

RSA® Conference 2020 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



RSA® Conference 2020 APJ

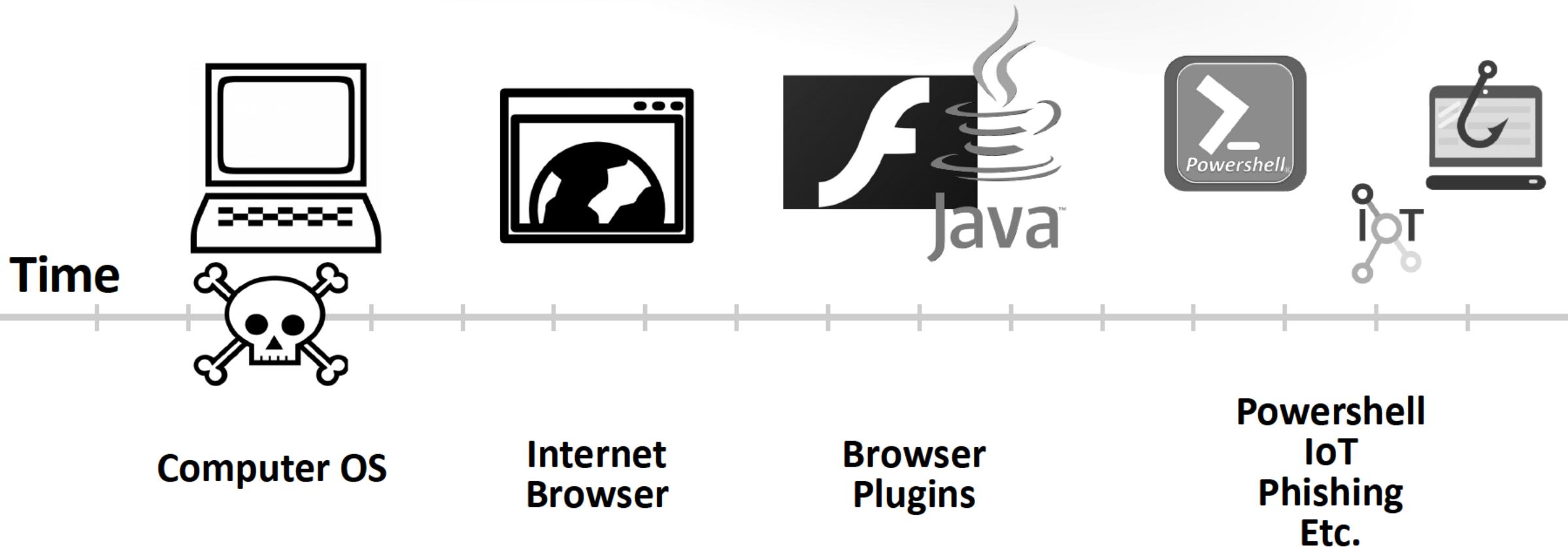
A Virtual Learning Experience

Why Care About This?

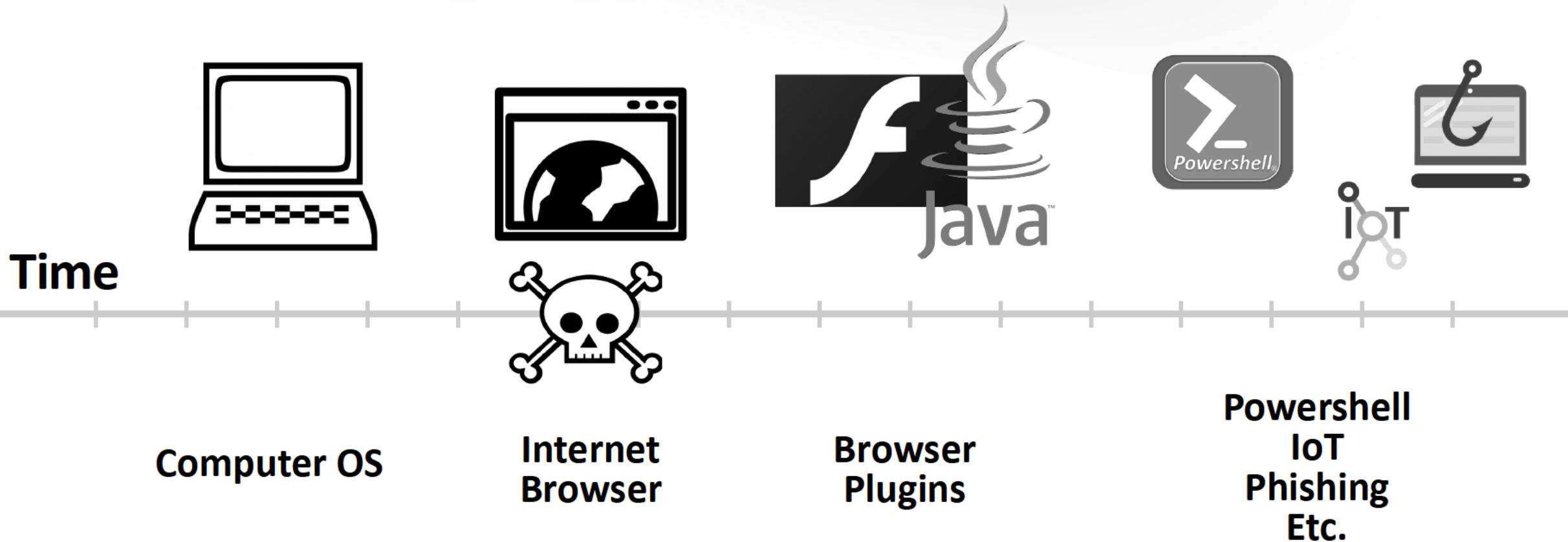




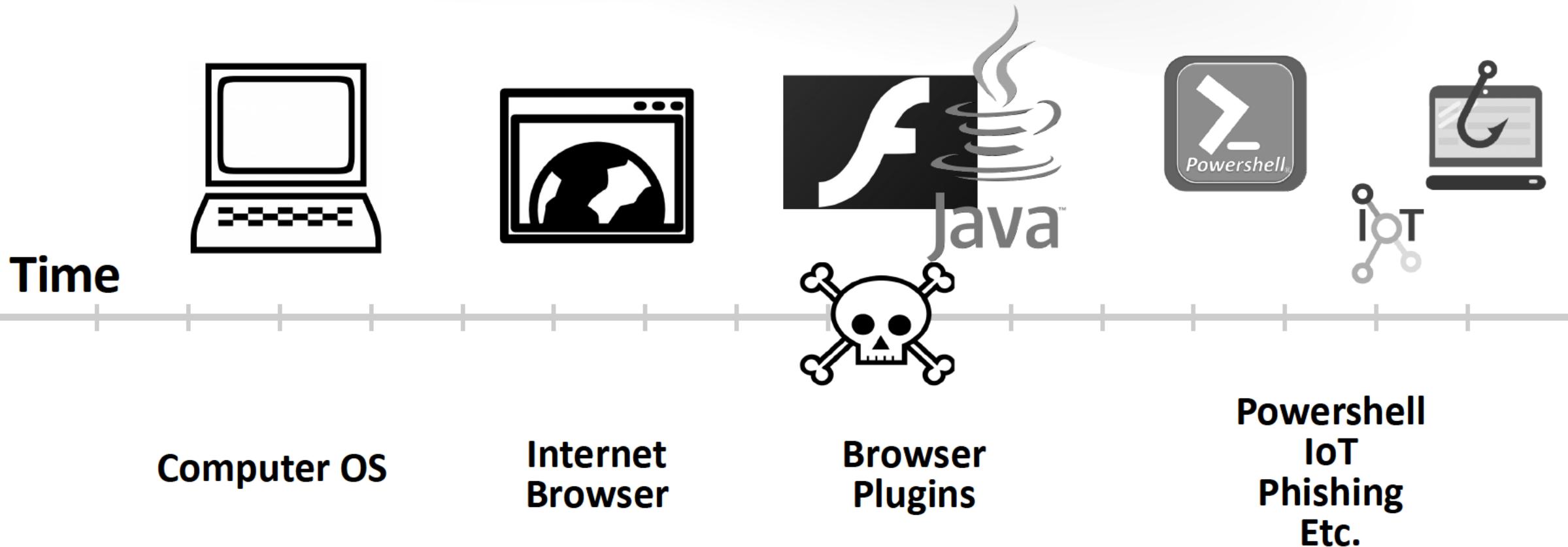
Cat And Mouse Game



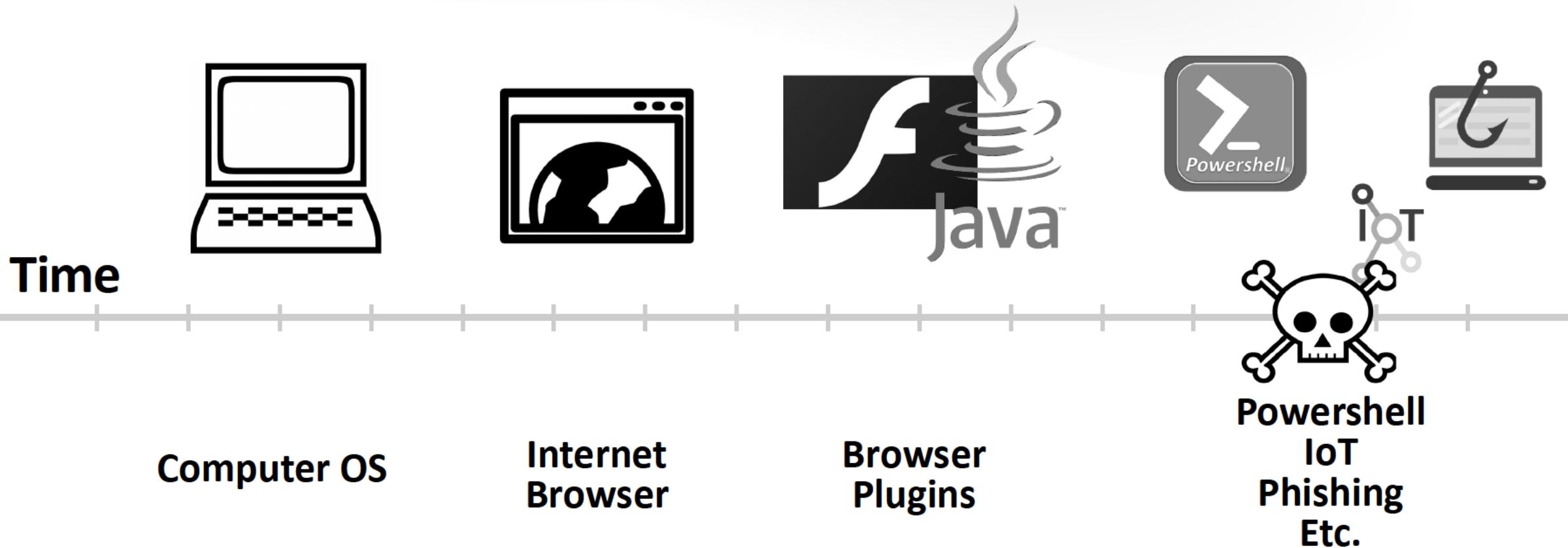
Cat And Mouse Game



Cat And Mouse Game



Cat And Mouse Game



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

A grid of 12 book and course covers related to cybersecurity, featuring Joseph Muniz as the author or speaker. The covers include:

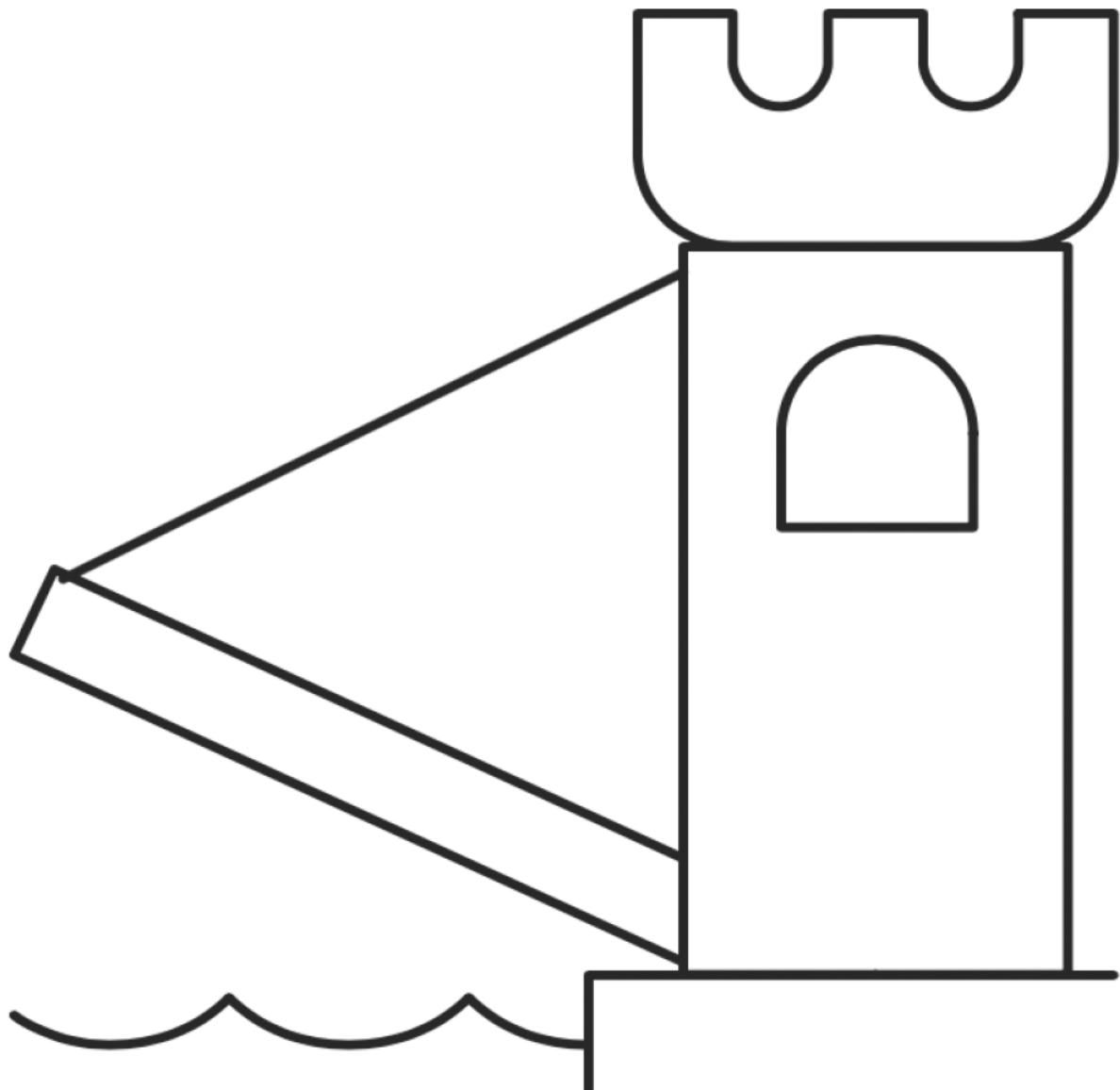
- Digital Forensics and Cyber Crime with Kali Linux Fundamentals (livelessons video)
- Investigating the Cyber Breach (Cisco)
- Penetration Testing with Raspberry Pi (Cisco)
- Complete Video Course: CompTIA Cybersecurity Analyst CSA+ (CS0-001) (livelessons)
- Official Cert Guide: CCNA Cyber Ops SECOPS 210-255 (cisco.com)
- Official Cert Guide: CCNP Security Virtual Private Networks SVPN 300-730 (cisco.com)
- Security Operations Center: Building, Operating, and Maintaining Your SOC (cisco.com)
- Official Cert Guide: CCNA Cyber Ops SECFND 210-250 (cisco.com)
- Complete Video Course: CCNP Security Identity Management SISE 300-715 (livelessons)
- Web Penetration Testing with Kali Linux (packet.net)

RSA®Conference2020 **APJ**

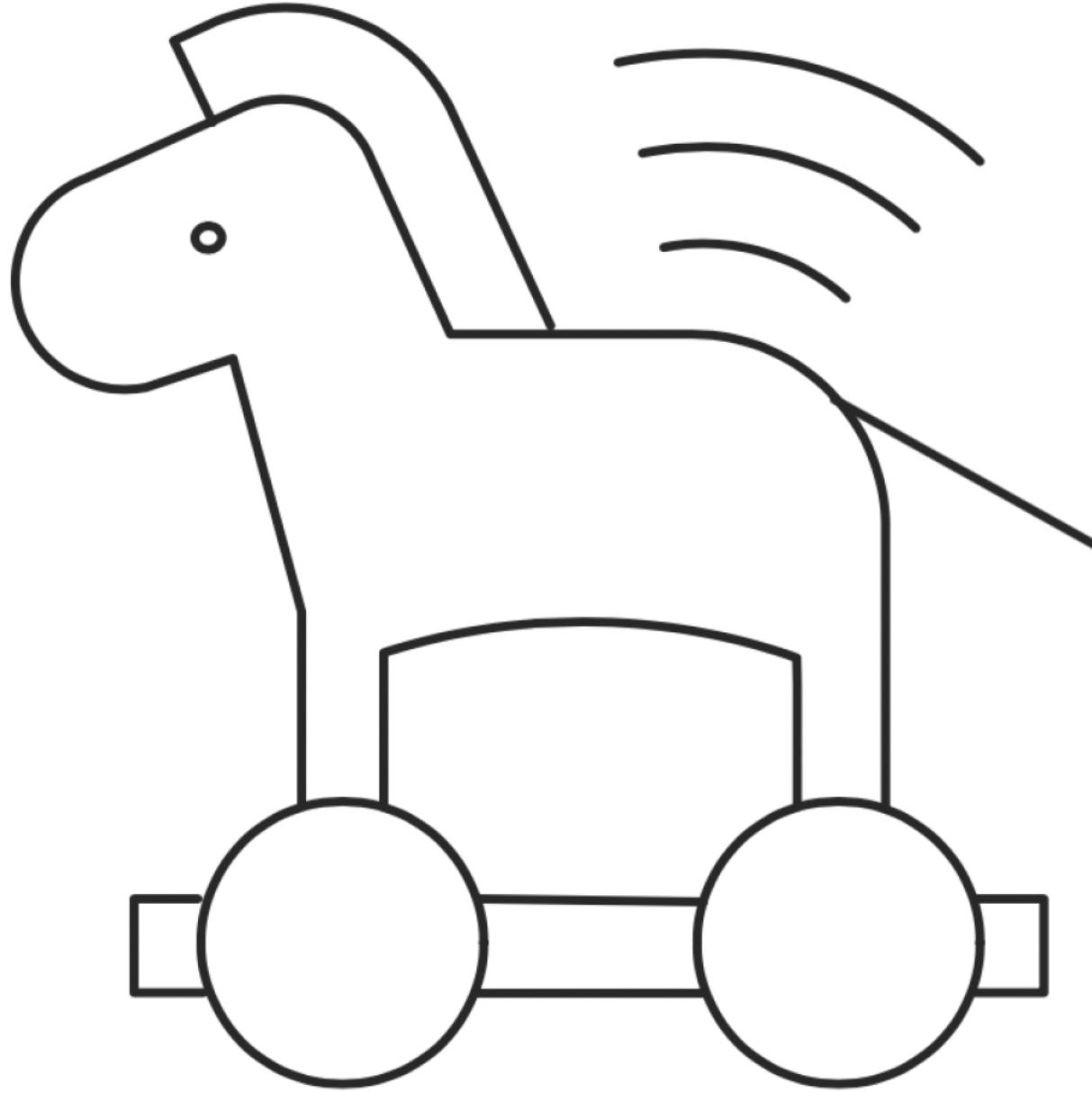
A Virtual Learning Experience

Breach Detection



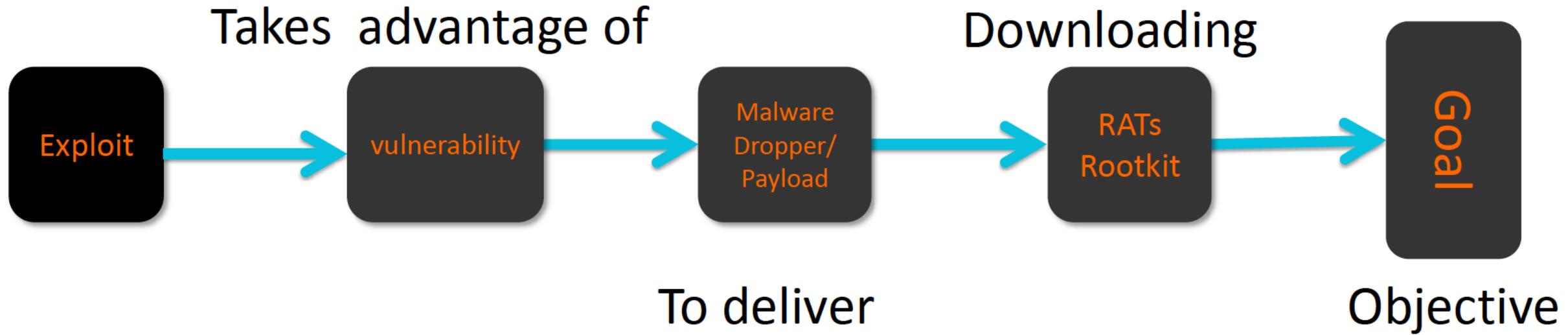


Perimeter-based defense

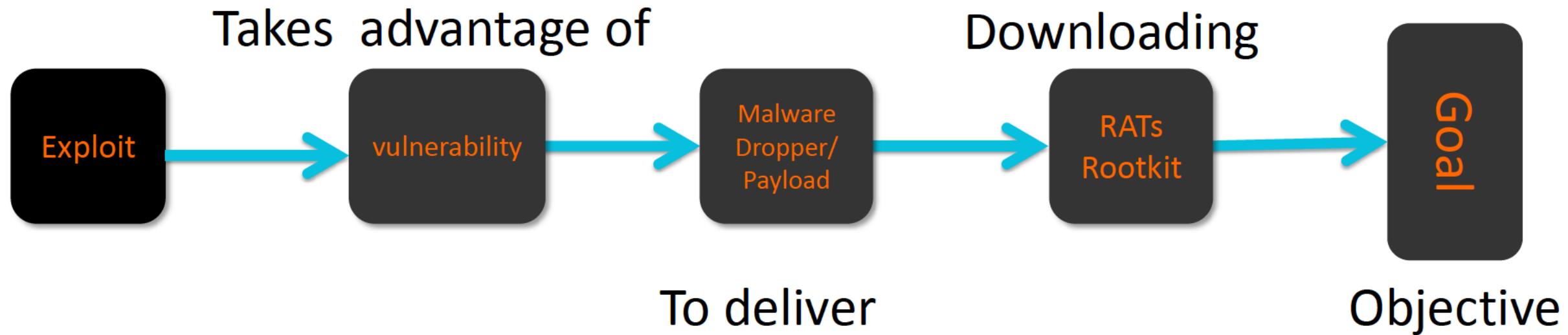


Change tactics, breach from inside

Basic Attack Conept



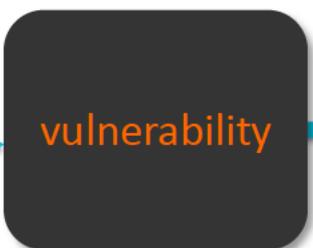
Attack Conept



Attack



Takes advantage of



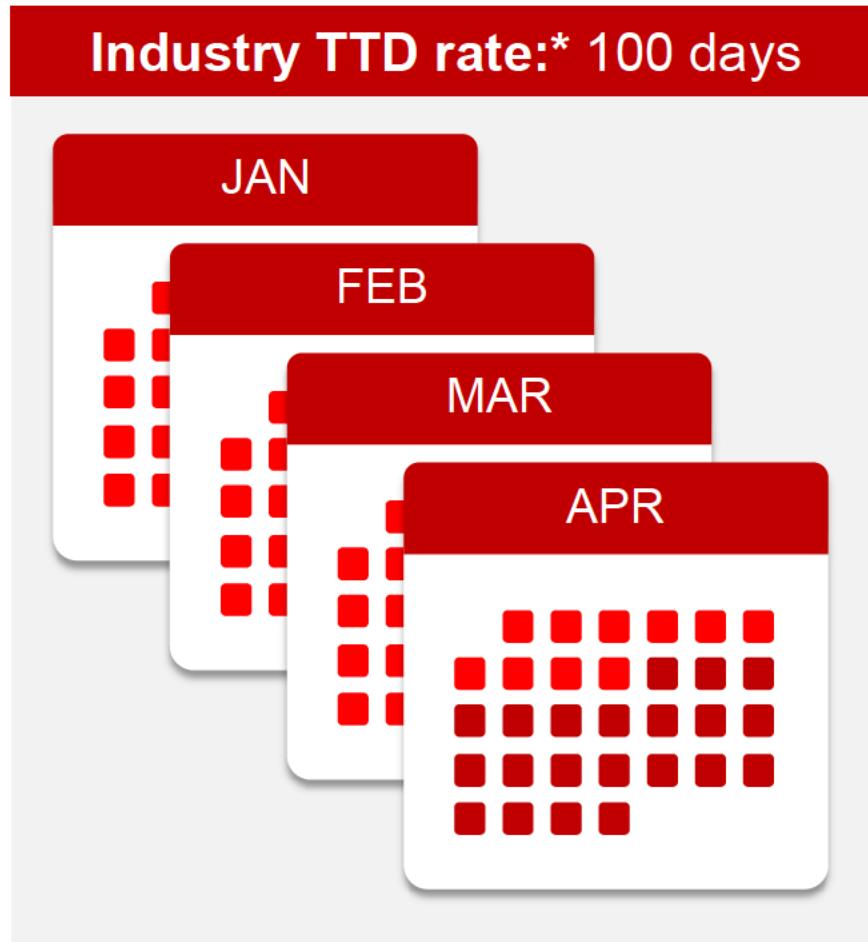
Downloading



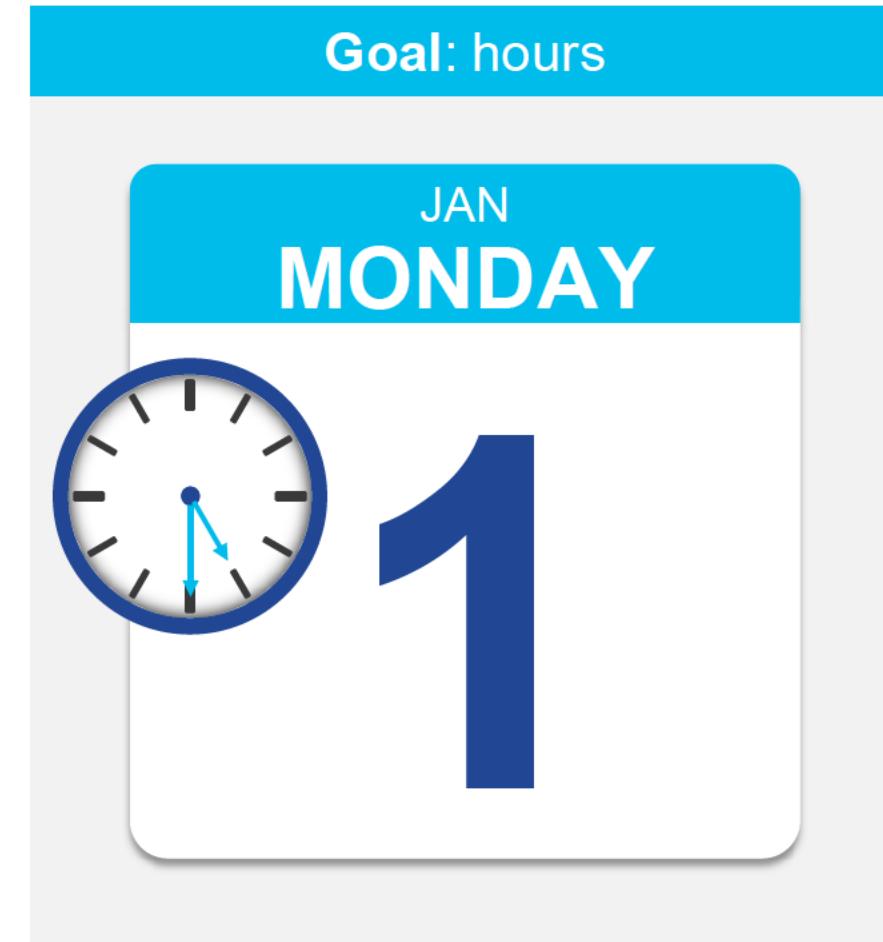
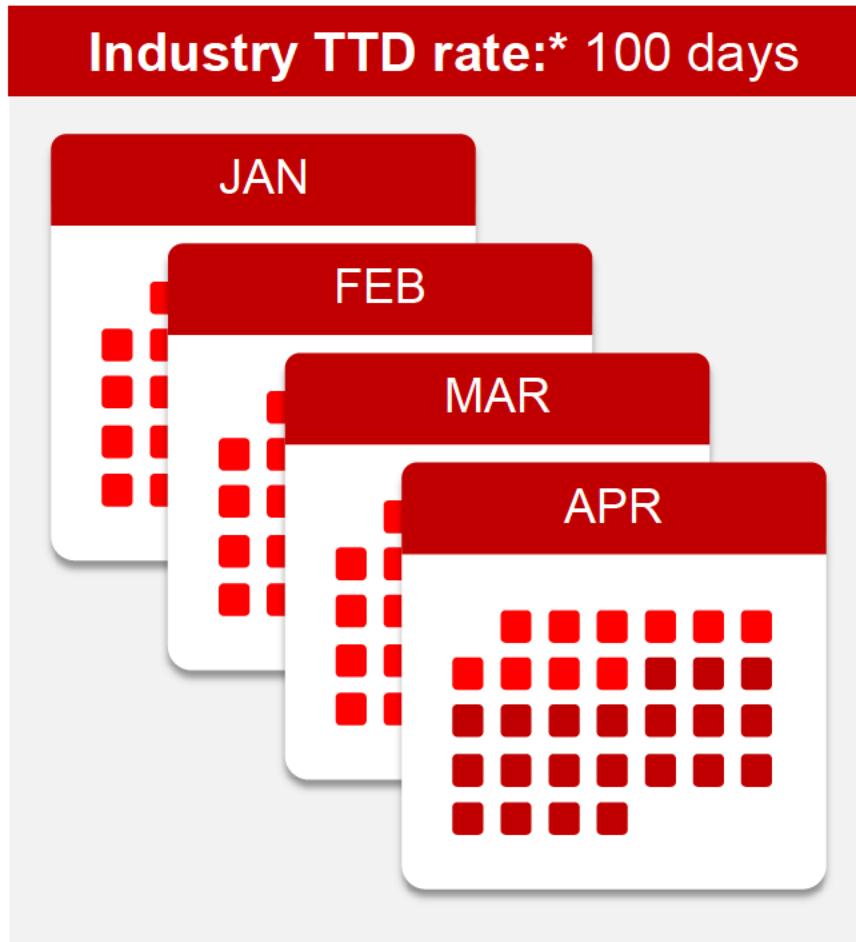
To deliver

Objective

BD Goal = Detect Infections Earlier and Act Faster



BD Goal = Detect Infections Earlier and Act Faster



A surreal illustration depicting a swarm of numerous quadcopter drones flying through a cloudy, grey sky. Each drone has a large, stylized eye on its front-facing propeller hub, giving them a life-like, observational quality. The eyes vary in color, including shades of blue, green, and yellow. The drones are scattered across the frame, some appearing closer and others further away, creating a sense of depth and surveillance.

Recon

Breach Detection Options (NIST / ISO)



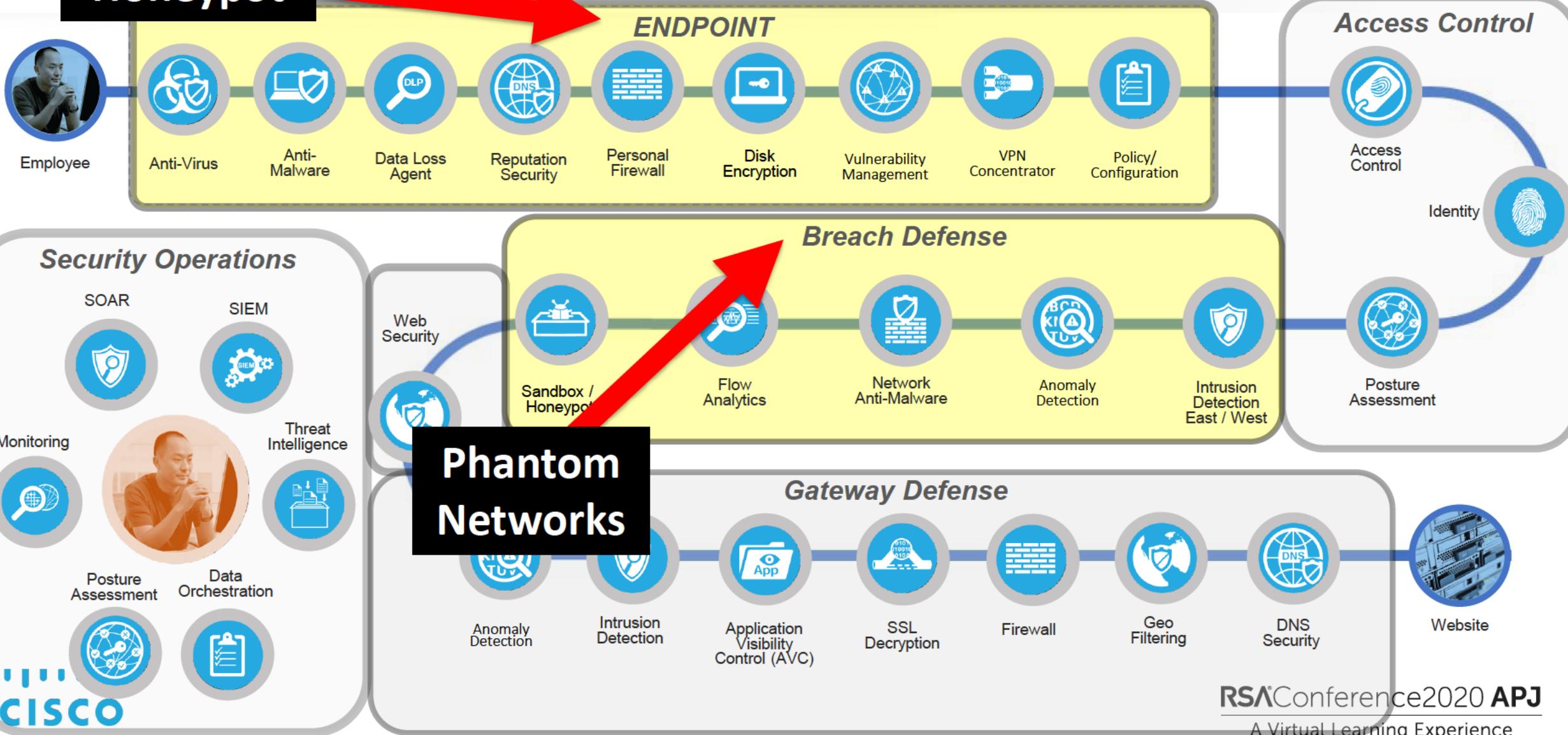
- Honey Pots
- Sandbox
- NetFlow
- IDS/IPS
- Packet Capturing
- Antimalware
- Continuous Monitoring
- Reputation Security



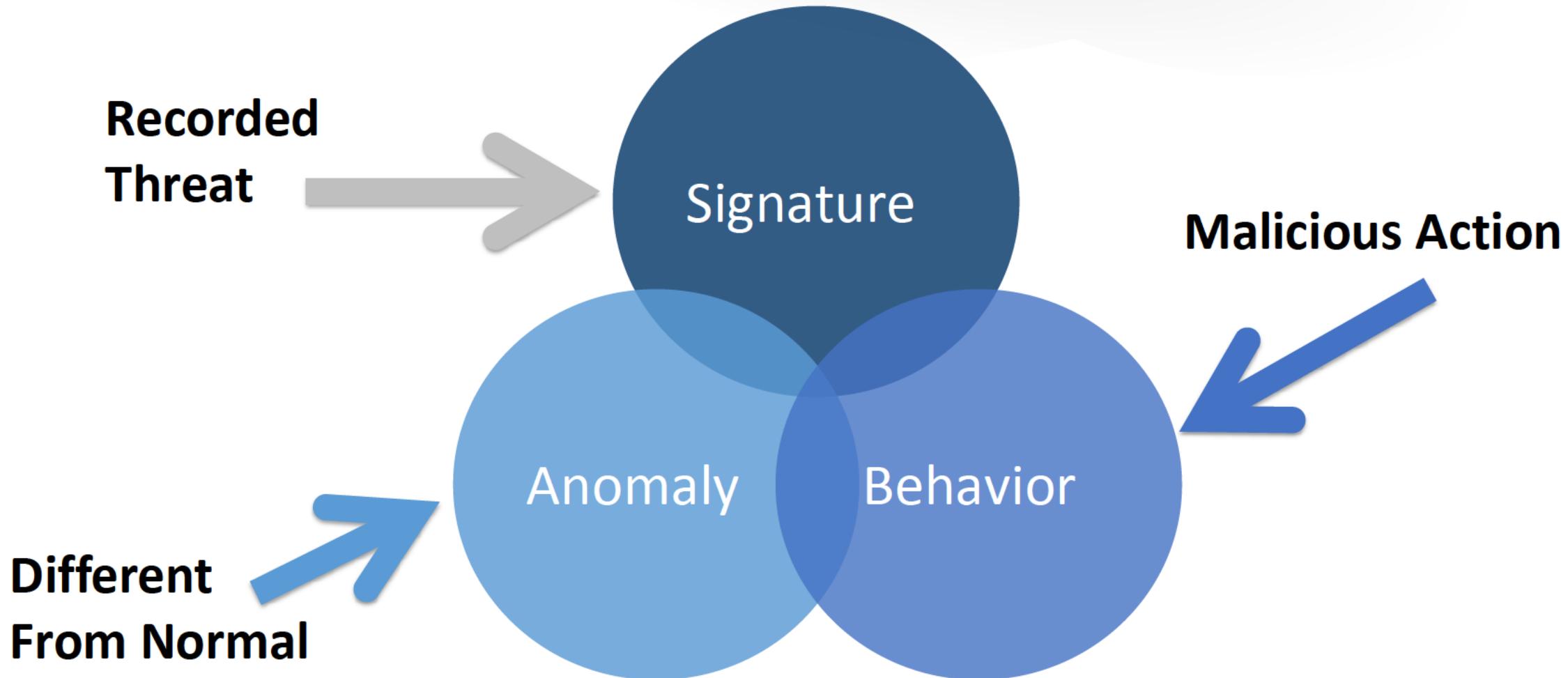
- Network**
- Routers
- Endpoints
- Datacenter
- Cloud
- IoT

Endpoint and Branch Network

Honeypot



Security Capabilities



RSA®Conference2020 **APJ**

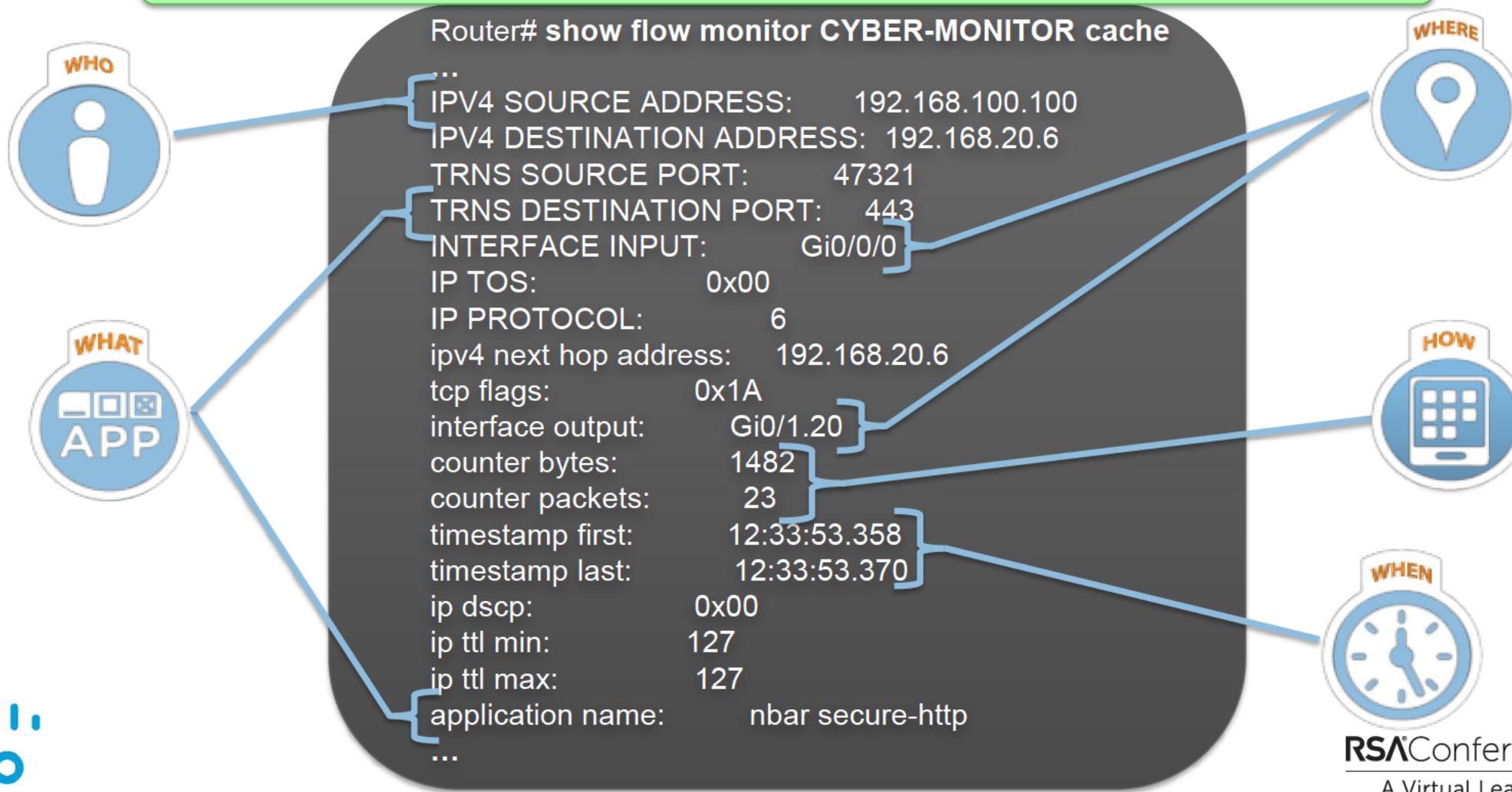
A Virtual Learning Experience

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



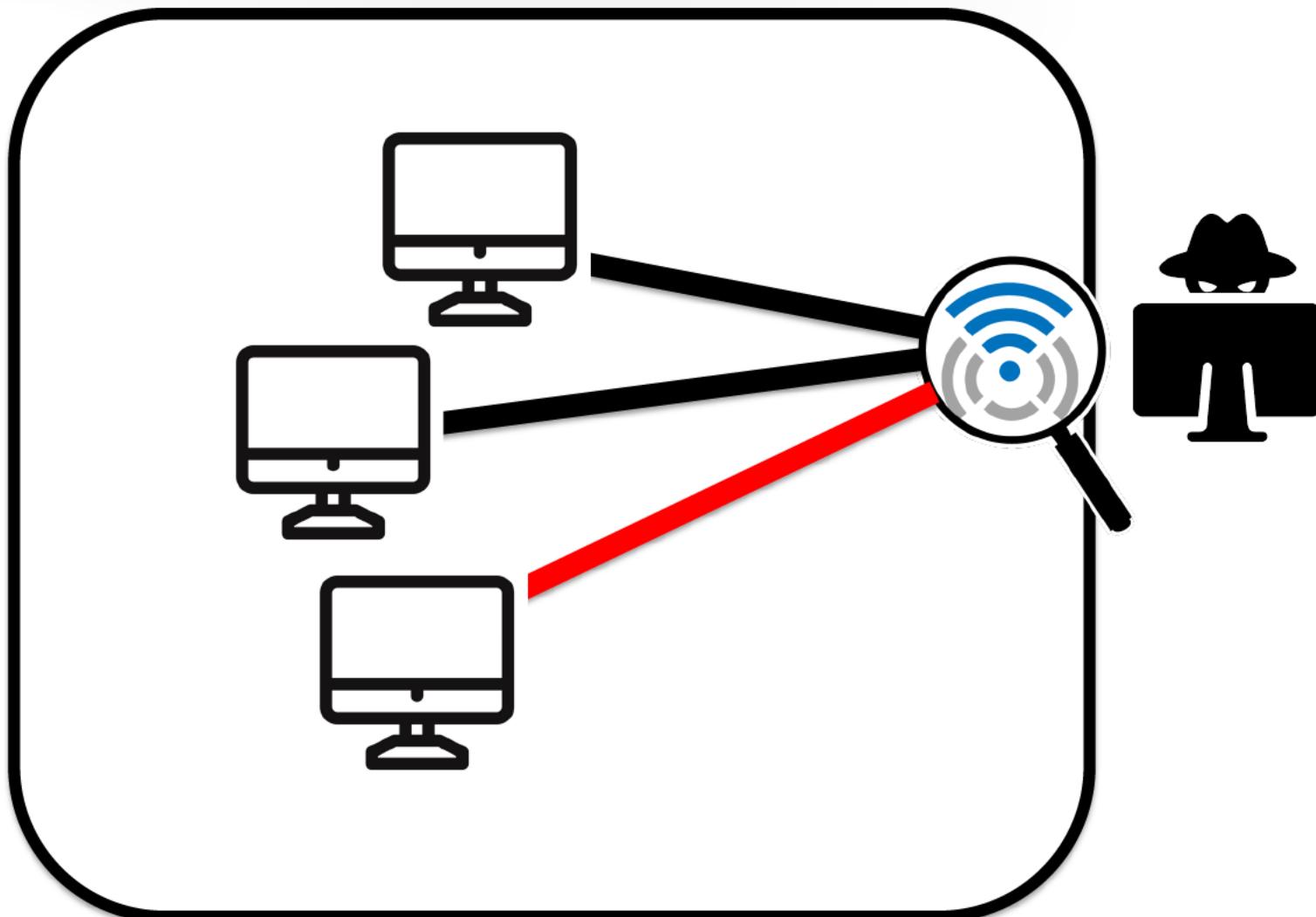
Full NetFlow

- 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
(10.34.100.42)	205,529,732	263% █	

Splunk scanning example which led to breach discovery

New Search

host="198.19.10.6" cat=Recon

Last 24 hours

✓ 464 events (5/12/20 2:00:00,000 PM to 5/13/20 2:13:23,000 PM) No Event Sampling ▾

Job ▾ II III ▾ 1 hour Fast Mode ▾

Events (365) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

May 13, 2020 3:00 AM May 13, 2020 4:00 AM 1 hour

List ▾ ✎ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS
 ↗ cat 1
 ↗ host 1
 ↗ index 1
 ↗ _linecount 1
 ↗ source 1
 ↗ sourcetype 1

i Time Event
 > 5/13/20 3:55:00,000 AM May 13 03:59:00 198.19.10.6 May 13 10:59:00 SMC Stealthwatch[5280]: 51|0x7C|src=198.19.10.15|dst=0.0.0.0|dstPort=[proto]=[msg=Unauthorized, potentially malicious scans using TCP or UDP] are being run against your organization's hosts and may be early indicators of attacks against your network.|fullMessage=Observed 15k points. Policy maximum allows up to 15k points.|start=2020-05-13T10:58:16Z|end=[cat=Recon|alarmID=8P-1FV2-AT0J-ID06-Q|sourceHG=Servers|targetHG=Unknown|sourceHostSnapshot=https://198.19.10.6/lc-lending-page/smc.html#/host/198.19.10.15|targetHostSnapshot=https://198.19.10.6/lc-lending-page/smc.html#/host/0.0.0.0|flowCollectorName={device_na_me}|flowCollectorIP=198.19.10.7|domain=dCloud|exporterName=[exporterIPAddress =|exporterInfo=|targetUser=|targetHostname=|sourceUser=|alarmStatus=ACTIVE|alarmSeverity=Major|cat = Recon | host = 198.19.10.6 | index = main | _linecount = 1 | source = udp:21514 | sourcetype = disco:stealthwatch:alerts | splunk_server = splunk.ed.hackmds.com



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



RSA®Conference2020 **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





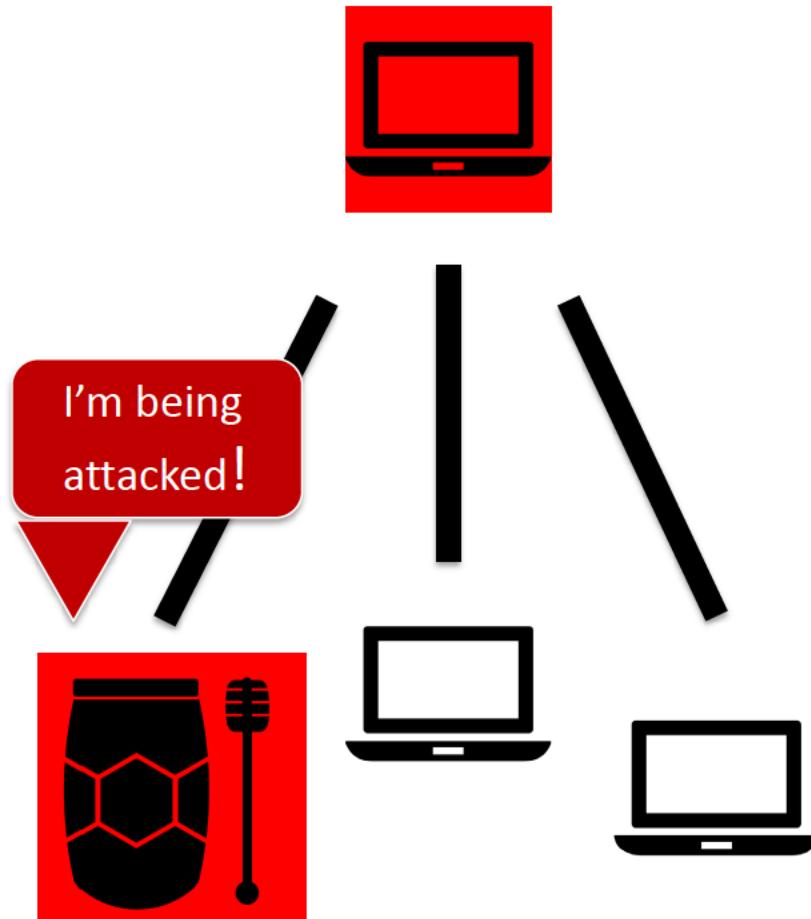
**YouTube
Warning!**

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

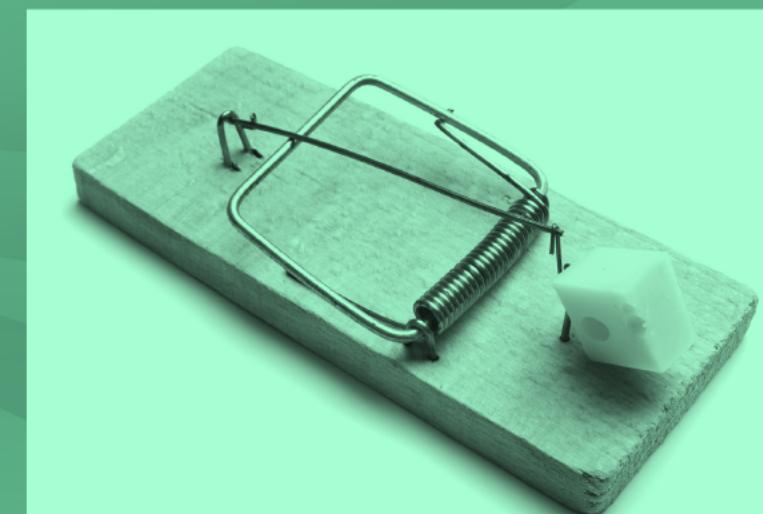
```
Module options (auxiliary/scanner/ssh/detect_kippo) :  
  
Name      Current Setting  Required  Description  
-----  -----  
RHOSTS    [REDACTED].53   yes        The target address range or CIDR identifier  
RPORT     2222            yes        The target port  
THREADS   1               yes        The number of concurrent threads  
  
msf auxiliary(detect_kippo) > run  
  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(detect_kippo) >
```



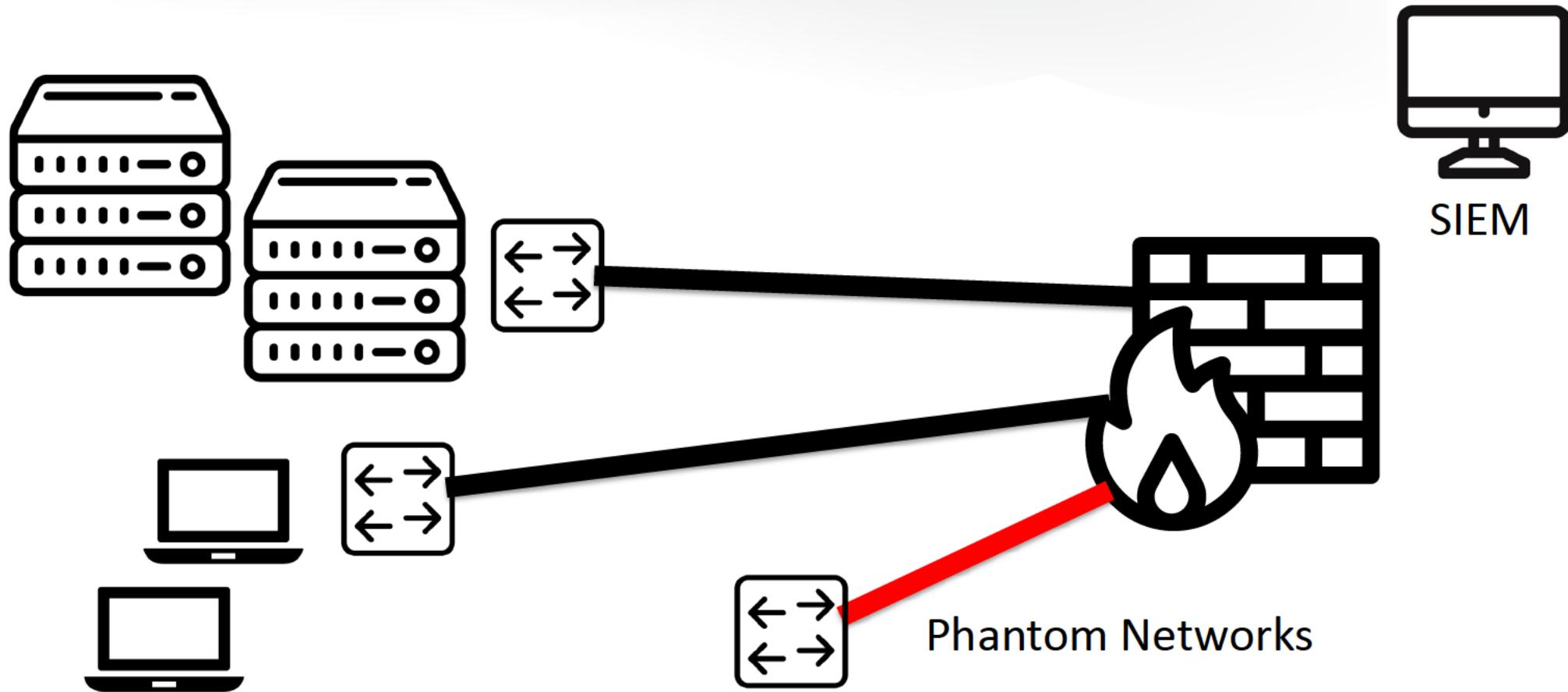
RSA®Conference2020 **APJ**

A Virtual Learning Experience

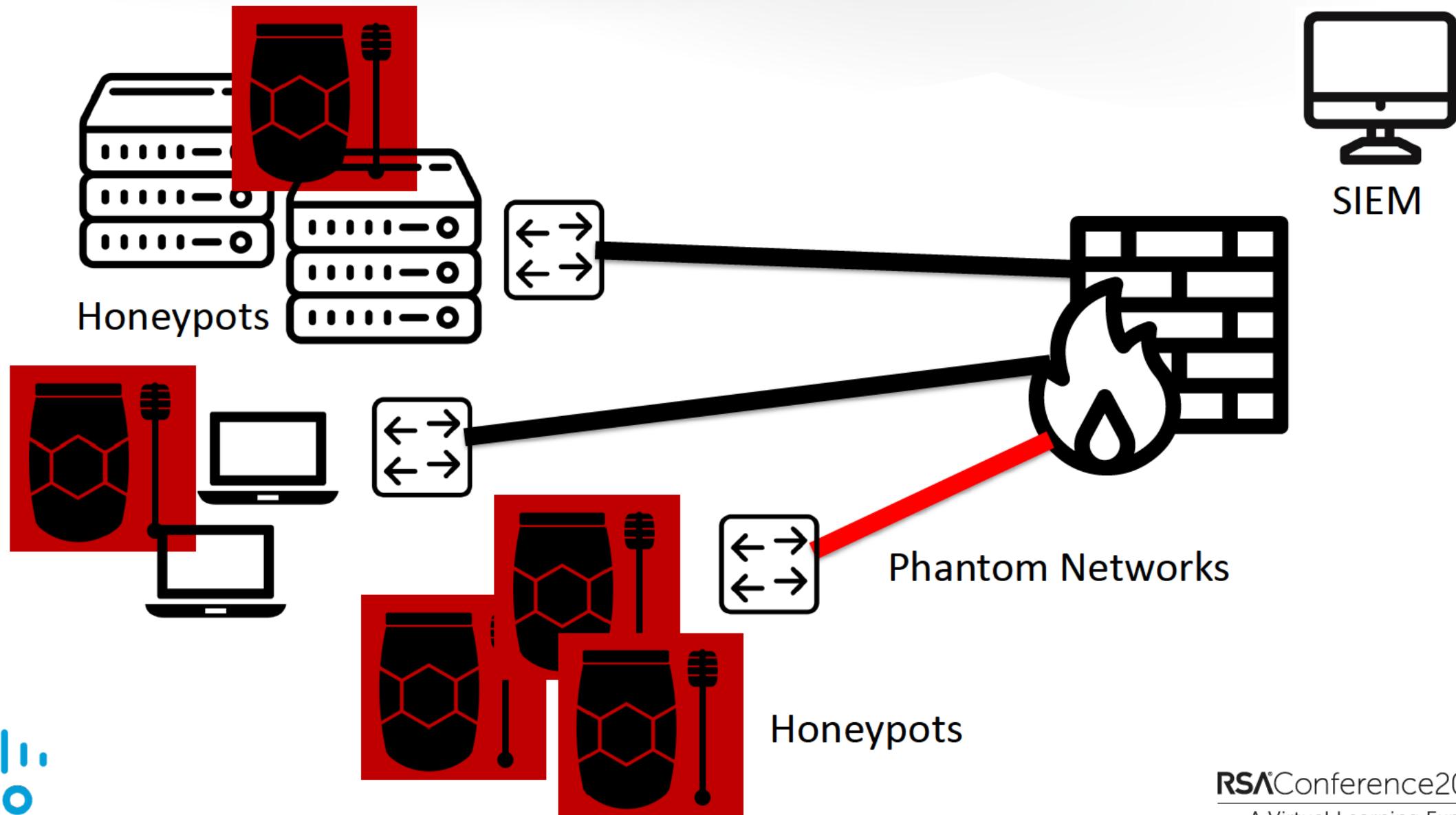
Honey Networks – Total Deception



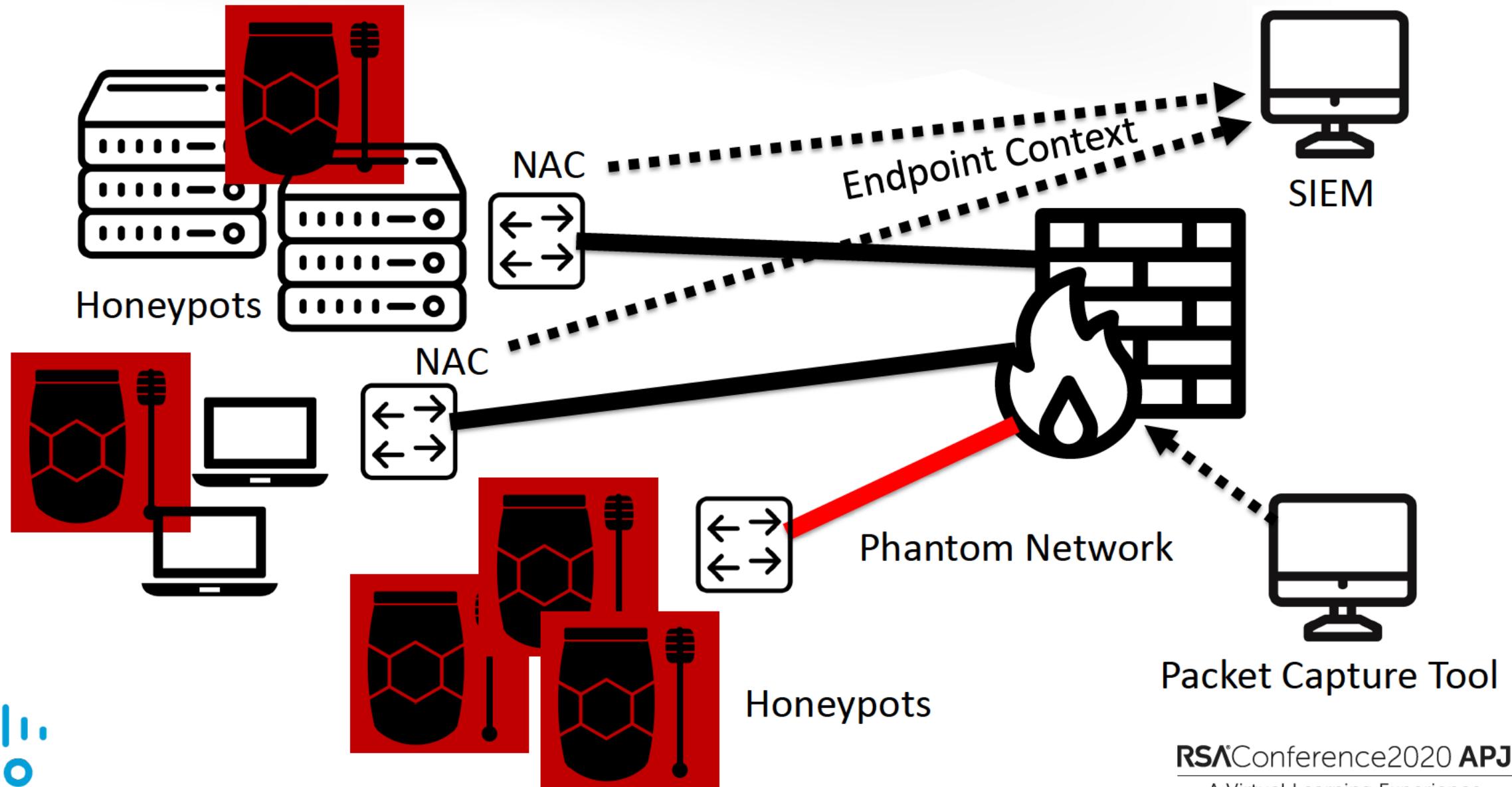
Combine Phantom Networks, Honeypots + Others



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** – Wireshark, LiveAction Omnipacket, 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

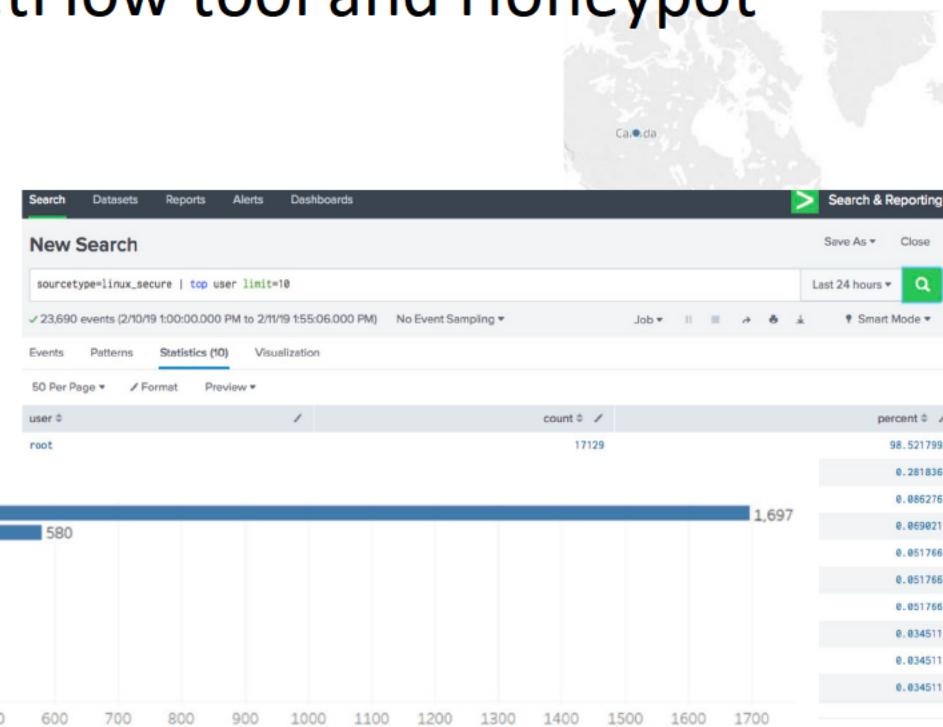
Configure Triggers

- 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

splunk>enterprise App: Cisco Stealthwatch App ▾

Alarm ▾ Monitor ▾ Analyze ▾

New Search

stealthwatch category=Recon cowrie

✓ 59,199 events (before 6/2/2012 12:22:23 000 PM) No Events

Events (59,199) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection

src_ip		
34 Values, 100% of events		
Selected Yes No		
Reports		
Top values	Top values by time	Rare values
Events with this field		
Top 10 Values	Count	%
198.19.10.11	51,644	54.95%
198.19.10.1	20,096	21.382%
198.19.30.102	11,608	12.351%
198.19.28.8	6,234	6.633%
0	1,793	1.908%
198.19.40.51	1,384	1.387%
198.18.133.6	493	0.524%
208.90.58.115	308	0.328%
198.18.133.10	131	0.139%
198.19.30.105	130	0.138%

splunk>enterprise App: Cisco Stealthwatch App ▾

Alarm ▾ Monitor ▾ Analyze ▾

Administrator ▾ Messages ▾ Settings ▾

Alarms

IP Address: Alarm Type: Recon

Submit Hide Filters

Daily Alarm Summary:

Weekly Alarm Summary:

First Active	Alarm	Status	Source IP	Source Hostname	Source Username	Source Host Group(s)
2020-06-02 10:21:07 PDT	Recon	Active	198.19.10.15	splunk.ad.hackeds.com		Inside Hosts/CTR/Servers
2020-06-02 10:01:59 PDT	Recon	Active	198.19.10.3	scanner.ad.hackeds.com		Inside Hosts/CTR/Servers
2020-06-02 09:58:15 PDT	Recon	Active	198.19.30.100	www.ad.hackeds.com		Inside Hosts/CTR/End-User Devices

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!

