Cisco Threat Response

Unleash the full power of your security architecture

Cisco Knowledge Network Webinar Series
April 10, 2019
Today’s Presenters

John Malzahn
Senior Manager,
Service Provider
Solutions Marketing
Cisco Systems

Dale Long
Consulting Security
Engineer, Advanced
Threat Solutions
Cisco Systems
Attending CiscoLive This June?
Come See Us

Cisco Live San Diego
• June 9–13
• Cisco Service Provider Booth Located in World of Solutions Hall
A CIO just asked me about a new banking Trojan... I had no answer...

“I need to know now... are we impacted?”
Typical Investigation Steps

- Search security blogs for latest threat information
- Find indicators of compromise (IoCs) to search
- Search security operations systems looking for activity associated with IoCs
- Verify existing threats are blocked
- Investigate related activity to trace the threat
- Investigate and block any new threats related to the activity
Security must work together
But too often it doesn’t...

Security Operations

How?
Is it bad?

Why?
Has it affected us?

Technologies and Intelligence

- Threat Intel
- Endpoint Security
- SIEM
- Next-Gen IPS
- Malware Detection
- Secure Internet Gateway
- Email Security
- Web Security
- Third party Sources
- Network Analytics
- Next-Gen Firewall
- Identity Management

© 2018 Cisco and/or its affiliates. All rights reserved.
### Cisco Security Portfolio

Over $7 billion invested in industry-leading security solutions

<table>
<thead>
<tr>
<th>Network</th>
<th>User/Endpoint</th>
<th>Cloud</th>
<th>Customer SOC</th>
<th>Cisco Threat Intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-Perimeter</td>
<td>SD-Perimeter</td>
<td>SIG / CASB Workload Protection</td>
<td>Incident Response</td>
<td>Incident Investigations</td>
</tr>
<tr>
<td>NGFW UTM Web Security</td>
<td>MFA / SSO BYOD SD-Perimeter Email Security</td>
<td>Security Analytics</td>
<td>Internet Investigations</td>
<td>File Investigations</td>
</tr>
<tr>
<td>Security Analytics NGIPS</td>
<td>EPP / EDR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Trusted Access**  **Threat Defense**

© 2018 Cisco and/or its affiliates. All rights reserved.
Customers want more integration and automation

Difficult

- Attack detection across multiple technologies from different vendors
- SIEM integration
- Manual correlation of threat intelligence with context information
- Coordination and collaboration among several responders
- Remediation through multiple, inconsistent consoles

Time-Consuming

Manual
Introducing Cisco Threat Response
Unleashing the power of the Cisco Integrated Security Architecture

Key pillar of our integrated security architecture

- Automates integrations across Cisco security products
- Reduces the time and effort spent on key security operations functions:
  - Detection
  - Investigation
  - Remediation
- Included as part of Cisco Security product licenses
Cisco Threat Response reduces complexity across the growing Incident Response toolset

- Marries external threat intelligence to internal log data
- Combines data from multiple Cisco and 3rd party sources
- Single location for most common IR tasks across multiple tools
- Use cases before, during, and after an attack
- Reduces investigation, triage and mitigation time
Cisco Threat Response in your SOC
Complements your existing investments and supports your IR team

Multiple Cisco Products and Intel/Identity Context

Other Existing Products and Intel/Identity Context

Cisco Threat Response

- Detect
- Investigate
- Remediate

Existing SIEM

Stand-alone SOAR (optional)

IR Team

SOC
Cisco Threat Response in action
Three simple ways to get started

1. Intelligence Sources
2. Casebook via Browser Plug-In
3. High-Fidelity Events

Observables:
- File hash
- IP address
- Domain
- URL
- More...

- AMP for Endpoints
- Umbrella
- Email Security
- NGFW/NGIPS

Investigate (search interface)
Incident Manager

Cisco Talos
Threat Grid
Virus Total

- Have we seen these observables? Where?
- Which endpoints connected to the domain/URL?
- Are these observables suspicious or malicious?
Using Cisco Threat Response
I am a Cisco Security customer using Cisco Threat Response

My team can:

- Answer questions faster about observables.
- Block and unblock domains from Cisco Threat Response.
- Block and unblock file executions from Cisco Threat Response.
- Hunt for an observable associated with a known actor and immediately see organizational impact.
- Save a point in time snapshot of our investigations for further analysis.
- Document our analysis in a cloud casebook from all integrated or web-accessible tools, via an API.
- Integrate Cisco Threat Response easily into existing processes and custom tools.
My team can hunt for an observable associated with a known actor and see organizational impact

- Targets affected
- Additional IPs connected
- Programs associated
My team can answer questions faster about observables

- Learn more about observables with Unknown dispositions
- See how they affect my organization
- Get the details of programs executing
My team can block and unblock domains from Cisco Threat Response

• Execute a block directly from Cisco Threat Response
• Block is effected in Cisco Umbrella
• API integration to block and unblock
My team can block and unblock file executions from Cisco Threat Response

- Execute block from Cisco Threat Response
- Block is effected in Cisco AMP for Endpoints
  - And, via AMP Unity feature: NGFW, WSA, ESA, etc
- API integration to block and unblock
My team can save a point in time snapshot of our investigations for further analysis

- Point in time
- Reference
- Launch point for subsequent investigations
My team can document our analysis

Casebooks

- Available across multiple products
  - Officially integrated products
  - Non-integrated but web accessible products via Browser extension

- Notes and observables for workflow continuity

- Immediate access to
  - Verdicts
  - Response actions
Cisco Threat Response in the real world
Join Cisco Security customers who are gaining value from it now

4100+
Organizations are using it today

“I like quickly being able to see infections on my network, and this presents them in a really nice fashion…”

“You cannot hit a target you cannot see. Cisco Threat Response really simplifies security analysis…”
Cisco Threat Response for everyone
Scales with the changing needs of your organization

Commercial Organizations
and State and Local Governments
• Small security team
• Limited SIEM deployment
• Leverage full stack with API

Large Enterprises
and Large Government Agencies
• Security Operations Center
• Extensive SIEM deployment
• APIs across the stack is key

Managed Security Service Providers
• Security Operations Center
• Multi-tenant SIEM deployment
• APIs across the stack is key
Cisco Threat Response is included
...with select Cisco Security product licenses

You’re already entitled to Threat Response if you have...

- Cisco AMP for Endpoints
- Cisco Threat Grid
- Cisco Umbrella
- Cisco Email Security
- Cisco NGFW/NGIPS

Not a customer yet?
Request your free trial of Cisco AMP for Endpoints... and try both solutions right now!

www.cisco.com/go/amp
Digital Resources
Cisco Threat Response

CS.co/threat_response

Security that works together
Cisco Threat Response.

How threat response is enabled in the cloud

SalesConnect

• BDM
• TDM
• Whitepaper
• + other resources

Demo on dCloud

• Log into dCloud and search for “Cisco Threat Response”
• Click on “Cisco Threat Response v1 - Instant Demo” You will see 3 other Threat Response related demos that allow you to conduct an integrated demo with AMP/TG/Umbrella
• Download and follow the demo guide (under the “Related Documents” link).

Threat Hunting Workshops

• 161+ global workshops
• 411+ participants
• See upcoming workshops here

YouTube Series

Overview
The power of Cisco Threat Response
Ben Greenbaum

Cisco Threat Response demo and walkthrough
Ben Greenbaum

A quick tour of the Relations Graph in Cisco Threat Response
Ben Greenbaum

Configuration
How to Enable Cisco Threat Response
Ben Greenbaum

HOWTO Series
Cisco Security HOWTO: Threat Hunting: PowrLiks Part 1
Jesse Munoz
For more information

Visit
www.cisco.com/ctr
www.cisco.com/go/mssp

or contact your Cisco account representatives
Questions?
Cisco Threat Response

Learn more about Cisco Threat Response at cisco.com/go/threatresponse

Security That Works Together