Your Time Is Now

Cisco Connect

Portorož, 15. in 16. marec 2017
How to securely connect user endpoints to network access wireless or wired

Gyorgy Acs
Consulting Systems Engineer
Cisco

Portorož, 15. in 16. marec 2017
• Introduction – Using ISE in a Security Ecosystem
• Anomaly, Vulnerability and Threat Detection in Action
  • Anomaly Detection with Profiling
  • Posture assessment with ISE 2.2
• Threat-Centric NAC
• Identity, application and Cisco Stealthwatch
• Rapid Threat Containment
Incident Response challenge

Contextual awareness key to security event prioritization and response

Potential Breach Event!

Associate User to Event

Associate User to Authorization

Check Endpoint Posture

Where is it on the Network?

What Kind of Device is it?

How Do I Mitigate?

Security Event

AAA Logs

IAM

NAC

???

???

???

???

MANY SCREENS
DATA EXPLOSION
MISSING LINKS
EXPENSIVE FIX
“Complexity is the enemy of security…

… a real platform is something that, somebody else can develop code for, somebody else can integrate with in a fundamental way....”

Marty Roesch @ RSA Conference 2016
Cisco Security VP

https://youtu.be/pafHZmWWGo8
Using ISE in a Security EcoSystem
Enable Unified Threat Response by Sharing Contextual Data

Cisco Platform Exchange Grid (PxGrid)

Who

What

When

Where

How

Posture

Threat

Vulnerability

Context

Cisco and Partner Ecosystem

Cisco Network

pxGrid Controller

ISE
pxGrid enables these 4 scenarios

<table>
<thead>
<tr>
<th>CONTEXT TO PARTNER</th>
<th>ENRICH ISE CONTEXT</th>
<th>THREAT MITIGATION</th>
<th>CONTEXT BROKERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco ISE</strong></td>
<td><strong>Enrich ISE context. Make ISE a better Policy Enforcement Platform</strong></td>
<td><strong>Enforce dynamic policies in to the network based on Partner's request</strong></td>
<td><strong>ISE brokers Customer's IT platforms to share data amongst themselves</strong></td>
</tr>
<tr>
<td><strong>ECO-PARTNER</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ISE makes Customer IT Platforms User/Identity, Device and Network Aware.
ISE nodes can publish specific topics or subscribe to specific topics.
### Capabilities or Topics

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GridControllerAdminService</td>
<td>Provides pxGrid services to subscriber</td>
</tr>
<tr>
<td>Core</td>
<td>Provides pxGrid client the capability to query all the registered capabilities on the ISE pxGrid node</td>
</tr>
<tr>
<td>AdaptiveNetworkControl</td>
<td>Provides enhanced pxGrid ANC mitigation capabilities to subscriber</td>
</tr>
<tr>
<td>EndpointProfileMetadata</td>
<td>Provides pxGrid clients with available device information from ISE.</td>
</tr>
<tr>
<td>EndpointProtectionService</td>
<td>Provides compatible EPS/ANC pxGrid mitigation actions from ISE 1.3/1.4.</td>
</tr>
<tr>
<td>TrustSecMetaData</td>
<td>Provides pxGrid clients with exposed security group tag (SGT) information</td>
</tr>
<tr>
<td>IdentityGroup</td>
<td>Provides pxGrid clients with Identity Group information that may not be available via 802.1X authentications</td>
</tr>
<tr>
<td>SessionDirectory</td>
<td>Provides pxGrid clients with ISE published session information, or available session objects.</td>
</tr>
</tbody>
</table>

https://communities.cisco.com/docs/DOC-68291
Agenda

• Introduction – Using ISE in a Security Ecosystem
• Anomaly, Vulnerability and Threat Detection in Action
  • Anomaly Detection with Profiling
• Posture assessment with ISE 2.2
• Threat-Centric NAC
• Identity, application and Cisco Stealthwatch
• Rapid Threat Containment
Anomaly Detection
ISE 2.2 Profiling Enhancements: Anomalous Behavior Detection

- Visibility Only and Dynamic Enforcement Options

---

Enable Anomalous Behavior including MAC Spoofing attempts

Enable option to dynamically change endpoint authorization and assign new policy based on Anomalous Detection flag
ISE 2.2 Profiling Enhancements : Anomalous Behavior Detection

- Anomalous Behavior/Spoofing Detection in ISE 2.2 (Phase 1)
- Offers Visibility-Only option as well Remediation option (flag endpoints for policy change)

Detection based on:
- Any change to DHCP Class
- Any changes to access method (wired / wireless)
- Significant Operating System change (for example, Windows -> Apple iOS)
- Significant profile change (for example, major change in classification such as Phone or Printer -> PC)
Agenda

- Introduction – Using ISE in a Security Ecosystem
- Anomaly, Vulnerability and Threat Detection in Action
- Anomaly Detection with Profiling
- Posture assessment with ISE 2.2
- Threat-Centric NAC
- Identity, application and Cisco Stealthwatch
- Rapid Threat Containment
Posture defines the state of compliance with the company's security policy

**Posture Flow**

- **AUTHENTICATE USER/DEVICE**
  Posture: Unknown / Non-Compliant?

- **QUARANTINE**
  Limited Access: VLAN / dACL / SGTs

- **POSTURE ASSESSMENT**
  Check Hotfix, AV, Pin lock, USB Device, etc.

- **REMEDIATION**
  WSUS, Launch App, Scripts, MDM, etc.

- **AUTHORIZATION CHANGE**
  Full Access – VLAN / dACL / SGTs.
## App Inventory from ISE 2.2

### Endpoints / 98:4B:4A:09:5A:28

**MAC Address:** 98:4B:4A:09:5A:28  
**Username:** Big_Boss  
**Endpoint Profile:** Mac Book Pro (Retina, 15-inch, 2.2 GHz Intel Core i7)  
**Current IP Address:** 1.1.2.1  
**Location:** San Jose, CA United States

### Application Details

<table>
<thead>
<tr>
<th>Application name</th>
<th>Version</th>
<th>Vendor</th>
<th>Running process ID</th>
<th>Process Name/Hash</th>
<th>Install Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco AnyConnect</td>
<td>98.55.98</td>
<td>Cisco</td>
<td>1338</td>
<td>VPNagent.exe</td>
<td>C:\program files\Cisco\cisco anyconnect\vpnagent.exe</td>
</tr>
<tr>
<td>Visual Studio 2005 professional edition</td>
<td>10.0.40219</td>
<td>Microsoft</td>
<td>5172</td>
<td>mspserv.exe</td>
<td></td>
</tr>
<tr>
<td>Winzip</td>
<td>12.1.8519</td>
<td>Winzip Computing</td>
<td>Not running</td>
<td>No traffic</td>
<td></td>
</tr>
<tr>
<td>Firefox</td>
<td>44.0.2</td>
<td>Mozilla</td>
<td>Not running</td>
<td>No traffic</td>
<td>C:\program files\Mozilla Firefox</td>
</tr>
</tbody>
</table>

### Running process file path

- **Process ID:** 17BE1824D29704D666E581A41F758953C141278C54F0FA1719319E1A709E457A

### Clear Threats & Vulnerabilities
If an Admin can create a requirement that if a malicious app is installed/running, then uninstall/terminate all processes of application A

The enforcement is at
- Initial posture
- PRA time
USB Checks are “Dynamic” a.k.a real time enforced, although USB check could be configured at initial posture check or Passive Reassessment checks (PRA).

- From AnyConnect 4.3 enforces the Disk Encryption Policy
- ISE 2.1 only supports it for Windows
Agenda

- Introduction – Using ISE in a Security Ecosystem
- Anomaly, Vulnerability and Threat Detection in Action
- Anomaly Detection with Profiling
- Posture assessment with ISE 2.2
- Threat-Centric NAC
- Identity, application and Cisco Stealthwatch
- Rapid Threat Containment
Threat Centric NAC explained

Reduce vulnerabilities, contain threats

Problem

1. Malware infection
2. Malware scans for vulnerable endpoints
3. Vulnerability detected
4. Infection spread

Compromised endpoints spread malware by exploiting known vulnerabilities in the network

Solution

IOC
CVSS

“Threat detected”
Quarantine and Remediate

Flag compromised and vulnerable hosts and limit access to remediation Segment

Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC) | Advanced Malware Protection (AMP)

Most endpoint AMP deployed in ‘visibility only’ mode
What is Threat Centric NAC?

Compliments Posture
Vulnerability data tells endpoint’s posture from the outside

Expanded control
driven by threat intelligence and vulnerability assessment data

Faster response
with automated, real-time policy updates based on vulnerability data and threat metrics

Create ISE authorization policies based on the threat and vulnerability attributes

- Vulnerability assessments
- Threat notifications

Cisco ISE

Endpoints

AMP

Qualys

ISE 2.2

Who

What

When

Where

How

Posture

Threat

Vulnerability

Compliments Posture
Vulnerability data tells endpoint’s posture from the outside

Expanded control
driven by threat intelligence and vulnerability assessment data

Faster response
with automated, real-time policy updates based on vulnerability data and threat metrics

Create ISE authorization policies based on the threat and vulnerability attributes

- Vulnerability assessments
- Threat notifications

Cisco ISE

Endpoints

AMP

Qualys

ISE 2.2

Who

What

When

Where

How

Posture

Threat

Vulnerability

Compliments Posture
Vulnerability data tells endpoint’s posture from the outside

Expanded control
driven by threat intelligence and vulnerability assessment data

Faster response
with automated, real-time policy updates based on vulnerability data and threat metrics

Create ISE authorization policies based on the threat and vulnerability attributes

- Vulnerability assessments
- Threat notifications

Cisco ISE

Endpoints

AMP

Qualys

ISE 2.2

Who

What

When

Where

How

Posture

Threat

Vulnerability
Vulnerability based access control
High-level flow

1. Endpoint connects to the network

2. CoA based on scan status (Full Access / Quarantine)

3. ISE requests a VA scan for Endpoint

4. Qualys scans the Endpoint for Vulnerabilities

5. Qualys reports the CVSS score

6. Initial limited Authorization (VA-Scan)
<table>
<thead>
<tr>
<th>QID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90043</td>
<td>SMB Signing Disabled or SMB Signing Not Required</td>
</tr>
<tr>
<td>95001</td>
<td>X-Window Sniffing</td>
</tr>
<tr>
<td>38170</td>
<td>SSL Certificate - Subject Common Name Does Not Match Server FQDN</td>
</tr>
<tr>
<td>38173</td>
<td>SSL Certificate - Signature Verification Failed Vulnerability</td>
</tr>
<tr>
<td>38601</td>
<td>SSL/TLS use of weak RC4 cipher</td>
</tr>
<tr>
<td>90882</td>
<td>Windows Remote Desktop Protocol Weak Encryption Method Allowed</td>
</tr>
</tbody>
</table>
Limited initial access

Scan for vulnerability every 48 hours.
Cisco ISE integrates with Cisco CTA cloud which offers TAXII services which includes threat incidents as payload in STIX standard

Communication
CTA adapter would interact with TC-NAC core-engine via REST APIs and the AMQP message queues

Faster response
with automated, real-time policy updates based on STIX data

- Threat notifications

CTA

Endpoints

Cisco ISE

Unknown
Insignificant
Distracting
Painful
Damaging
Catastrophic

Network Access Policy

STIX over TAXII | Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC)
Cognitive Threat Analytics: CTA

MALWARE DGA
100% confidence in 3 CONFIRMED

AFFECTING
wsa_s50065_6@wsa
10.62.67.69

 Client-IP: Server-IP: URL, SHA

<table>
<thead>
<tr>
<th>SERVER-IP</th>
<th>URL</th>
<th>REFERRER</th>
<th>USER-AGENT</th>
<th>BYTES-UP</th>
<th>BYTES-DOWN</th>
<th>HEADERS</th>
<th>HTTP-S</th>
<th>TIMESTAMP</th>
<th>DURATION</th>
<th>FILENAME</th>
<th>CATEGORY</th>
<th>SHA-256</th>
<th>ANY-CONNECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>216.172.59.243</td>
<td><a href="http://malware.info/bestweblinks.com/result/">http://malware.info/bestweblinks.com/result/</a>?...</td>
<td>Mozilla5.0 (Wi)</td>
<td>605</td>
<td>320</td>
<td>203 = OK</td>
<td>Feb 26, 2016 17:19:57</td>
<td></td>
<td>320 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.172.59.243</td>
<td><a href="http://malware.info/bestweblinks.com/result/">http://malware.info/bestweblinks.com/result/</a>?...</td>
<td>Mozilla5.0 (Wi)</td>
<td>605</td>
<td>320</td>
<td>203 = OK</td>
<td>Feb 26, 2016 17:17:21</td>
<td></td>
<td>402 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.172.59.243</td>
<td><a href="http://malware.info/bestweblinks.com/result/">http://malware.info/bestweblinks.com/result/</a>?...</td>
<td>Mozilla5.0 (Wi)</td>
<td>579</td>
<td>320</td>
<td>203 = OK</td>
<td>Feb 26, 2016 17:23:16</td>
<td></td>
<td>395 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.172.59.243</td>
<td><a href="http://malware.info/bestweblinks.com/result/">http://malware.info/bestweblinks.com/result/</a>?...</td>
<td>Mozilla5.0 (Wi)</td>
<td>579</td>
<td>320</td>
<td>203 = OK</td>
<td>Feb 26, 2016 17:26:51</td>
<td></td>
<td>323 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.172.59.243</td>
<td><a href="http://malware.info/bestweblinks.com/result/">http://malware.info/bestweblinks.com/result/</a>?...</td>
<td>Mozilla5.0 (Wi)</td>
<td>579</td>
<td>320</td>
<td>203 = OK</td>
<td>Feb 26, 2016 17:40:06</td>
<td></td>
<td>317 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Traffic: 5.3 MiB up / 8.8 MiB down. Requests: 11967. Duration: 38 days 14 hours 2 minutes 23 seconds. User Agents: 4. No Referrer: 0%. HTTP: 403, 506, 200, 504

Find IP in AMP for Endpoints
What is STIX?

STIX (Structured Threat Information eXpression) is a standardized XML programming language for conveying data about Cyber Security threats in a common language that can be easily understood by humans and security technologies.

**Indicators:** Describe patterns for what might be seen and what they mean if they are.

**Incidents:** Describe instances of specific adversary actions.

**Courses of Action:** Describe response actions that may be taken in response to an attack or as a preventative measure.

**Source:** https://stixproject.github.io/about/
"192.168.10.10": {
  "vendor": "CTA",
  "incident": {
    "Course_Of_Action": "Internal Blocking",
    "Impact_Qualification": "Catastrophic",
    "Confidence": "High"
  },
  "title": "Microsoft Outlook attack",
  "time-stamp": "1473985383762"
}
Pretty identical configuration for most deployments
**Authorization Policy**

- **Authorization policy for ‘vulnerability’**

  - **Initial ‘limited access’ + Vulnerability Scan**

---

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Conditions (Identity groups and other conditions)</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Wireless Black List Default</td>
<td>if Blacklist AND Wireless_Access</td>
<td>then Blackhole_Wireless_Access</td>
</tr>
<tr>
<td></td>
<td>Profiled Cisco IP Phones</td>
<td>if Cisco_IP_Phone</td>
<td>then Cisco_IP_Phone</td>
</tr>
<tr>
<td></td>
<td>Profiled Non Cisco IP Phones</td>
<td>if Non_Cisco_Profiled_Phone</td>
<td>then Non_Cisco_IP_Phone</td>
</tr>
<tr>
<td></td>
<td>Basic_Authenticated_Access</td>
<td>if Network_Access_Authentication_Passed</td>
<td>then VA_Access_Scan</td>
</tr>
<tr>
<td></td>
<td>Default</td>
<td>if no matches, then DenyAccess</td>
<td></td>
</tr>
</tbody>
</table>

---

**Cisco Connect**  
Portorož, Slovenija  
15. – 16. marec 2017
TC-NAC service on ISE

Threat Centric NAC attributes appear in the Policy Administration Node.

TC-NAC service runs in the ‘Policy Services Node’ when enabled.
‘Compromised Endpoints’ based on Incidents and Indicators
Agenda

- Introduction – Using ISE in a Security Ecosystem
- Anomaly, Vulnerability and Threat Detection in Action
- Anomaly Detection with Profiling
- Posture assessment with ISE 2.2
- Threat-Centric NAC
- Identity, application and Cisco Stealthwatch
- Rapid Threat Containment
The Cyber Killchain

1. Reconnaissance
   Harvest information to create attack strategy and toolset

2. Weaponization
   Coupling exploit with backdoor into deliverable payload

3. Delivery
   Delivering weaponized bundle to the victim via email, web, USB, etc.

4. Exploitation
   Exploiting a vulnerability to execute code on victim’s system

5. Installation
   Installing malware on the asset

6. Command & Control
   Command channel for remote manipulation of victim’s system

7. Actions on Objectives
   With ‘Hands on Keyboard’ access, intruders accomplish
Cisco StealthWatch: System Overview

**Cisco Connect**

Network Devices

- Collect and analyze
- Up to 4,000 sources
- Up to 240,000 FPS sustained

StealthWatch FlowSensor

- Generate NetFlow

Non-NetFlow Capable Device

SPAN

StealthWatch FlowCollector

- Collect and analyze
- Up to 4,000 sources
- Up to 240,000 FPS sustained

StealthWatch Management Console (SMC)

- Management and reporting
- Up to 25 FlowCollectors
- Up 6 million FPS globally

NetFlow / NBAR / NSEL

- Collect and analyze
- Up to 4,000 sources
- Up to 240,000 FPS sustained

- Management and reporting
- Up to 25 FlowCollectors
- Up 6 million FPS globally

15. – 16. marec 2017 | Cisco Connect | Portorož, Slovenija
There are 11 high level alarm categories; mapping to the kill chain or the attack lifecycle.

Each category accrues points.
Traffic Analysis without Identity

Who is Sender?
Shows an IP Address
- Yes, Useful, But...

<table>
<thead>
<tr>
<th>DURATION</th>
<th>SUBJECT</th>
<th>PORT/PROTOCOL</th>
<th>TRAFFIC SUMMARY</th>
<th>PORT/PROTOCOL</th>
<th>PEER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start: 01/10 - 10:32:41 AM&lt;br&gt;End: 01/10 - 10:34:59 AM&lt;br&gt;Duration: 2m 18s</td>
<td><img src="10.201.3.149" alt="IP Address" /> View URL Data</td>
<td>50654/UDP</td>
<td>106.93KB</td>
<td>311 packets</td>
<td>443/UDP</td>
</tr>
<tr>
<td><img src="10.201.3.149" alt="RFC 1918" /> View URL Data</td>
<td>443/UDP</td>
<td>Undefined UDP</td>
<td>United States</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Search Subject Details

- Packets: 311
- Packet Rate: 2.25pps
- Bytes: 106.93KB
- Byte Rate: 793.47bps
- Percent Transfer: 52.65%
- Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing

<table>
<thead>
<tr>
<th>Totals</th>
<th>Peer Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets: 830&lt;br&gt;Packet Rate: 6.01pps&lt;br&gt;Bytes: 203.09KB&lt;br&gt;Byte Rate: 1.51Kbps&lt;br&gt;Subject Byte Ratio: 52.65%&lt;br&gt;RTT: --&lt;br&gt;SRT: --</td>
<td>Packets: 519&lt;br&gt;Packet Rate: 3.76pps&lt;br&gt;Bytes: 96.16KB&lt;br&gt;Byte Rate: 713.51bps&lt;br&gt;Percent Transfer: 47.35%&lt;br&gt;Host Groups: United States</td>
</tr>
</tbody>
</table>
### Traffic Analysis with Identity

**Who is Sender?**

- Employee1
  - More Useful, right?

#### Search Subject Details

<table>
<thead>
<tr>
<th>Duration</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start: 01/11 - 03:43:22 PM</td>
<td>10.1.41.104</td>
</tr>
<tr>
<td>Duration: 8s</td>
<td></td>
</tr>
</tbody>
</table>

#### Port/Protocol

<table>
<thead>
<tr>
<th>Subject</th>
<th>Port/Protocol</th>
<th>Traffic Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.100.103</td>
<td>88/TCP</td>
<td>7.67KB</td>
</tr>
<tr>
<td>win10-desktop.securitydemo.net</td>
<td>50629/TCP</td>
<td>5.48KB</td>
</tr>
</tbody>
</table>

#### Totals

<table>
<thead>
<tr>
<th></th>
<th>Packets: 60</th>
<th>Packet Rate: 7.5pps--</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bytes: 13.36KB</td>
<td>Byte Rate: 1.01Kbps</td>
</tr>
<tr>
<td></td>
<td>Percent Transfer: 58.94%--</td>
<td></td>
</tr>
</tbody>
</table>

#### Peer Details

<table>
<thead>
<tr>
<th></th>
<th>Packets:</th>
<th>Packet Rate: 3.75pps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bytes: 7.87KB</td>
<td>Byte Rate: 1.71Kbps</td>
</tr>
<tr>
<td></td>
<td>Percent Transfer: 41.06%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Host Groups:</td>
<td>Host Groups: Catch All</td>
</tr>
</tbody>
</table>
HTTPS Unclassified now Known

- AnyConnect NVM with Cisco Stealthwatch

- Application Identified – Dropbox
- Application Hash – Who else is running?
- Identity – nedzaldivar (even without ISE or Identity, from non domain asset)
RTC w/ Stealthwatch & ISE

1. SW is Analyzing Flows from Flow Collector

2. SW is Also Merging Identity Data from ISE

3. Admin is Alerted of Suspicious Behavior
4. Admin Initiates Endpoint Quarantine (EPS over pxGrid)

5. Endpoint Assigned Quarantine + CoA-Reauth Sent
RTC w/ Stealthwatch & ISE

6. New Traffic Rules apply to the new state of the endpoint

6a. Could Deny Access (ingress)

6b. Could Filter it within network (egress)
Give The Right People On The Right Devices The Right Access To The Right Resources (TrustSec)

Implement Granular Control on Traffic, Users, and Assets

Enforce Business Role policies for All Network Services and Decisions

Define Security Groups and Access Policies Based on Business Roles

Who: Doctor
What: Laptop
Where: Office

Who: Receptionist
What: iPad
Where: Office

Who: Guest
What: iPad
Where: Office

Confidential Patient Records

Internal Employee Intranet

Internet
Multiple TrustSec & DEFCON Matrices

Multiple levels of "failsafe" policy sets

Stops Lateral Movement
Agenda

• Introduction – Using ISE in a Security Ecosystem
• Anomaly, Vulnerability and Threat Detection in Action
• Anomaly Detection with Profiling
• Posture assessment with ISE 2.2
• Threat-Centric NAC
• Identity, application and Cisco Stealthwatch
• Rapid Threat Containment
Rapid Threat Containment

- FMC 6.1 and pxGrid / Fire+ISE is supported in as an integrated solution
- No more pxGrid connection agent / external remediation module is needed
- Session information obtained from ISE via pxGrid
- SGTs can be used in FMC 6.1 access control policies
- ISE remediation capabilities:
  - Quarantine, Un-quarantine (VLAN, dACL, SGT), port shutdown
- Quarantine actions triggered per policy with FMC and ISE
- Infected users can be notified and re-directed to portal for remediation
pxGrid Clients authenticate and subscribe to the Grid

- Authenticates to ISE pxGrid node using self-signed or CA-signed certificates
- Subscribe or direct queries
- Communicate TCP/5222 to ISE pxGrid node
Remediation Modules:

- Cisco RTC
- Guidance Encase
- Set Host Attributes
- Security Intelligence Blacklisting
- Nmap Scan
- SSH / Expect Scripts
- F5 iRules
- Solera DeepSee
- Netscaler
- PacketFence
- Bradford
Remediation Options

- **Quarantine**: quarantines an endpoint based on source IP address
- **portBounce**: temporarily bounces the endpoint or host port
- **Terminate**: terminates the end-user session
- **Shutdown**: initiates a host port shutdown, this will insert a “shutdown” command on the switch port configuration
- **reAuthenticate**: reAuthenticates the end-user
- **UnQuarantine**: unquarantines the endpoint
### Quarantine Service with Authorization Policy

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.

For Policy Export go to **Administration > System > Backup & Restore > Policy Export Page**

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Description</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VPN</td>
<td>Policy for VPN Users</td>
<td>DEVICE:Device Type EQUALS Device Type#All Device Types#Firewalls</td>
</tr>
</tbody>
</table>

#### Authentication Policy

- Default Rule (If no match) : Allow Protocols : PAP_ONLY and use : AD1

#### Authorization Policy

**Exceptions (0)**

**Standard**

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Conditions (identity groups and other conditions)</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ITadms Quarantine</td>
<td>if (AD1:ExternalGroups EQUALS dclouid.cisco.com/Builtin/ITAdmins AND Session.EPSStatus EQUALS Quarantine )</td>
<td>then APITadms_Quarantine AND ITadms</td>
</tr>
<tr>
<td></td>
<td>ITadms</td>
<td>if AD1:ExternalGroups EQUALS dclouid.cisco.com/Builtin/ITAdmins</td>
<td>then APITadms AND ITadms</td>
</tr>
</tbody>
</table>
Rapid Threat Containment with Firepower Management Center and ISE

1. Security Events / IOCs Reported

2. Correlation Rules Trigger Remediation Action

3. pxGrid EPS Action: Quarantine + Re-Auth

pxGrid controller
4. Endpoint Assigned Quarantine + CoA-Reauth Sent
Information Sharing:

- pxGrid to Cisco only
- RADIUS for CDA compatibility
- No NAD communication
Almost Anything
Agenda

• Introduction – Using ISE in a Security Ecosystem
• Anomaly, Vulnerability and Threat Detection in Action
  • Anomaly Detection with Profiling
  • Posture assessment with ISE 2.2
• Threat-Centric NAC
• Identity, application and Cisco Stealthwatch
• Rapid Threat Containment
ISE Resources

http://cs.co/ise-design

Design guides focusing on ISE

- Deployment Strategy
- ISE Configuration
- Network Access Device Configuration
- Guest and Web Authentication
- Mobile Device Management (MDM)
- Cisco pxGrid
- Third-Party Integration
- etc.

http://cs.co/ise-community

Cisco Identity Services Engine Software

- Configure HTTPS Support for ISE SCEP Integration 31/Jul/2013
- ISE Guest Accounts for RADIUS/802.1x Authentication Configuration Example 15/Jan/2013
- Network Admission Control (NAC) Agent Discovery Process for Identity Services Engine (ISE) 15/Jan/2013
- ISE Version 1.3 Hotspot Configuration Example 11/Feb/2015
- Install a 3rd party CA certificate in ISE 2.0 15/Dec/2015
- Location based authorization with Mobility Services Engine (MSE) and Identity Services Engine (ISE) ISE 2.0 05/Sep/2015
Thank you!