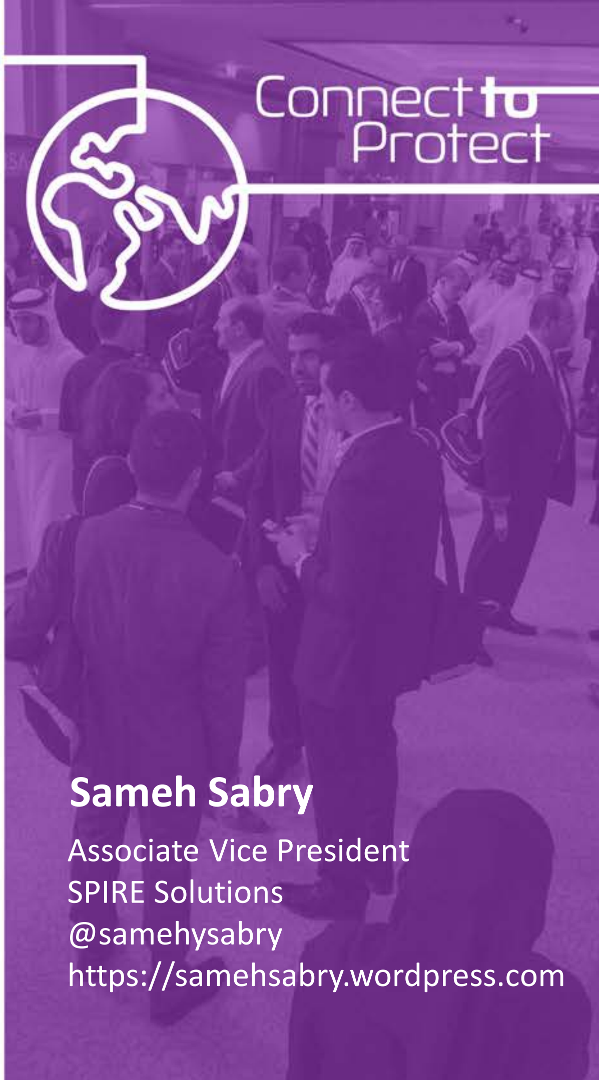
RSA® Conference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: SPO2-T07

Serious Threat Hunting: Hunting for Advanced Adversaries Without Indicators of Compromise



Sameh Sabry

Associate Vice President
SPIRE Solutions
@samehysabry
https://samehsabry.wordpress.com

#RSAC

Hunting

Introduction

- Attacker trends and challenges
- A new approach – Hunt
- How to hunt
- Is this really for me (spoiler alert: yes)

Today’s Reality

76%

of organizations compromised

146 days

average dwell time

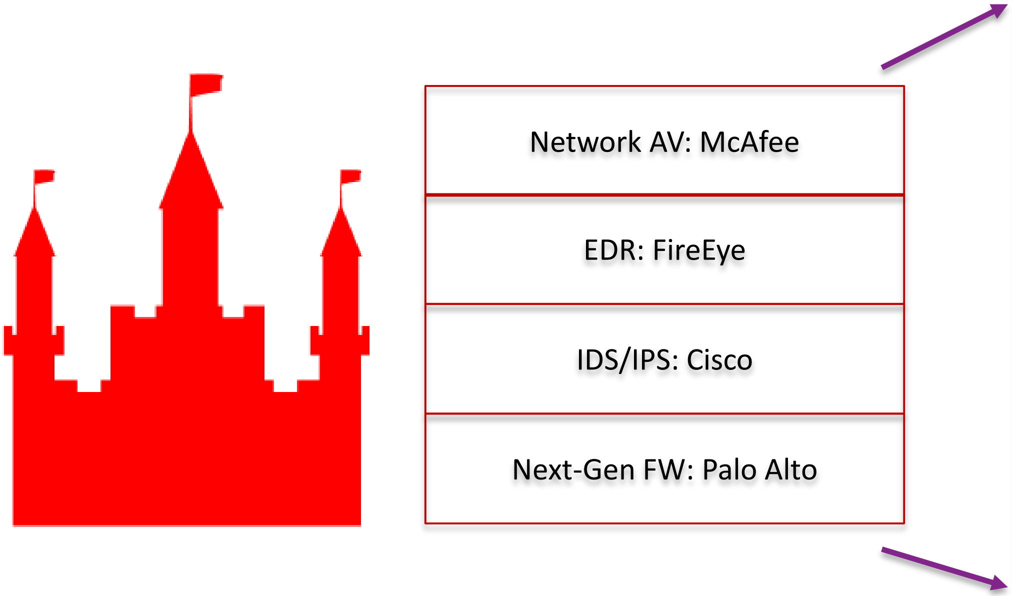
$75B

spent on enterprise security

The cycle isn’t working: Prevention, detection, triage, response

- Prevention is important but will be bypassed
- Search and signature based detection is way behind
- Often, breach notification is external
- Often, additional adversaries are there while a known incident is closed

Today’s Reality: Why?



Network AV: McAfee

EDR: FireEye

IDS/IPS: Cisco

Next-Gen FW: Palo Alto

Advanced Adversaries

- Evade security tools
- Know to avoid tripping known IOCs
- Advanced human-directed attacks
- Use polymorphic malware & customized attacks
- Avoiding outlier analysis

What is Adversary Hunting?

Hunting is the proactive, stealthy, and methodical pursuit and eviction of never-before-seen adversaries inside your network without relying on Indicators Of Compromise (IOCs).

Hunting is

Attacker Technique Focus

- Signatures are stale
- Attacks are unique
- Sophisticated attacks are tailored

Proactive, Stealthy, Methodical

- Hunt for the adversary before an alert
- Hide from the adversary
- Plan the hunt, focus on the target of the attack (their endgame)

Get Ahead of the Onslaught

- Move from IR to proactive adversary detection

Hunting is not…

☒ Searching for IOCs:

- Advanced attacks are unique to organizations
- Hunters discover and pivot on indicators, not start with indicators

☒ Data Gathering

- Hunting is not just the ability to collect mass amounts of data
- Effective hunting finds the adversary by automating and facilitating expert analysis

☒ Waiting for an Alert

- Hunting is IR with a different starting point

Hunting Challenges

Lack of Resources

- Process
- People
- Technology

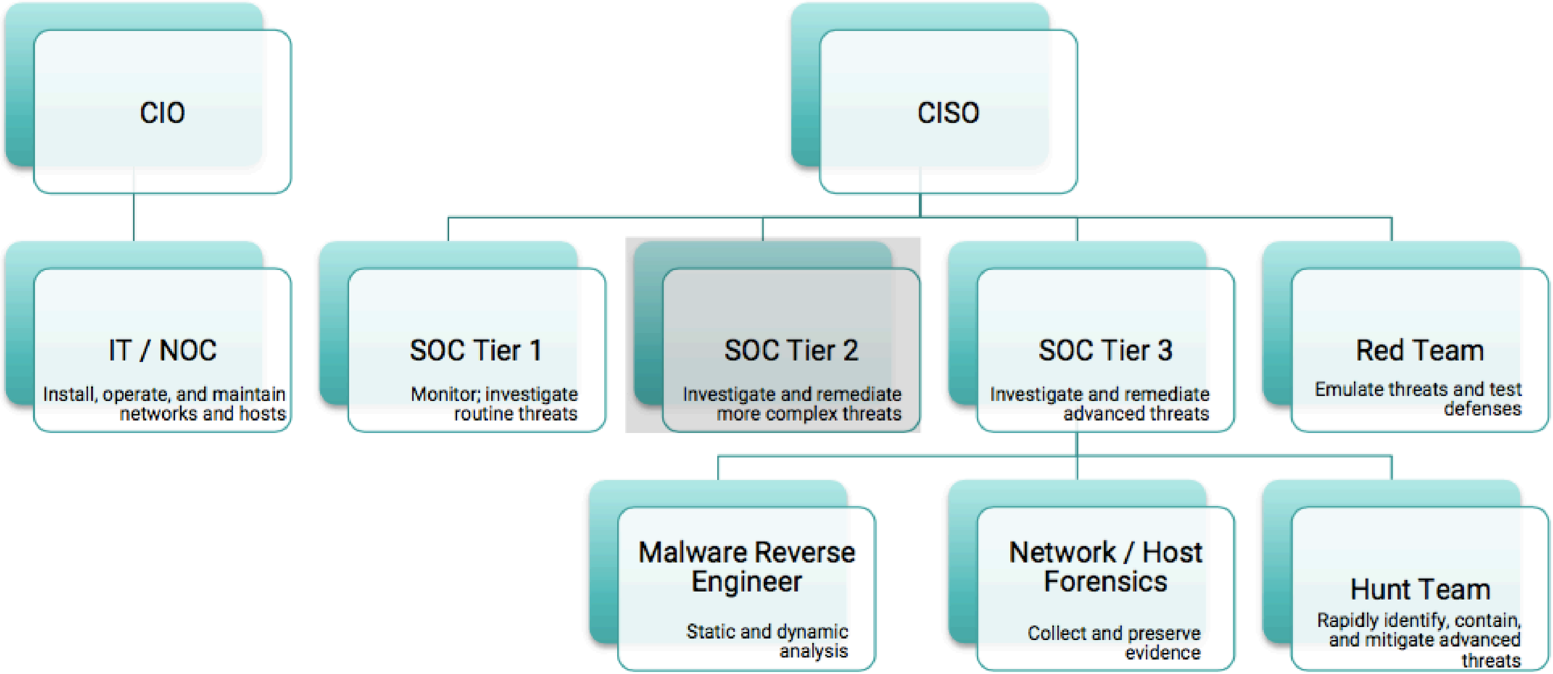
Drowning in Data

- Knowing where to look for the problem
- Search is not enough
- Automating analysis at scale

Tipping off the Adversary

- Hiding from the adversary
- Strong anti-tampering to prevent detection gaps

Hunting Roles Within Security Team


CIO
IT / NOC
Install, operate, and maintain networks and hosts
CISO
SOC Tier 1
Monitor; investigate routine threats
SOC Tier 2
Investigate and remediate more complex threats
SOC Tier 3
Investigate and remediate advanced threats
Red Team
Emulate threats and test defenses
Malware Reverse Engineer
Static and dynamic analysis
Network / Host Forensics
Collect and preserve evidence
Hunt Team
Rapidly identify, contain, and mitigate advanced threats

Hunt Approaches

Topic	Current Approach	The Hunt
Detect threat	• IOCs / signatures of past events • External threat intel feeds • Cloud-based analytics	• Behavior-based protections prevent never-before-seen threats • Data science encapsulated in sensor
Avoid adversary detection	• Separate process easily identified	• Stealth installation, operations, and communications prevent disruption by adversary
Data	• Wholesale data collection (network-intensive)	• Answer critical questions • Automated analysis
Hunt	• EDR: respond to alerts • Search IOCs	• Proactive investigations • Automation
Remediation	• Kill entire processes	• Surgical response: thread-level precision

The Hunt Cycle

SURVEY

Recon of internal network

Identification of assets to protect

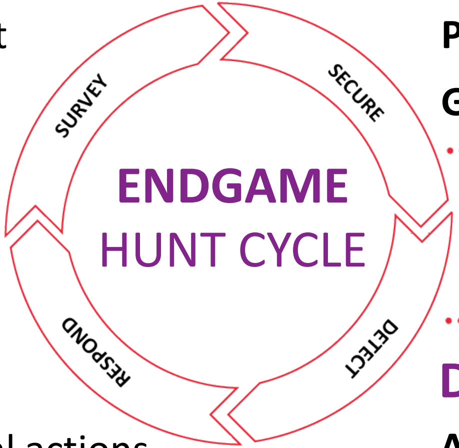
Gather data

SECURE

Implement mitigation techniques

Prevent adversary techniques

Gather uncompromised systems



RESPOND

Respond intelligently with surgical actions

Act at scale to evict the adversary

Report on the hunt

DETECT

Analyze collected data for outliers

Discover new indicators of compromise

Pivot to determine the full extent of breach

Attacker Chokepoints

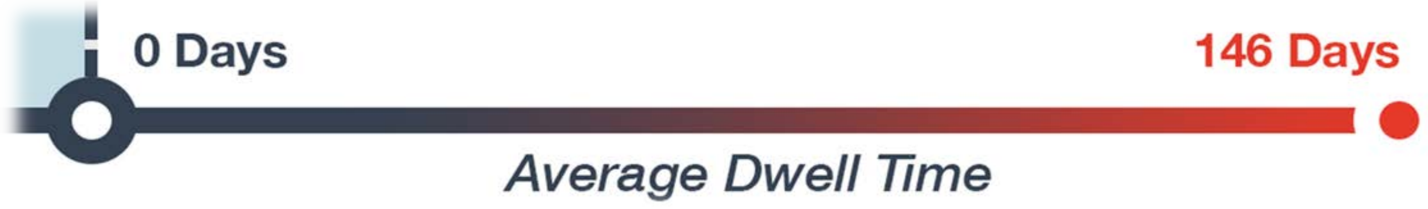
- Chokepoints: Specific low-level system resources which must be accessed, used, or manipulated by the adversary to meet an objective.
- Some common attacker techniques visible on endpoints
  - Injecting code into running processes
  - Dumping credentials from memory
  - Impersonating tokens
  - Evading AV products

Attacker Chokepoints

- Chokepoint monitoring is critical to detect and prevent known and never-before-seen adversaries
- Benefit – you can block in addition to detecting at chokepoints
  - Stop whole classes of techniques

Hunting Benefits

The attack lifecycle:



Catch Advanced, Customized Attacks

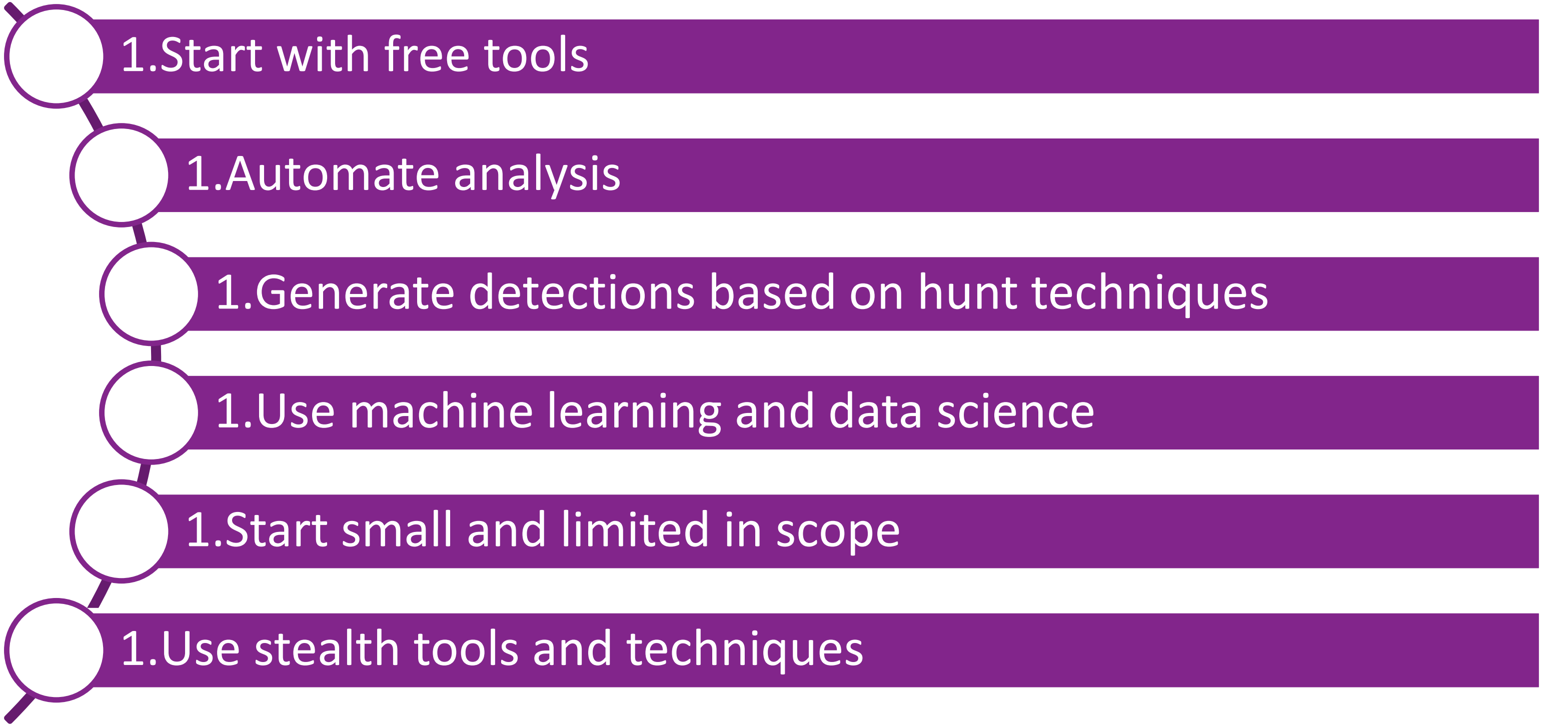
Reduce Dwell Time

Scaled Detection and Response

Summary

- Hunting allows you to find and remediate intrusions earlier
- Start hunting now – best way to find new and tailored attacks
- Hunt on and across the systems simultaneously with complementary methods
- Automate, automate, automate

Apply



1.Start with free tools

1.Automate analysis

1.Generate detections based on hunt techniques

1.Use machine learning and data science

1.Start small and limited in scope

1.Use stealth tools and techniques

Thank You