RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **Sao-W03V**

You See Honey, I See Beehive
- Developing Honey Networks -

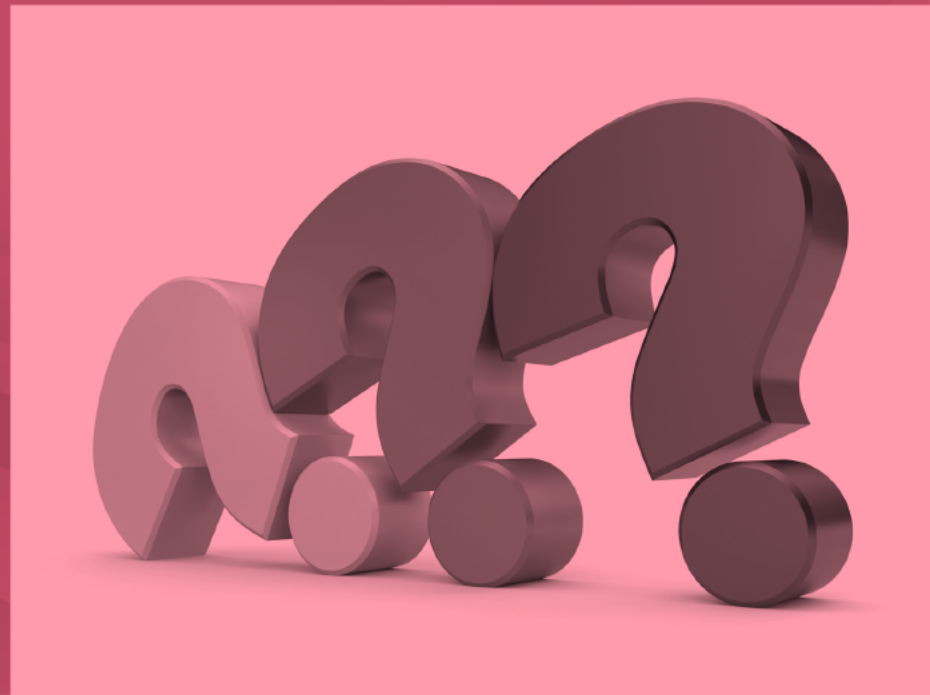
Joseph Muniz

Security Architect / Researcher
Cisco Systems
@SecureBlogger

RSAConference2020 APJ

A Virtual Learning Experience

Why Care About This?



Cat And Mouse Game

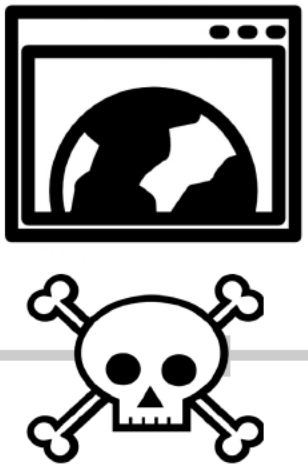
Computer OS

Internet Browser

Browser Plugins

Powershell
IoT
Phishing
Etc.

Cat And Mouse Game



Time

Computer OS

Internet Browser

Browser Plugins

Powershell
IoT
Phishing
Etc.

Cat And Mouse Game

Time

Computer OS

Internet Browser

Browser Plugins

Powershell
IoT
Phishing
Etc.

Cat And Mouse Game

Time

Computer OS

Internet Browser

Browser Plugins

Powershell
IoT
Phishing
Etc.

Joseph Muniz

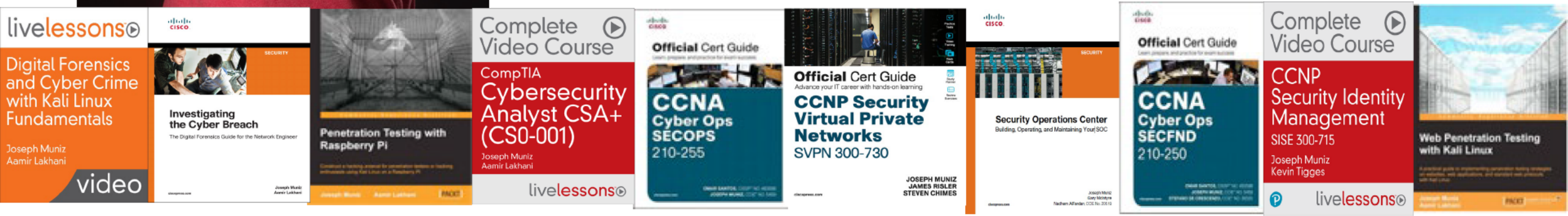
Security Architect – Americas Sales Organization

Security Researcher – www.thesecurityblogger.com

Speaker: Cisco Live / DEFCON / RSA / (ISC)2

Avid Futbal Player and Musician

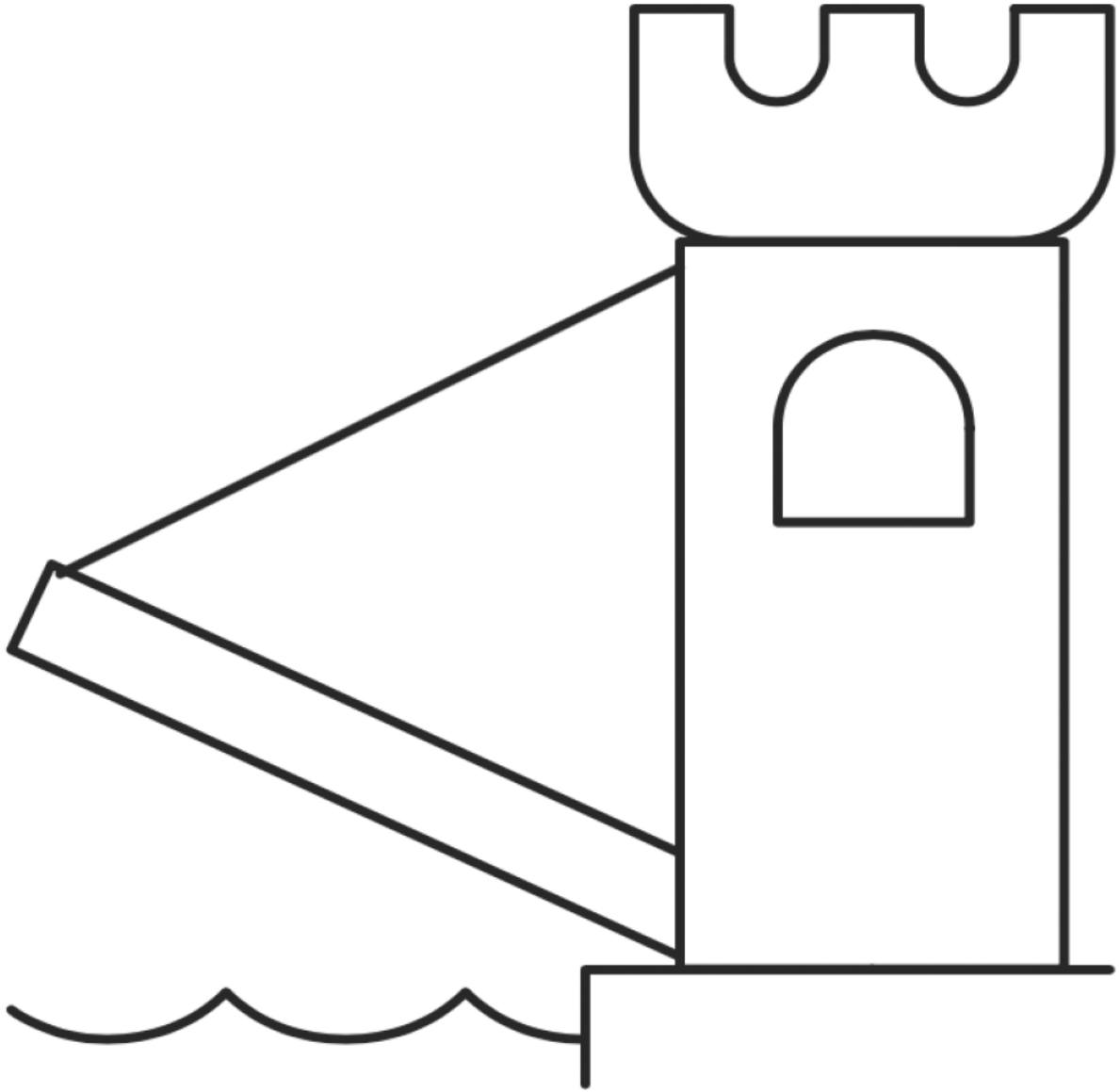
Twitter @SecureBlogger



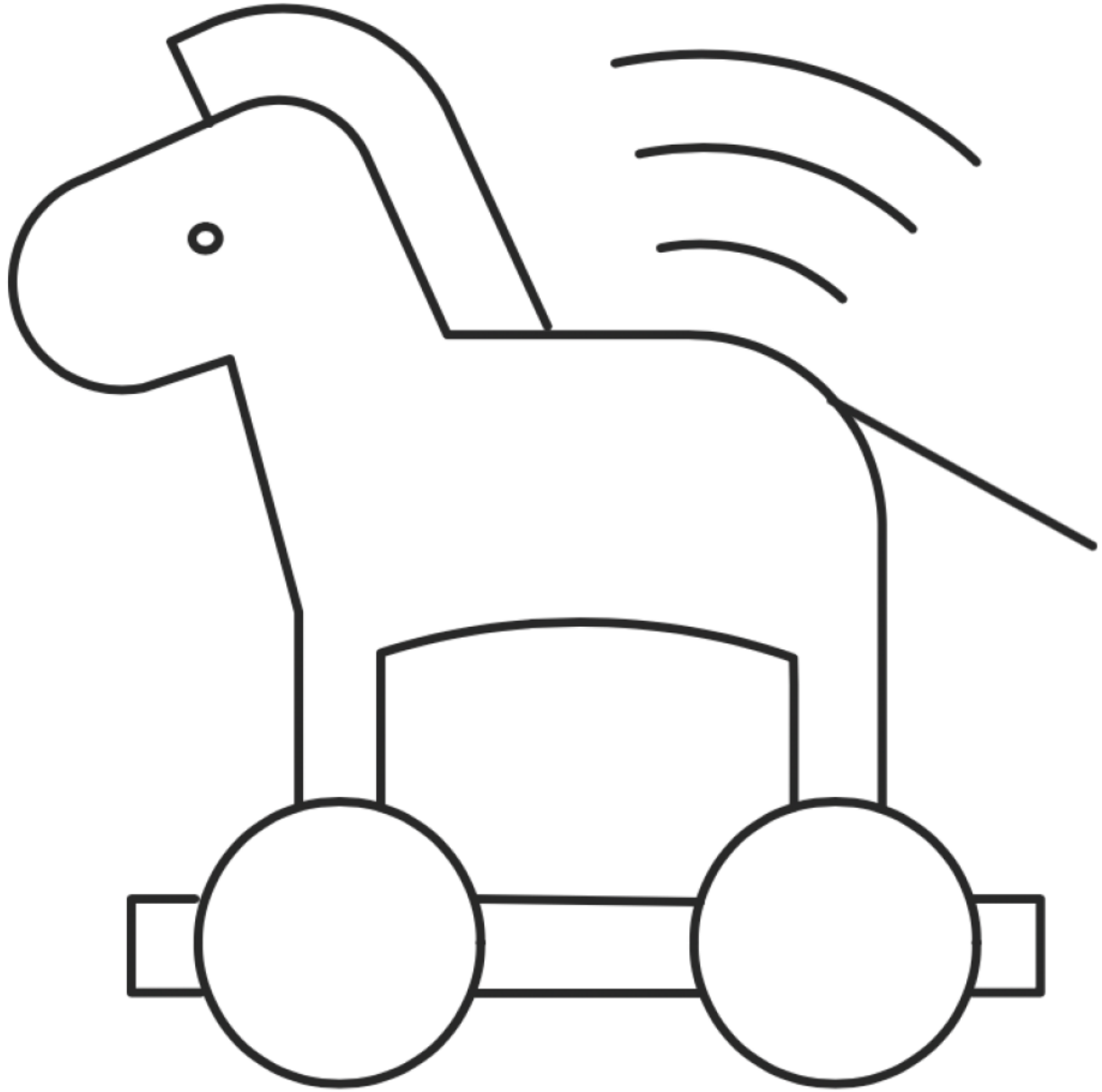
RSAConference2020 APJ

A Virtual Learning Experience

Breach Detection

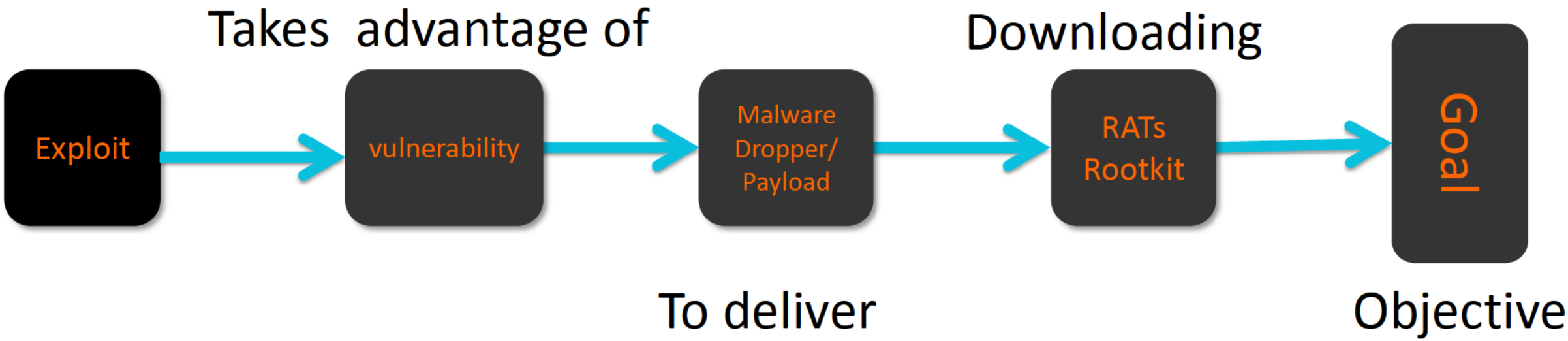


Perimeter-based defense



Change tactics, breach from inside

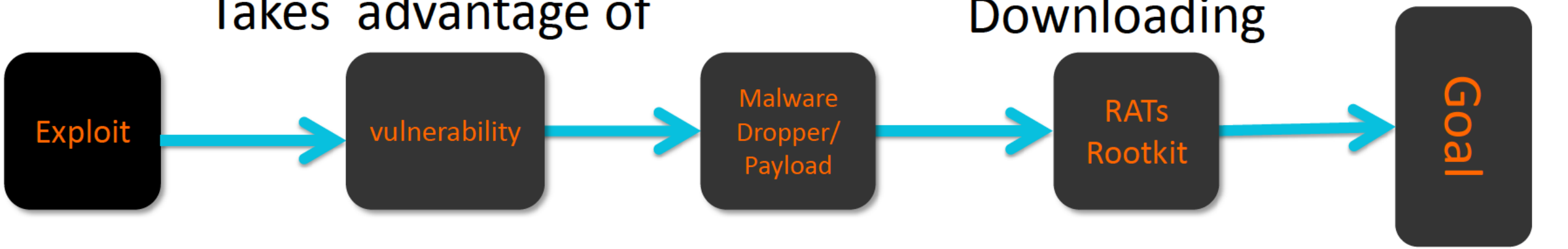
Basic Attack Conept



ttack Conept

Takes advantage of

Downloading



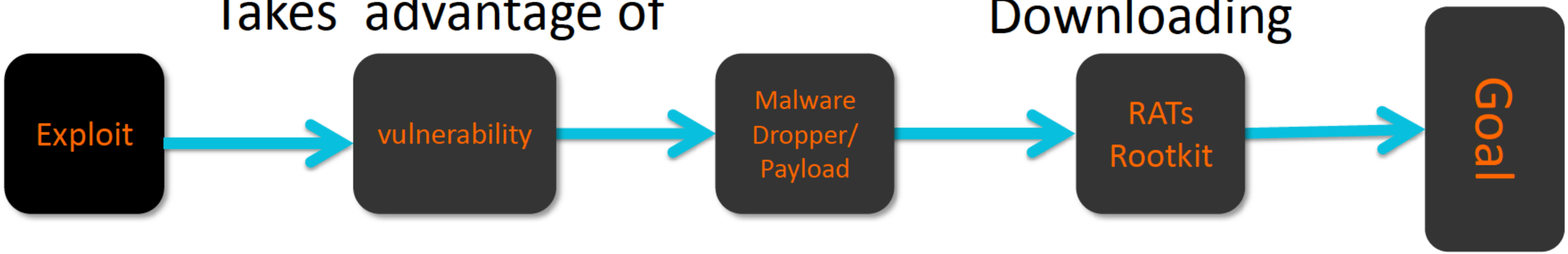
To deliver

Objective

ttack

Takes advantage of

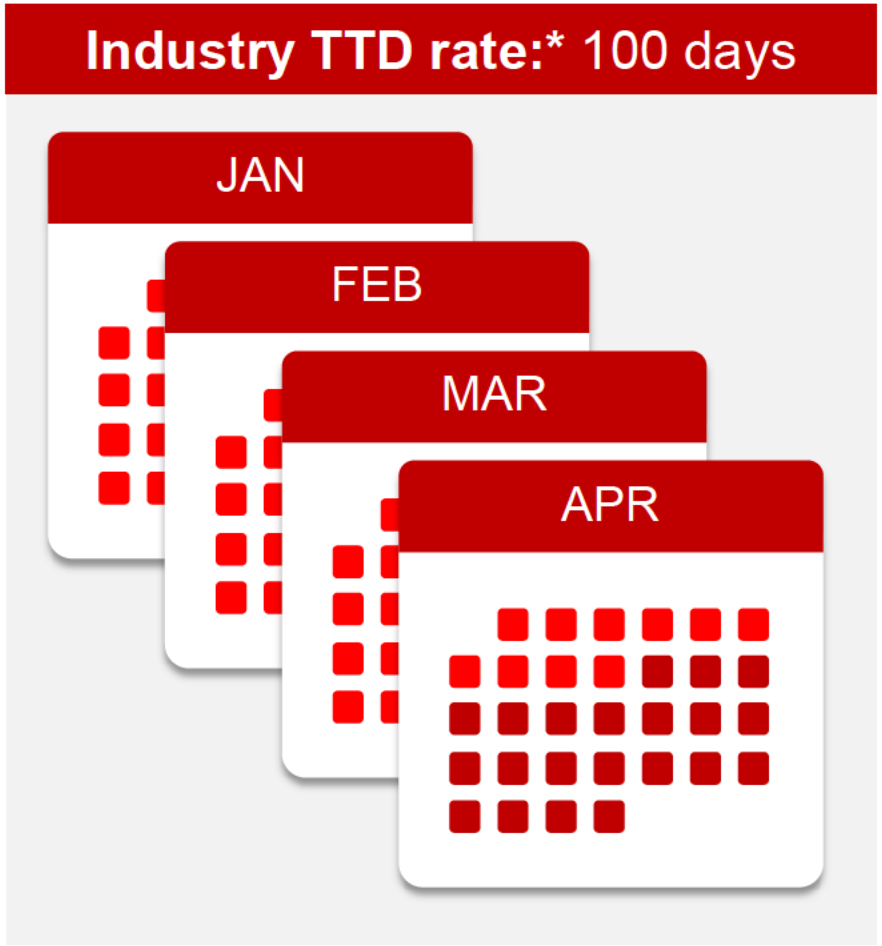
Downloading



To deliver

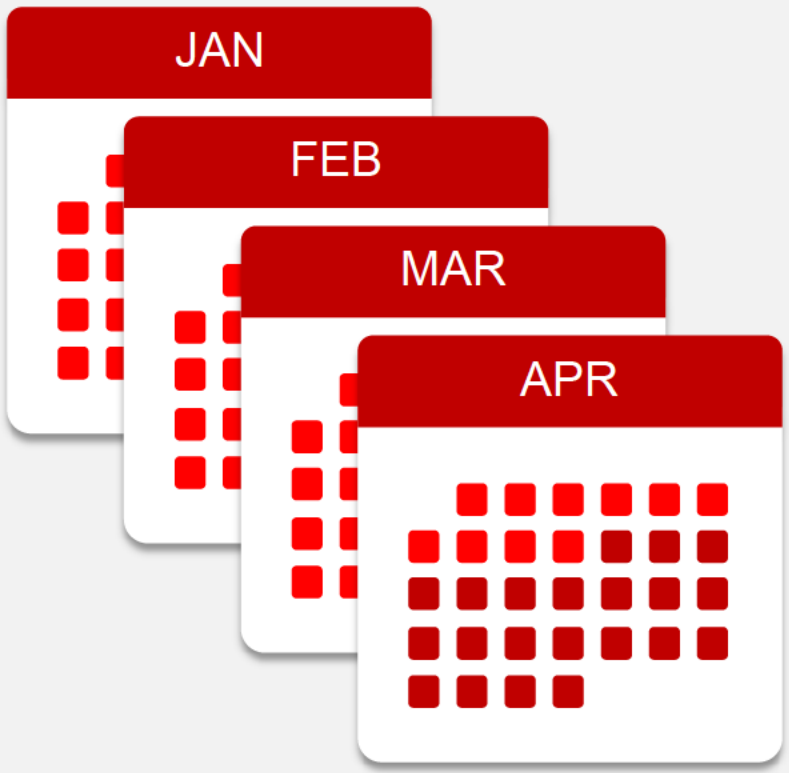
Objective

BD Goal = Detect Infections Earlier and Act Faster



BD Goal = Detect Infections Earlier and Act Faster

Industry TTD rate:* 100 days



Goal: hours


Recon

Breach Detection Options (NIST / ISO)

Honey Pots
Sandbox
NetFlow
IDS/IPS
Packet Capturing
Antimalware
Continuous Monitoring
Reputation Security

Network
Routers
Endpoints
Datacenter
Cloud
IoT

Endpoint and Branch Network

Honeypot

Employee

ENDPOINT

Anti-Virus | Anti-Malware | Data Loss Agent | Reputation Security | Personal Firewall | Disk Encryption | Vulnerability Management | VPN Concentrator | Policy/ Configuration

Access Control

Access Control | Identity | Posture Assessment

Security Operations

SOAR | SIEM | Monitoring | Threat Intelligence | Posture Assessment | Data Orchestration

CISCO

Web Security

Breach Defense

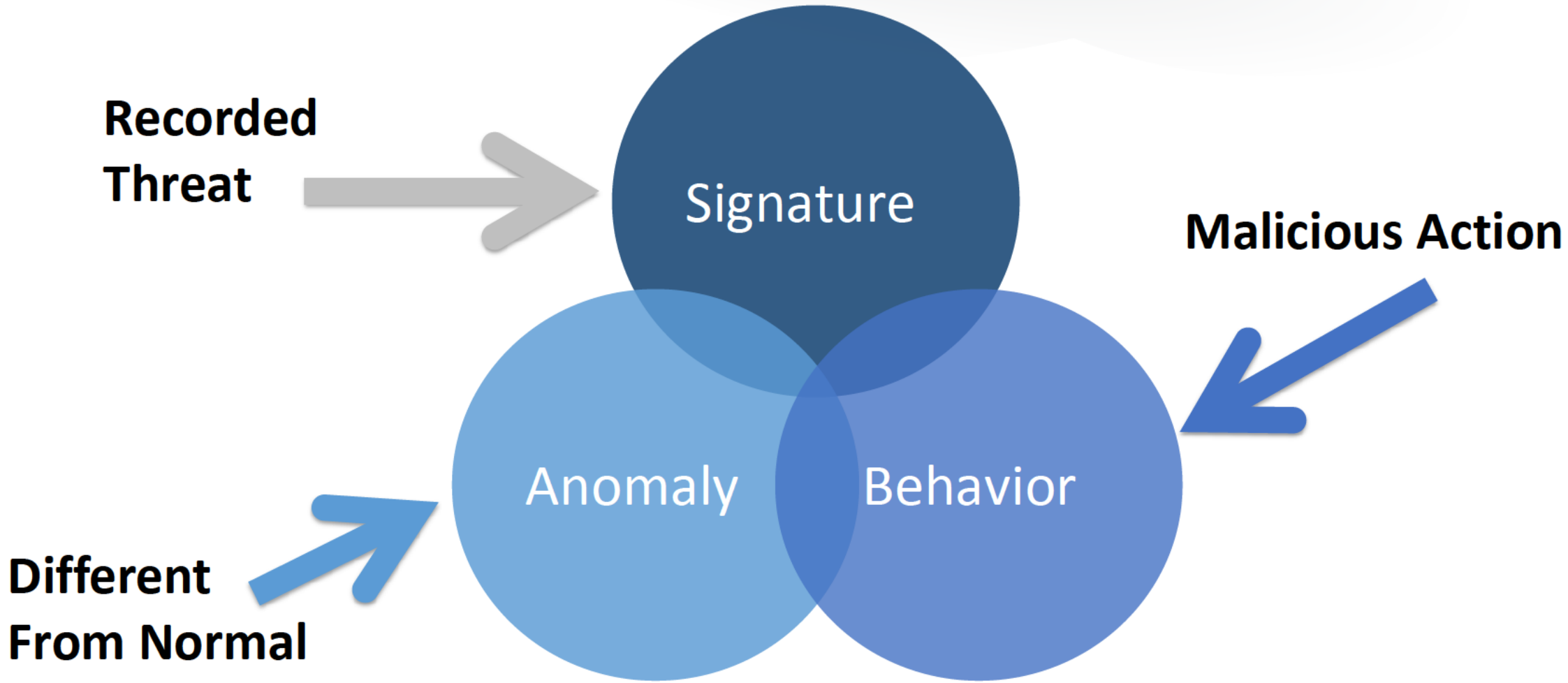
Sandbox / Honeypot | Flow Analytics | Network Anti-Malware | Anomaly Detection | Intrusion Detection East / West

Phantom Networks

Gateway Defense

Anomaly Detection | Intrusion Detection | Application Visibility Control (AVC) | SSL Decryption | Firewall | Geo Filtering | DNS Security | Website

Security Capabilities



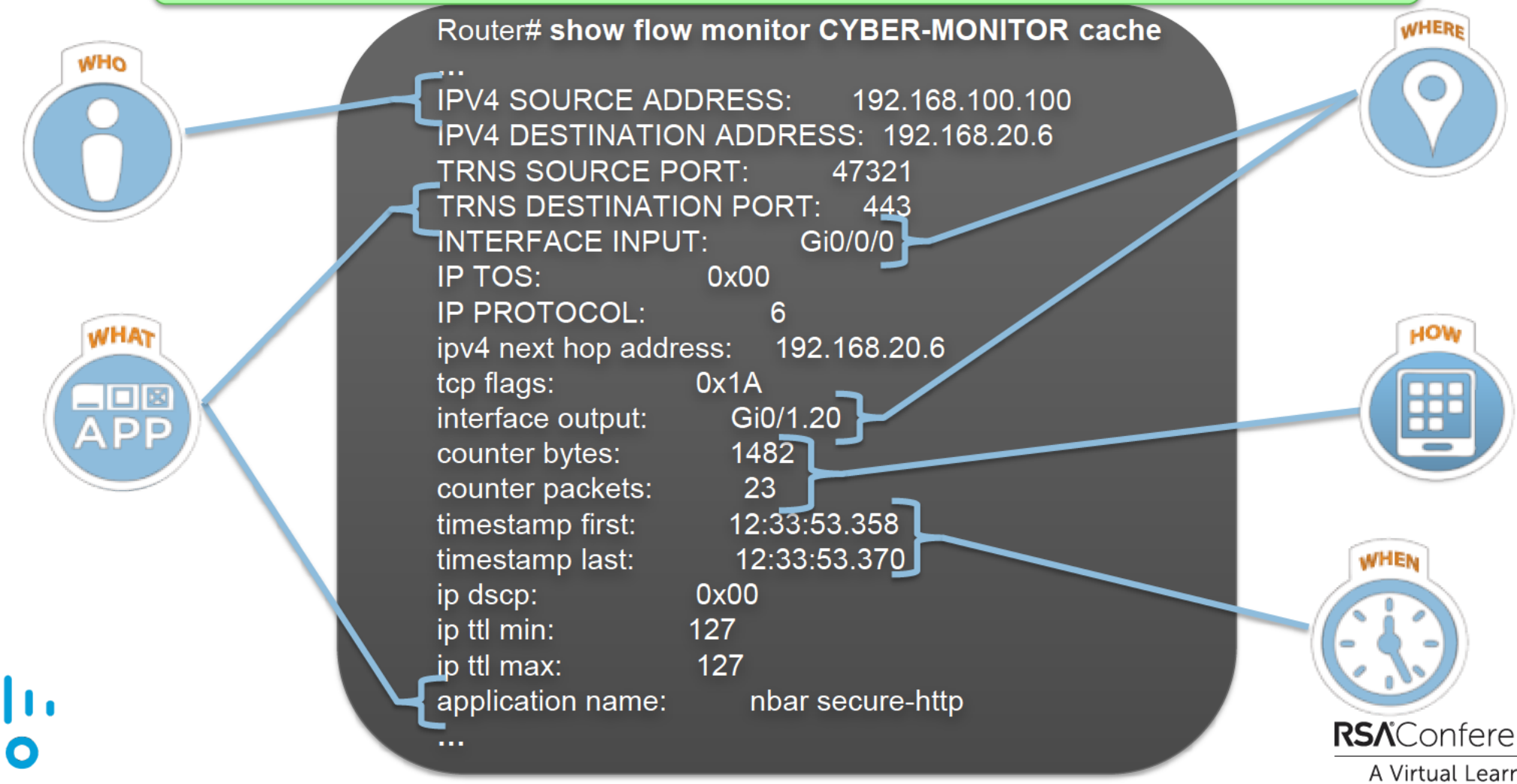
RSAConference2020 APJ

A Virtual Learning Experience

Phantom Networks

NetFlow = Visibility

A single NetFlow Record provides a wealth of information



Why Unsampled NetFlow?

Sampled NetFlow

- Subset of traffic, usually less than 5%,
- Gives a snapshot view into network activity
- Similar to reading every 20th word of a book
- Suitable for detecting large scale DDoS attacks, but not extended, slow attacks

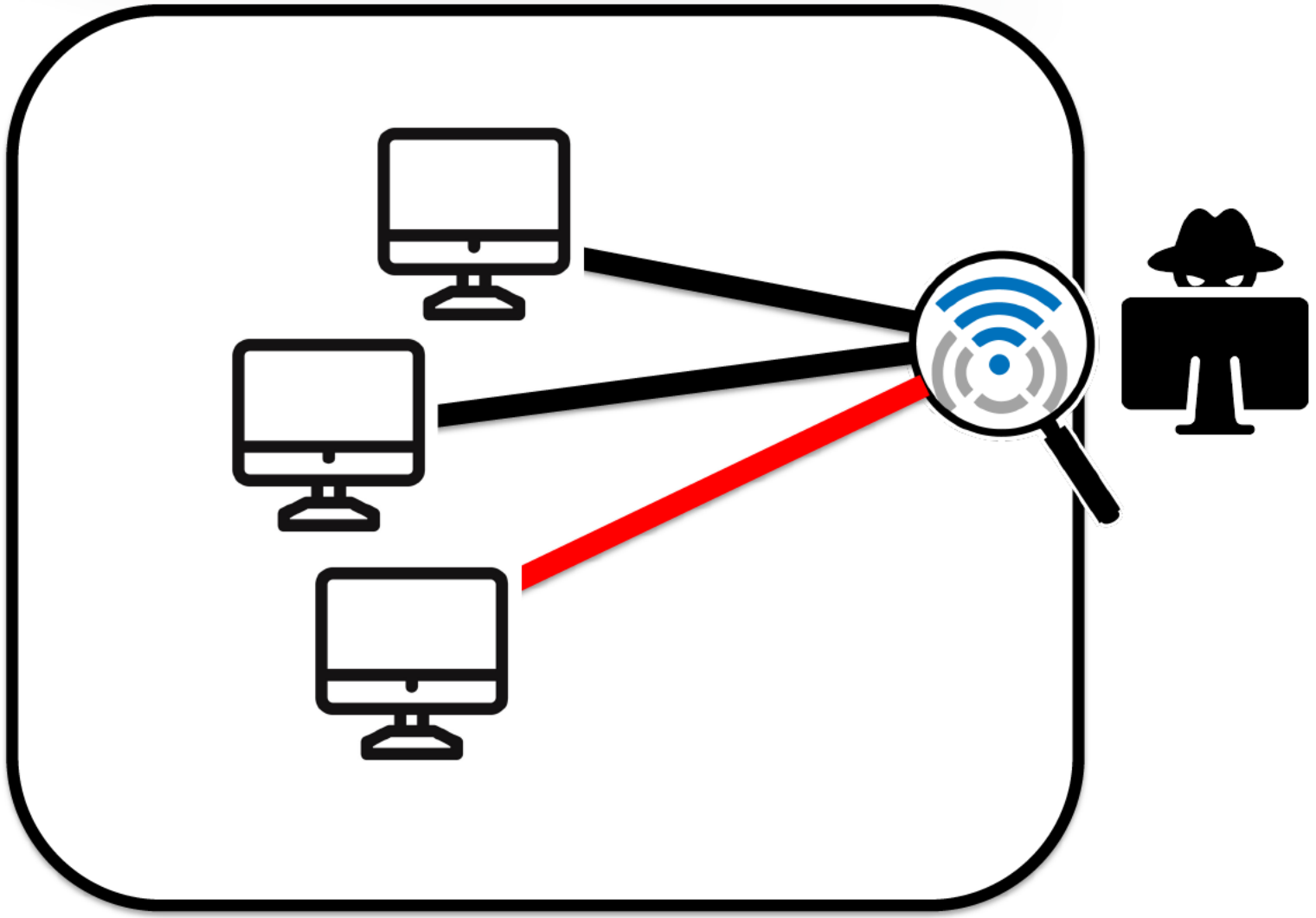
Full NetFlow

- All traffic is collected
- Provides complete view of all network activity
- Similar to reading every word, page of a book
- Suitable for detecting large scale as well as extended, slow attacks

Phantom Network Zones Concept

Malware, Attackers or other Internal Threats must perform **RECON** to identify other targets and networks.

A phantom network is a tripwire



Phantom Network Alarm Examples

Investigation revealed x-ray machine scanning Class B range on DISA owned Internet

Host	CI	CI%	Security Events
10.146.30.23	497,325,158	68,996%	Exploitation, High Concern Index, High SMB Peers, Max Flows Initiated, New Flows Initiated
[redacted] (10.34.100.42)	205,529,732	263%	

Splunk scanning example which led to breach discovery

Subnets Designed for "Threat Detection"

- **Monitor for connections** – NetFlow Triggers / Crossing network Zones
- **Configure packet capture triggers –** Linked to SIEM or NetFlow tool
- **Integration with NAC**
  - **Context** = Who and What
  - **Auto quarantine devices** = Many options for "quarantine"

Concerns

- False Positives – Whitelist vulnerability scanners, etc.
- Management of alarms

RSAConference2020 APJ

A Virtual Learning Experience

Honey Pots

Honeypots

- Decoy system to lure cyberattacks, and detect, deflect or study
- Learn attacker techniques and test new attacks in the wild

- ***2 Public Addresses*** *- 1 for management and 1 for honeypot services*
- ***No NAT*** *- Some attacker services not correctly recorded with NAT*
- ***VPS services*** *- Lots of attacks will cause termination of services*
- ***Honeypot compromises*** *- Used to host malware and illegal content*

Honeypot Personas

- **Low** – Emulate UDP / TCP listening ports to detect scanning
- **Medium** – Allows login attempts and contain basic file structures
- **High** – Complete emulation of a system

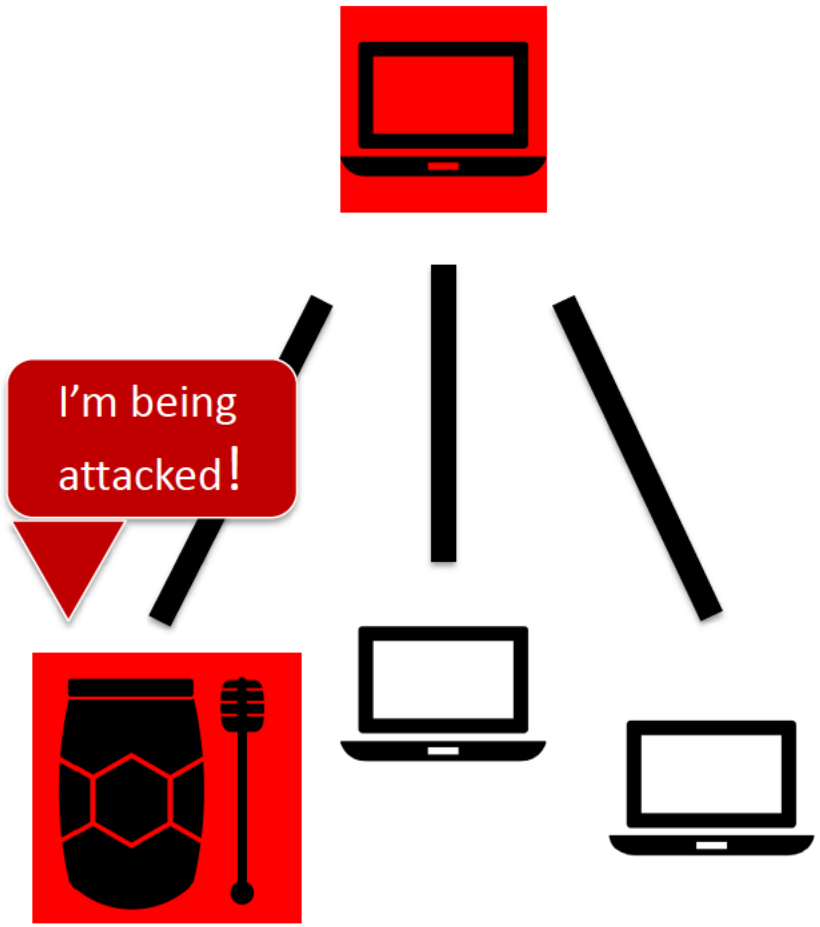
FTP Server | IoT Device | Laptop | WordPress | HTTP | Router


YouTube
Warning!

Honeypot Usage

- High interactive honeypots are also Sandboxes
  - Requires a lot more time to analyze data
- Opensource tends to be harder to setup but more flexible
  - EX) Honeyd can emulate over 100 operating systems down to windows Xp S1 vs S2
- Must have ownership for maintenance or it will be forgotten.
  - Use script to copy data to the honeypot

Internal Honeypots

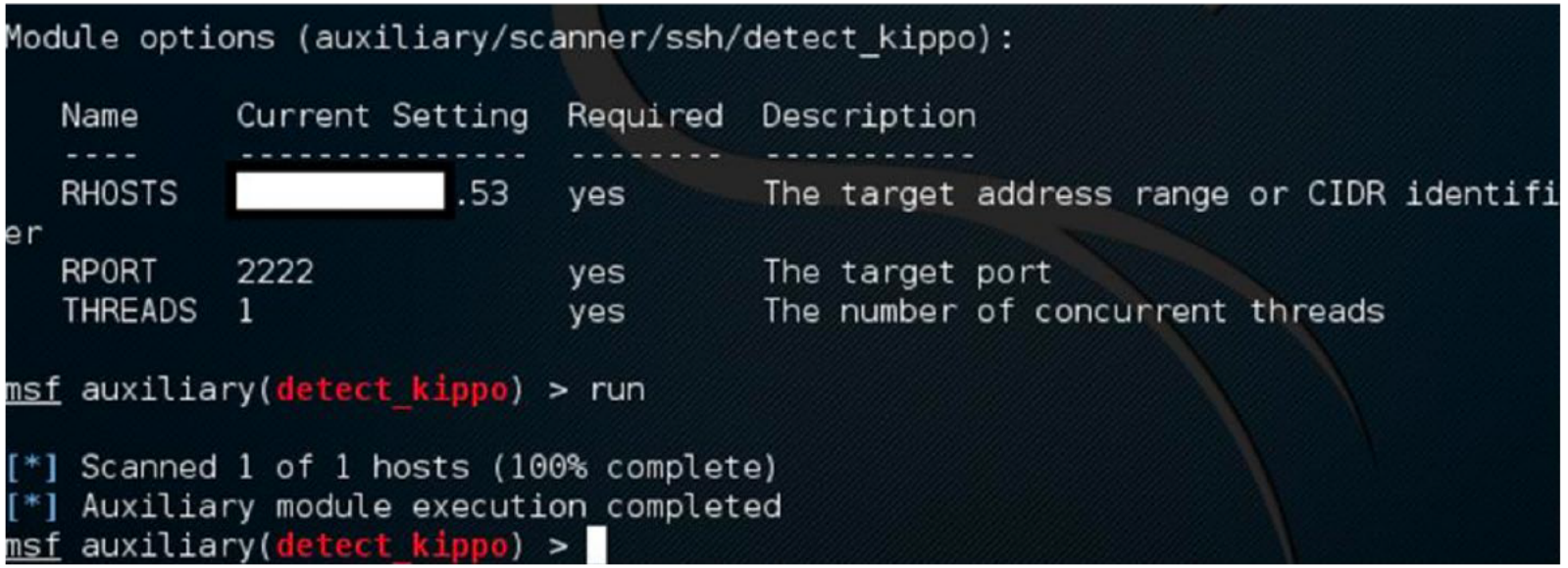


Internal Honeypot = Detect Threats That Breached Perimeter

- Configure vulnerable to lure attacker
- Hide within network (place near similar assets)
- Alert when contacted
- Possibly monitor like sandbox to learn attack behavior

Beware - Honeypot Recon

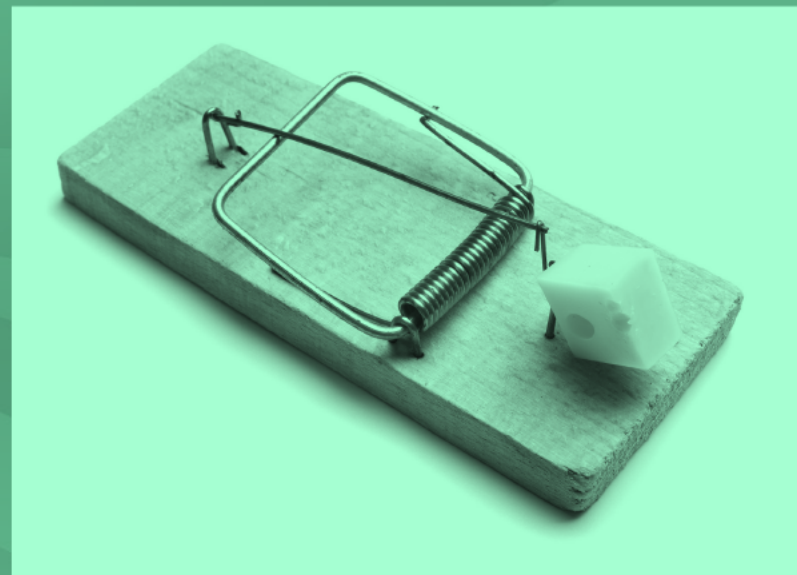
- Attacker pings from honeypot = Set results to unknown host
- Attacker pings a website from honeypot will not match = Simulate something
- Try Metasploit testing such as kippo even if you are using a different but similar honeypot



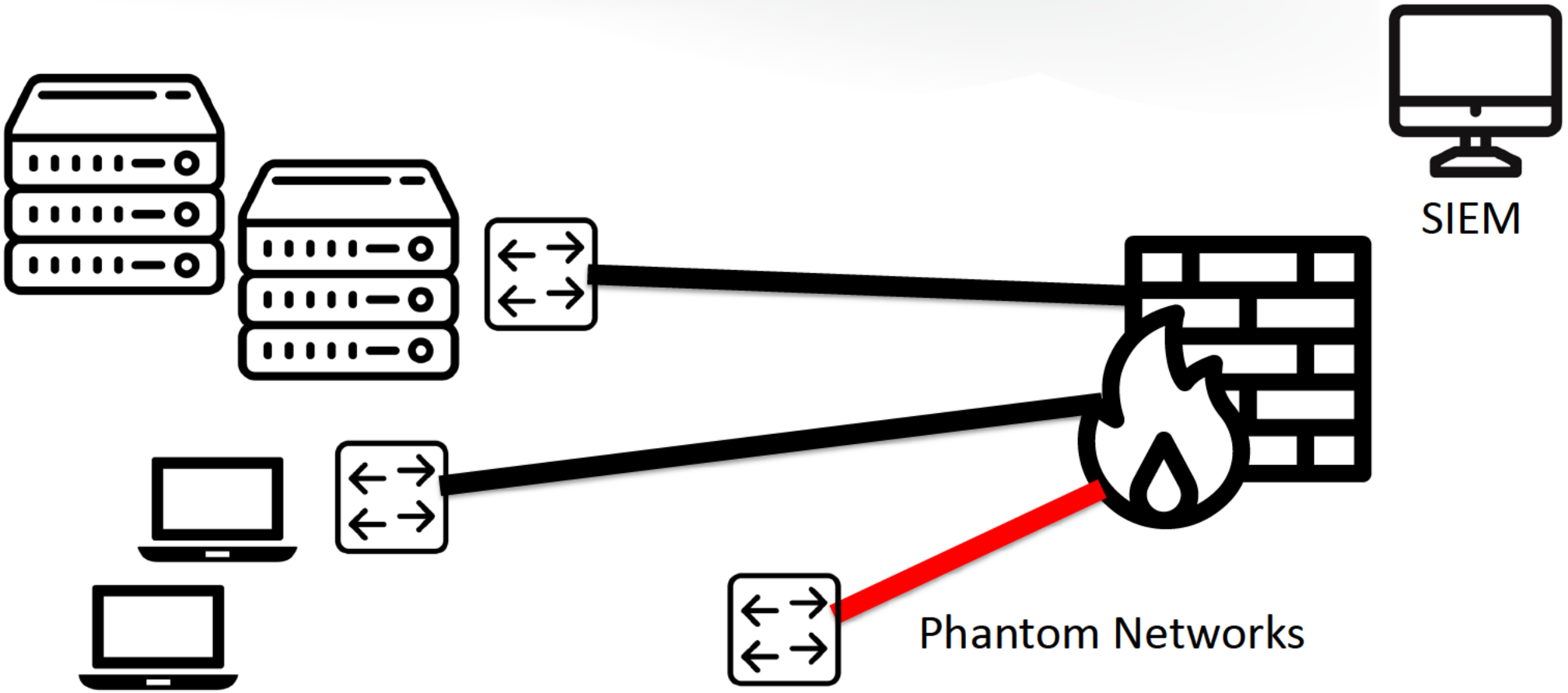
RSAConference2020 APJ

A Virtual Learning Experience

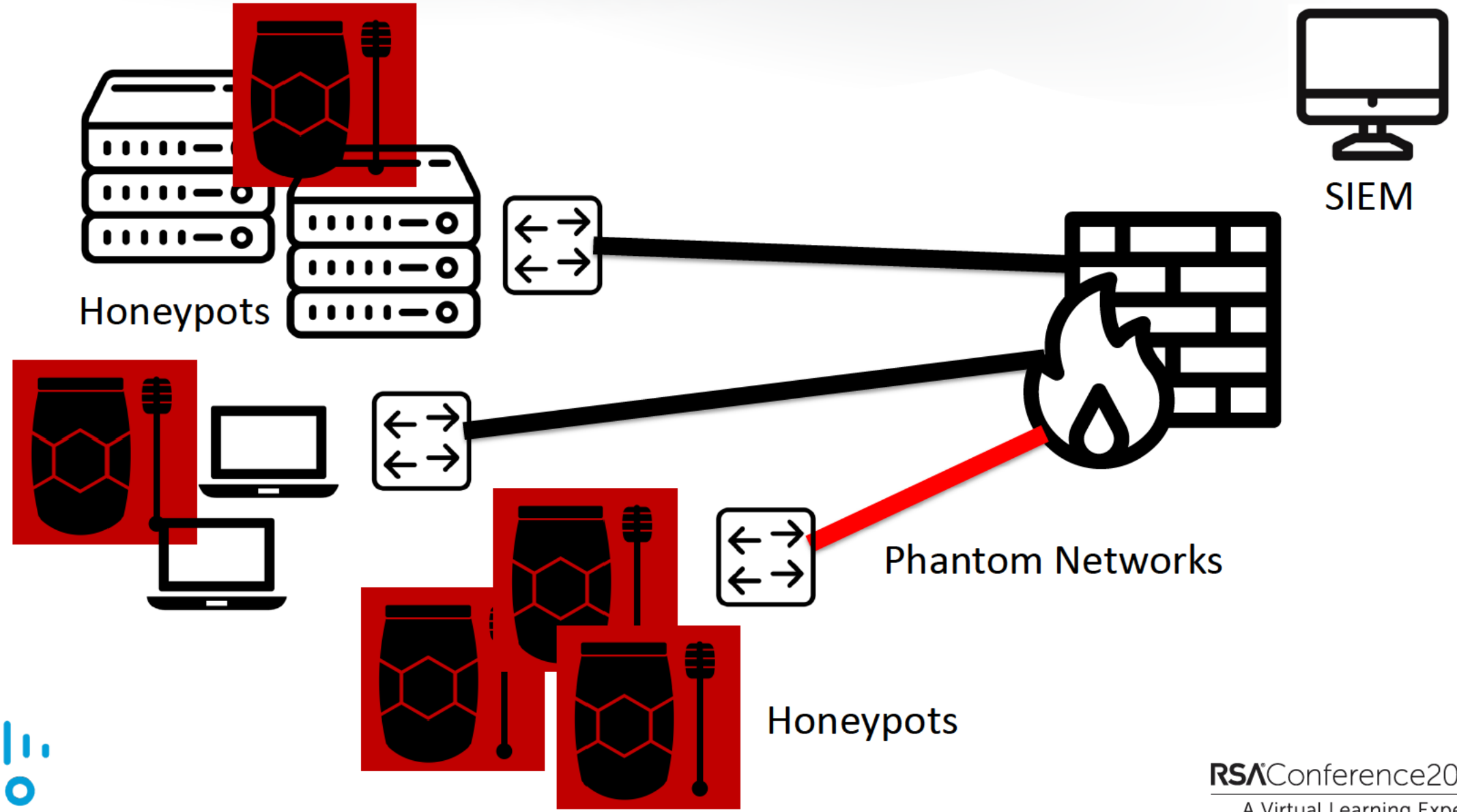
Honey Networks – Total Deception



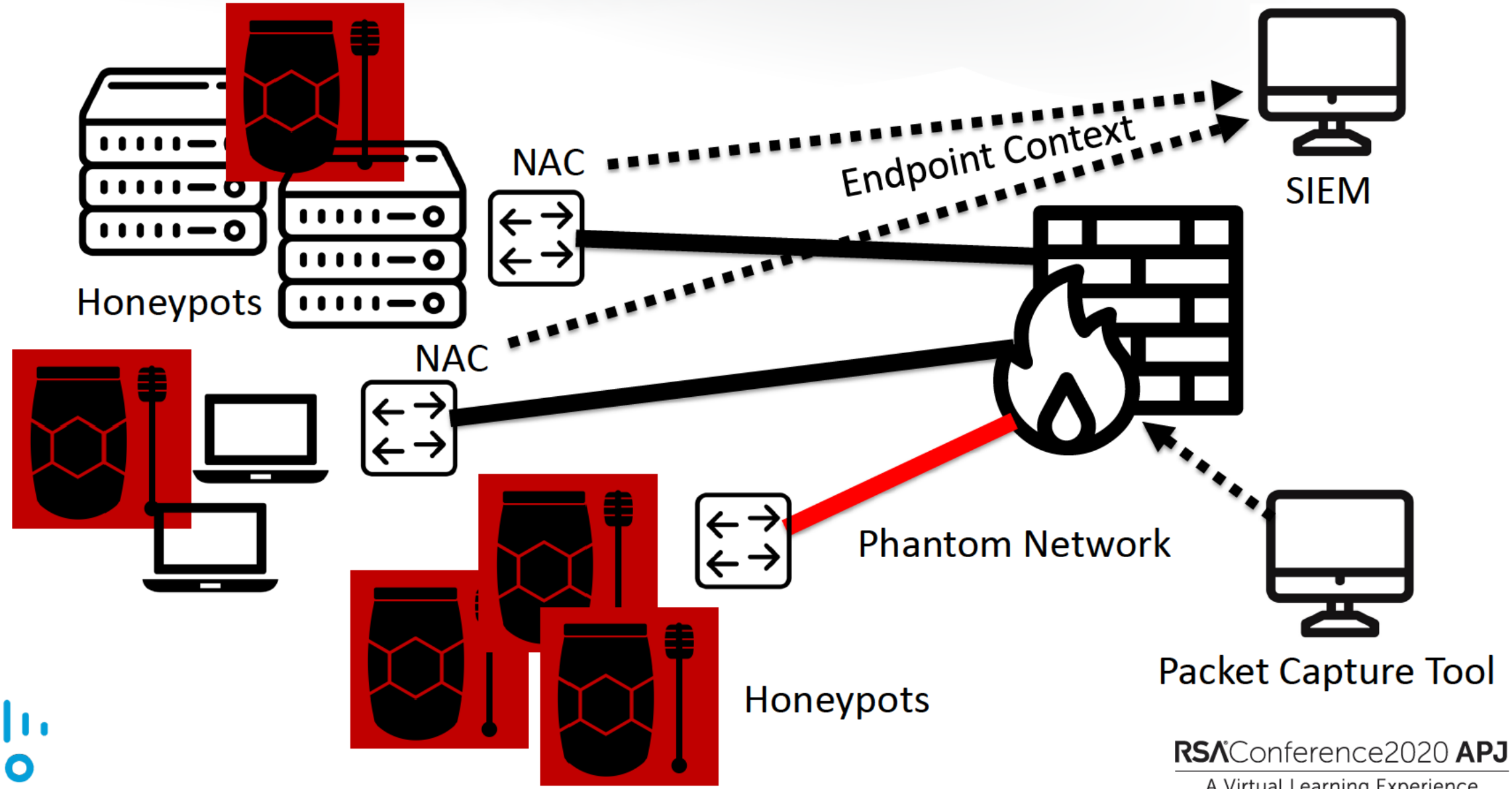
Combine Phantom Networks, Honeypots + Others



Combine Phantom Networks, Honeypots + Others



Combine Phantom Networks, Honeypots + Others



Technology Today

- **NetFlow** – Cisco Stealthwatch, Plixer
- **Honeypots** – Trapx, Attivo Networks, HoneyThing (IoT), ElasticHoney (Database), Thug (Client), Honeydrive, KFSensor,
- **SIEM** – Splunk, Qradar, Logrhythm, OSSIM, OSSEC
- **Packet Capture** – Wirehshark, LiveAction Omnipeek, tcpdump
- **NAC** – Cisco ISE, FortiNAC, ForeScout CounterACT

Tuning Your SIEM

Need Exporter on Honeypot

- Example for Splunk Apps (Splunk Stream, Splunk Universal Forwarder, etc.)

Alert on all inbound activity

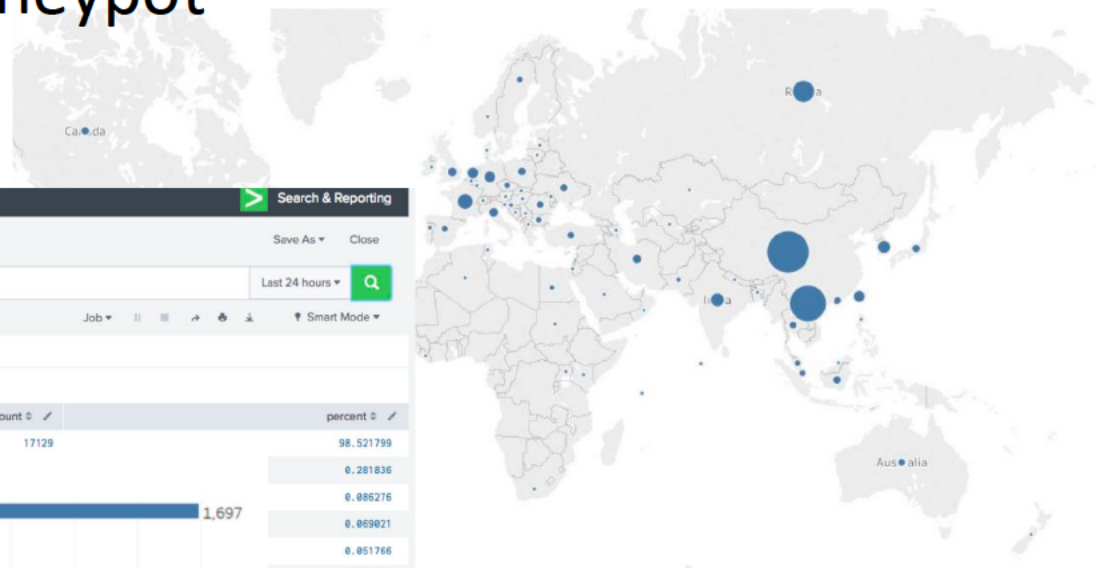
- Honeypot serves no purpose so inbound and pings received are of interest

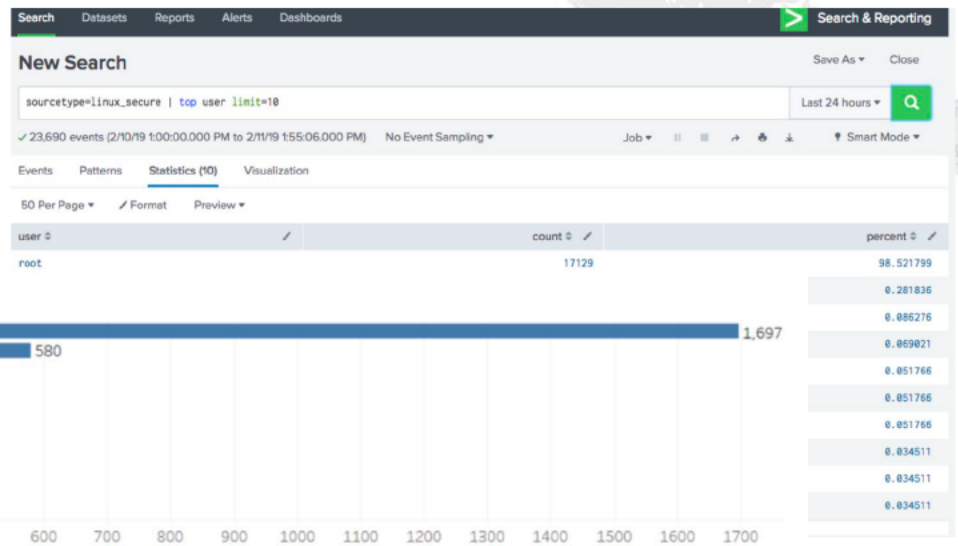
Configure Triggers

- File modification
- Unset command (used to hide history)
- System recon commands (free –m to see memory or id to see group)
- Wget command to download stuff
- IP addresses from other countries – convert into widget
- Login and password attempts – convert into widget

Widgets and Dashboards

- Countries associated with triggering phantom networks
- Login attempt credentials
- Recorded IP addresses
- NetFlow Concern Widgets – Focus on Recon
- Alerts Combining NetFlow tool and Honeypot





Keep it Simple

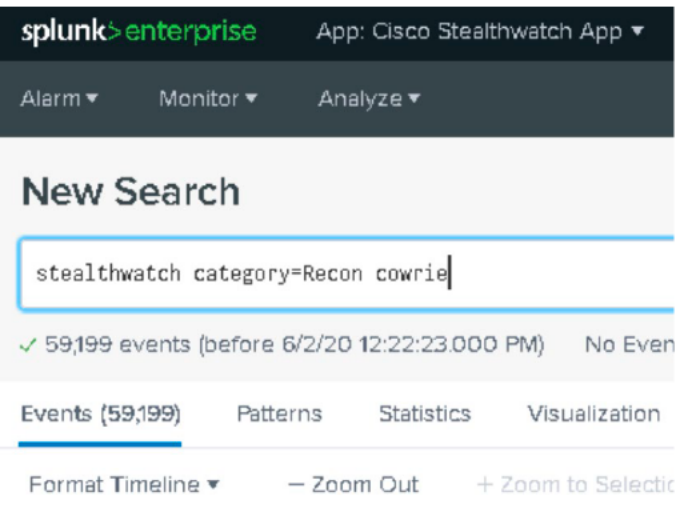
Phantom Networks = recon and IP address identifier.

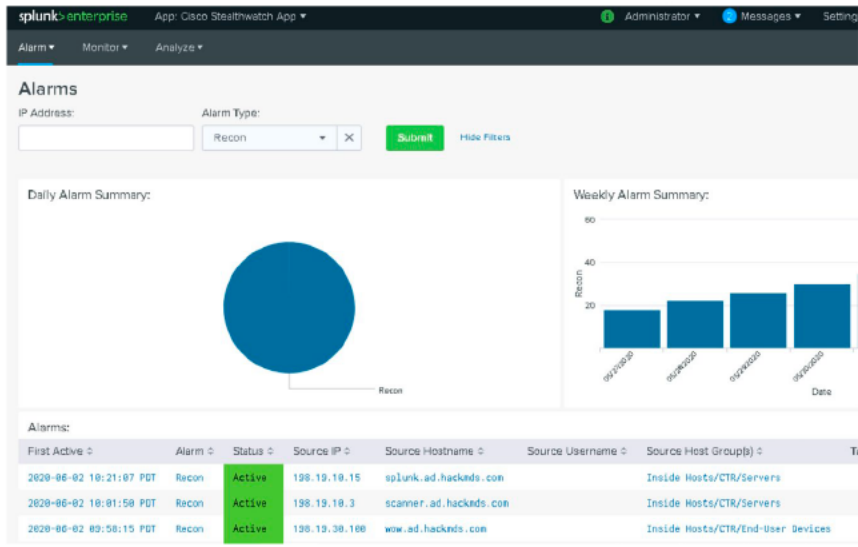
- Ex: Search Splunk: NetFlow or Vendor + recon or + IP

Honeypots = Login and action triggers

- Ex: Search Splunk: honeypot IP + event

Correlate alarms from honeypot and NetFlow tool





Next Steps – Try It Out

- Develop a phantom network (choose technology and triggers)
- Install a honeypot (recommended low interaction at first)
- Test port scanning (AngryIP/Zenmap/Etc.).
- Tune events within SIEM or other event tool
- Assignment management of system
- Add integration (NAC / Packet Capture) and more networks /honeypots

Security is a **Journey** … not a **Destination**!