demo

Changing AMP computer groups

Demo

Blocking arbitrary apps from executing

Summary

Business problem and AMP architecture

Build, test, and validate solution

Challenge:

- Try testing a mobile device
- Try blocking another app