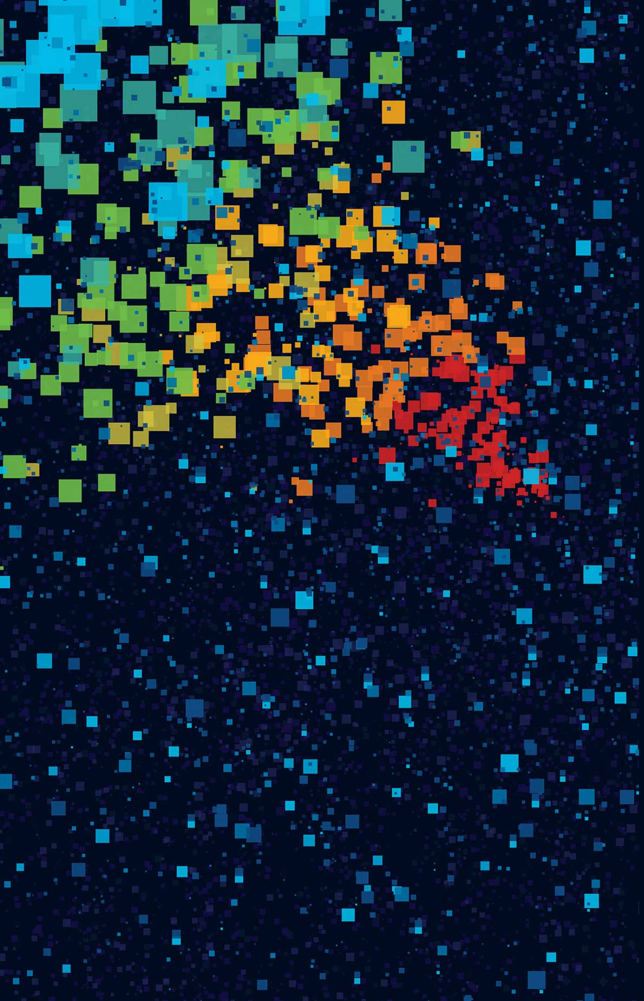
Possibilities

#CiscoLive

Threat Hunting

Do or Do Not, There is No Try

Adam G. Tomeo – Product Marketing Manager
Cisco AMP for Endpoints
DGTL-PSOSEC-1003



Agenda

- Why organizations struggle to adopt
- What is threat hunting
- Why is it necessary
- What are the outcomes
- Cisco AMP for Endpoints
- Next steps
- Questions

Why organizations struggle to adopt

Why organizations struggle to adopt

No dedicated hunting staff	Needs to be integrated with Cisco and other products	Needs to fit into current workflows
Needs to be automated	Needs to be quick and easy	Existing infrastructure limitations
Needs to aggregate information and enrich data	Needs to scale	Lack of public threat hunting methodologies and threat intelligence

Most of all it needs to

Be simple

Save time

Add value instantly

Today's security teams are challenged

1. Time
2. Abilities and headcount
3. Tool Integration
   1. Workflows
   2. Aggregation of information
   3. Orchestration
4. Alert fatigue

Threat Hunting needs

- Automation
- Integrated platform solution
- Noise reduction – high fidelity alerts
- Keep team size fixed and not require additional operating expenses

- Simplification
- Time Savings
- Shortened time to value
- Connect with other tools both Cisco and 3rd party

Threat Hunting

What is threat hunting?

- Analyst centric process to uncover hidden, advanced threats missed by automation
- Proactive approach to detection
- Output feeds into incident response process or provides input for new detection methods
- Tells a narrative

Types of Threat Hunts

Atomic indicators

- Intelligence driven

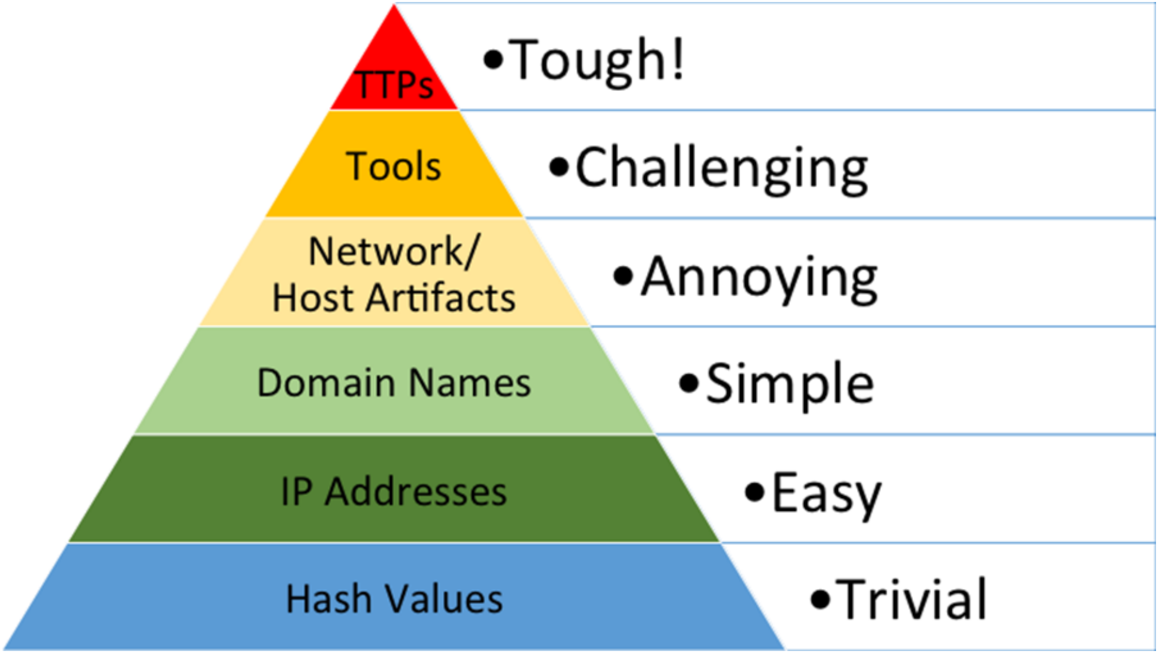
Behavior and compound indicators

- Tactic and technique driven

Generic Behaviors

- Anomaly driven

“Pyramid of Pain



TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial

Credit: David J Bianco

Why is it necessary

Why is it necessary?

Improve insight into visibility and coverage

Minimize attack surface exposure

Create more robust detections

Generate more accurate detections

Reduce time to containment

Decrease resources

What are the outcomes

What are the outcomes?

- Discovering and thwarting an attack before it causes damage
- Increased knowledge of vulnerabilities and risks which allows a hardening of the security environment
- Fewer breaches and breach attempts
- Reduced attack surface
- Increased speed and accuracy of threat responses
- Measurable improvements to MTTD and MTTR

Cisco AMP for Endpoints

Cisco AMP for Endpoints

Component of the SecureX platform

- Experience simplified
- Success accelerated
- Future protected

Integrated with the entire Cisco security platform

- Visibility into what has been done
- Integration to reduce complexity
- Orchestration and Automation

Three different product levels available

- Essentials
- Advantage
- Premier

Cisco AMP for Endpoints - Essentials

Next Gen Antivirus Protection

Continuous Behavioral Monitoring

Dynamic File Analysis

Vulnerability Identification

Endpoint Isolation

Cisco AMP for Endpoints - Advantage

Next Gen Antivirus Protection

Continuous Behavioral Monitoring

Dynamic File Analysis

Vulnerability Identification

Endpoint Isolation

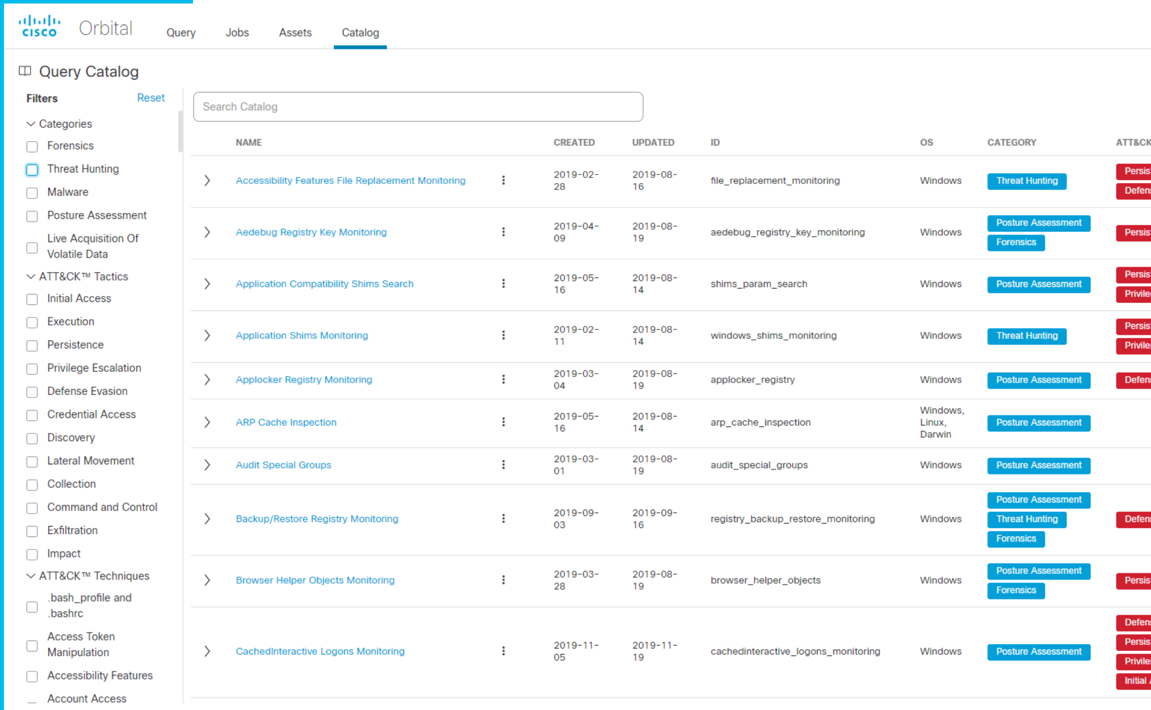
Orbital Advanced Search

Threat Grid Cloud

Cisco AMP for Endpoints – Advantage

Orbital Advanced Search

- Addresses challenges
- Business value gained
- How does it work?
  - Forensics snapshots
  - Live search
  - Predefined and customizable queries
  - Storage options
- Common use cases



Query Catalog

Filters Reset

Categories
- ☐ Forensics
- ☐ Threat Hunting
- ☐ Malware
- ☐ Posture Assessment
- ☐ Live Acquisition Of Volatile Data

ATT&CK™ Tactics
- ☐ Initial Access
- ☐ Execution
- ☐ Persistence
- ☐ Privilege Escalation
- ☐ Defense Evasion
- ☐ Credential Access
- ☐ Discovery
- ☐ Lateral Movement
- ☐ Collection
- ☐ Command and Control
- ☐ Exfiltration
- ☐ Impact

ATT&CK™ Techniques
- ☐ .bash_profile and .bashrc
- ☐ Access Token Manipulation
- ☐ Accessibility Features
- ☐ Account Access

Search Catalog

NAME	CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK
Accessibility Features File Replacement Monitoring	2019-02-28	2019-08-16	file_replacement_monitoring	Windows	Threat Hunting	Persis Defen
Aedebug Registry Key Monitoring	2019-04-09	2019-08-19	aedebug_registry_key_monitoring	Windows	Posture Assessment Forensics	Persis
Application Compatibility Shims Search	2019-05-16	2019-08-14	shims_param_search	Windows	Posture Assessment	Persis Privile
Application Shims Monitoring	2019-02-11	2019-08-14	windows_shims_monitoring	Windows	Threat Hunting	Persis Privile
Applocker Registry Monitoring	2019-03-04	2019-08-19	applocker_registry	Windows	Posture Assessment	Defen
ARP Cache Inspection	2019-05-16	2019-08-14	arp_cache_inspection	Windows, Linux, Darwin	Posture Assessment	
Audit Special Groups	2019-03-01	2019-08-19	audit_special_groups	Windows	Posture Assessment	
Backup/Restore Registry Monitoring	2019-09-03	2019-09-16	registry_backup_restore_monitoring	Windows	Posture Assessment Threat Hunting Forensics	Defen
Browser Helper Objects Monitoring	2019-03-28	2019-08-19	browser_helper_objects	Windows	Posture Assessment Forensics	Persis
CachedInteractive Logons Monitoring	2019-11-05	2019-11-19	cachedinteractive_logons_monitoring	Windows	Posture Assessment	Defen Persis Privile Initial

Cisco AMP for Endpoints - Premier

Next Gen Antivirus Protection

Continuous Behavioral Monitoring

Dynamic File Analysis

Vulnerability Identification

Endpoint Isolation

Orbital Advanced Search

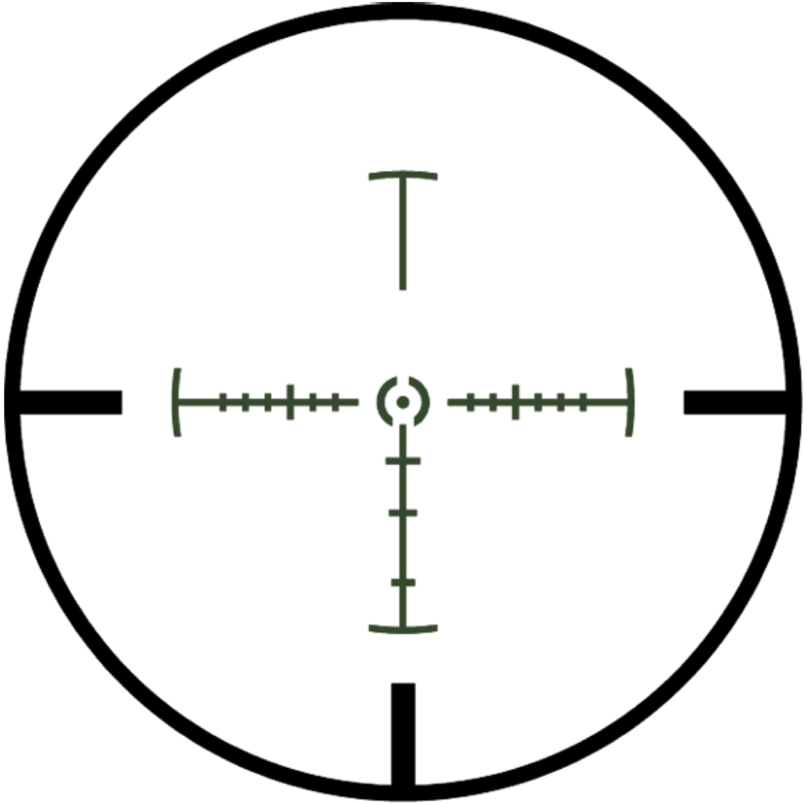
Threat Grid Cloud

Threat Hunting

Cisco AMP for Endpoints – Premier

Threat Hunting

- Uncovering hidden threats faster across the attack surface using MITRE ATT&CK™ and other industry best practices
- Performing human-driven hunts based on playbooks producing high fidelity alerts
- Continually developing systematic playbooks, executing on broad, low-level telemetry on product backend



Next Steps

Next steps

- Sign up for free product trials
  https://www.cisco.com/c/en/us/products/security/event-free-trials.html
- Attend a virtual Threat Hunting Workshop
  https://www.cisco.com/c/en/us/products/security/threat-hunting-workshop.html
- Register for virtual Cisco Security Insights Summit – June 17
  URL
- Register for your copy of the “Tame the Beast” report
  https://www.cisco.com/go/tamethebeast

Thank you

Possibilities

#CiscoLive