RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART2-T02**

Evolving Your Defense: Making Heads or Tails of Threat Actor Trends

Nick Biasini
Cisco Talos

Pierre Cadiex
Senior Manager
Cisco Talos Incident Response

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Speaker Background, Pierre Cadieux

- Leader of the global Incident Response service of Cisco Talos.
- Professional consultant for the past ten years after first starting his career as an Information Security executive in the financial services, technology, and pharmaceutical industries.
- Los Angeles, CA USA

Speaker Background, Nick Biasini

- Threat Researcher
- Seven years at Talos,
  15+ in the industry.
- Recovering SOC Analyst.
- Research focus is Crimeware including exploit kits.
- Austin, TX USA

RSAConference2022

Why are we here?

Threat Actors & Environments are Changing

Discuss broadly how the threat landscape has changed

- Nation States
- Big Game Hunting
- Vulnerability Access

Discuss how environments are changing

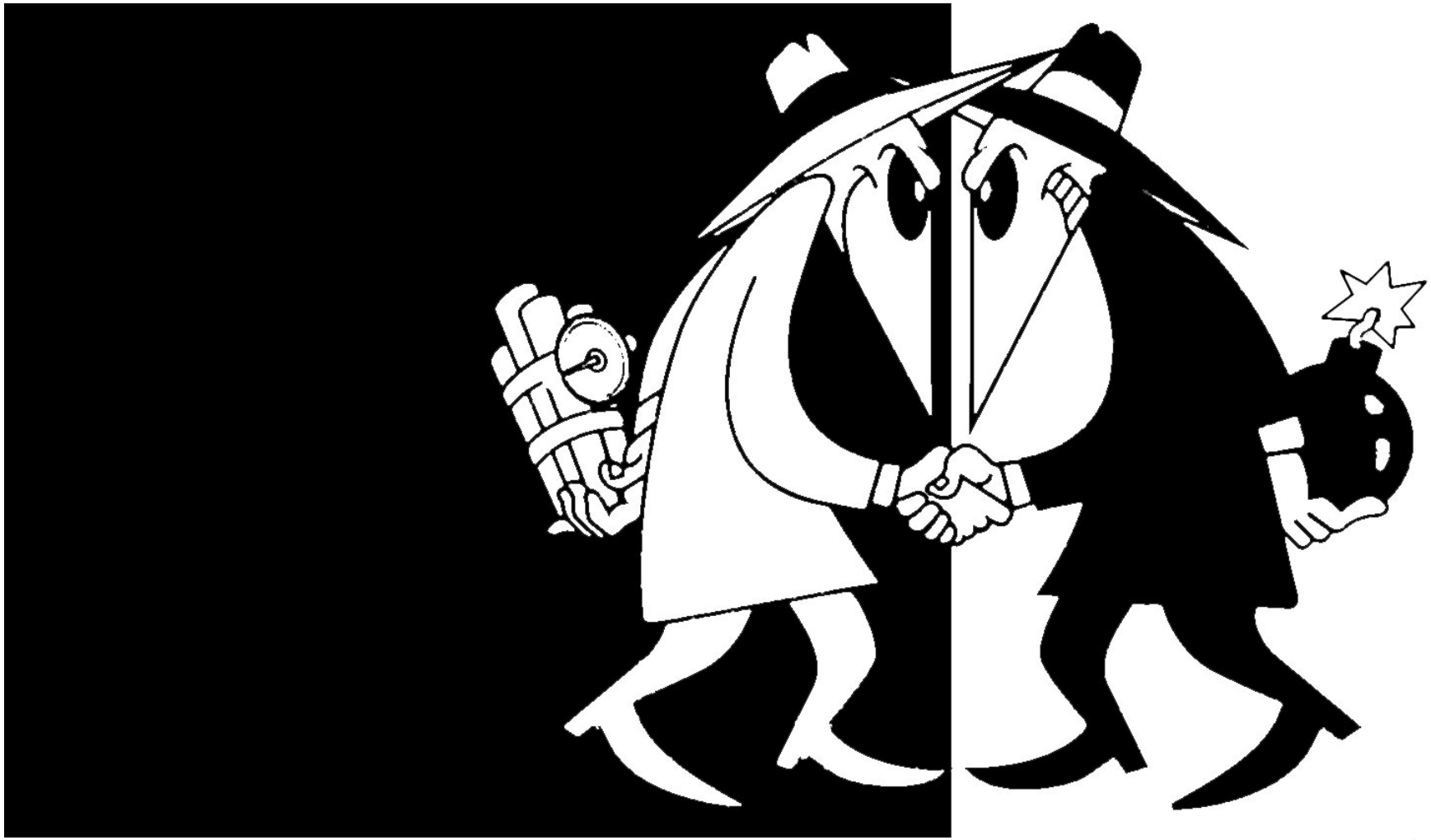
- Hybrid Work
- Trust Abuse
- Increased Attack Surface

RSAConference2022

Let’s Start with Trends

Looking back and looking forward

Nation State Activity Historically



Moonlight Maze

Description

- Advanced Actor associated with a Nation State
- Long running espionage campaign
- Targeted Government, Military, and Higher Ed.

Tools

- Attacked known unpatched vulnerabilities
- Hid activities using proxies
- Gathered and Exfiltrated huge amounts of data

Tactics

- Exploited known vulns
- Used proxied connections through innocuous networks including Universities
- Evaded detection for years

Processes

- Searched, obtained, and exfiltrated sensitive documents
- Thought to have stolen thousands or more documents

Operation Aurora

Description

- Advanced Actor associated with a Nation State
- Targeted Private Companies (Primarily Tech)
- Primary goal was to obtain information on persons of interest & IP

Tools

- Leveraged Zero-Days in Internet Explorer & Adobe Reader
- Delivered Custom Tools
- Data Exfiltration

Tactics

- Leveraged zero-days
- Targeted Private Industry
- Dissident Data & Source Code Targeted

Processes

- Compromised via Internet Explorer or Adobe Reader Zero-Day
- Goal was exfiltration of information and other IP

Section on current APT activity

- Cover series of examples highlighting the escalating activity of nation states.

- **Topics covered will include:**
  - Software Supply Chain
  - Zero-Day
  - Service Supply Chain
  - Mobile Targeting
  - Exploit availability

RSAConference2022

Software Supply Chain Attacks

Not Petya

Description

- Advanced Actor associated with a Nation State
- Destructive Attack Masquerading as Ransomware
- Most Expensive Incident in History

Tools

- Wormable Ransomware
- Designed to Spread Internally Not Externally
- Leveraged Eternal Blue / Eternal Romance and Admin Tools (WMI/PSExec)

Tactics

- Supply chain and victim to victim pivoting
- Rapid Infection Spread
- Destroyed Countless Systems / Networks

Processes

- Designed to inflict damage as quickly and effectively as possible.
- Appears to be Ransomware, but is purely destructive

C Cleaner

Description

- Advanced Actor associated with a Nation State
- Has the ability to run long and complex operations focused on IP level theft

Tools

- Software Supply Chain
- DGA Based C2
- Wide net cast to compromise small pool of companies
- Focused on tech companies

Tactics

- Supply chain and victim to victim pivoting
- Low and slow internal recon
- Complex multi-stage attacks

Processes

- Highly targeted victim identification though data mining
- Focused on stealth, in it for the long game

RSAConference2022

Targeting Starts to Shift

Olympic Destroyer

Description

- Targeted Korean Olympics
- Attributed to different nation states at different times
- Attempted attribution misdirection

Tools

- PSEXEC / WMI / Creds stealer / Browser stealer
- Use windows systems tools for most actions
- Mimikatz and Credential stealers
- Hot Patched Gathered Credentials

Tactics

- Self Propagating Wiper
- Lateral movement using WMI and PSEXEC
- Automated lateral movement using stolen creds

Processes

- Steals credentials and moves laterally
- Focused and targeted attack for political gain

VPN Filter / Cyclops Blink

Description

- Edge Device Botnet
- Attributed to Russia
- Infected over 500K devices

Tools

- Custom built bot framework
- Module architecture for updates
- Rather complex C2 and Stage 1, 2, 3 chain

Tactics

- Targets edge devices
- Redirects and modifies network traffic
- Pivot functional to get to end hosts and lateral movement

Processes

- Get everything, find interesting
- Pivot and hold

HermeticWiper/CaddyWiper/DoubleZero

Description

- Wipers Deployed as part of Ukranian invasion by Russia
- Wide variety of wipers deployed into environments.

Tools

- Designed to destroy data quickly
- Using various types of mechanisms to destroy data
- Allegedly, deployed using GPO

Tactics

- Varying techniques for wiping
- Made use of embedded drivers
- Designed to destroy systems methodically
- Exited if found running on Domain Controller

Processes

- Designed to inflict damage as quickly and effectively as possible.
- Didn’t have internal spreading mechanism (except for HermeticWizard)

RSAConference2022

Escalations Continue

Sea Turtle

Description

- Advanced Actor associated with a Nation State
- Targeted DNS infrastructure

Tools

- Attacked Registrants
- DNS Hijacking
- Modified records to point to actor owned servers

Tactics

- Service based supply chain attack
- Attacked Registrants and Registries
- Used to gain credentials for further espionage activities

Processes

- Targeted DNS infrastructure
- Allowed impersonation of several key government related sites

Solar Winds

Description

- Advanced Actor associated with a Nation State
- Affected thousands of customers and targeted Government Agencies and private companies

Tools

- Supply Chain Attack
- Long running campaign
- Used to obtain SAML tokens

Tactics

- Software supply chain attack
- SAML Tokens targeted
- Exploited monitoring/administration software

Processes

- Designed to evade detection for long time
- Resulted in significant compromise across industries

Hafnium / Exchange Vulnerabilities

Description

- Advanced Actor associated with a Nation State
- Affected thousands of customers
- Typical Nation State activity combined with criminal element

Tools

- RCE Vulnerability in MS Exchange
- Commonly used to deploy webshells and steal mailbox data

Tactics

- 0-Day Exploitation initially
- Spread quickly to criminal elements
- Clouds attribution

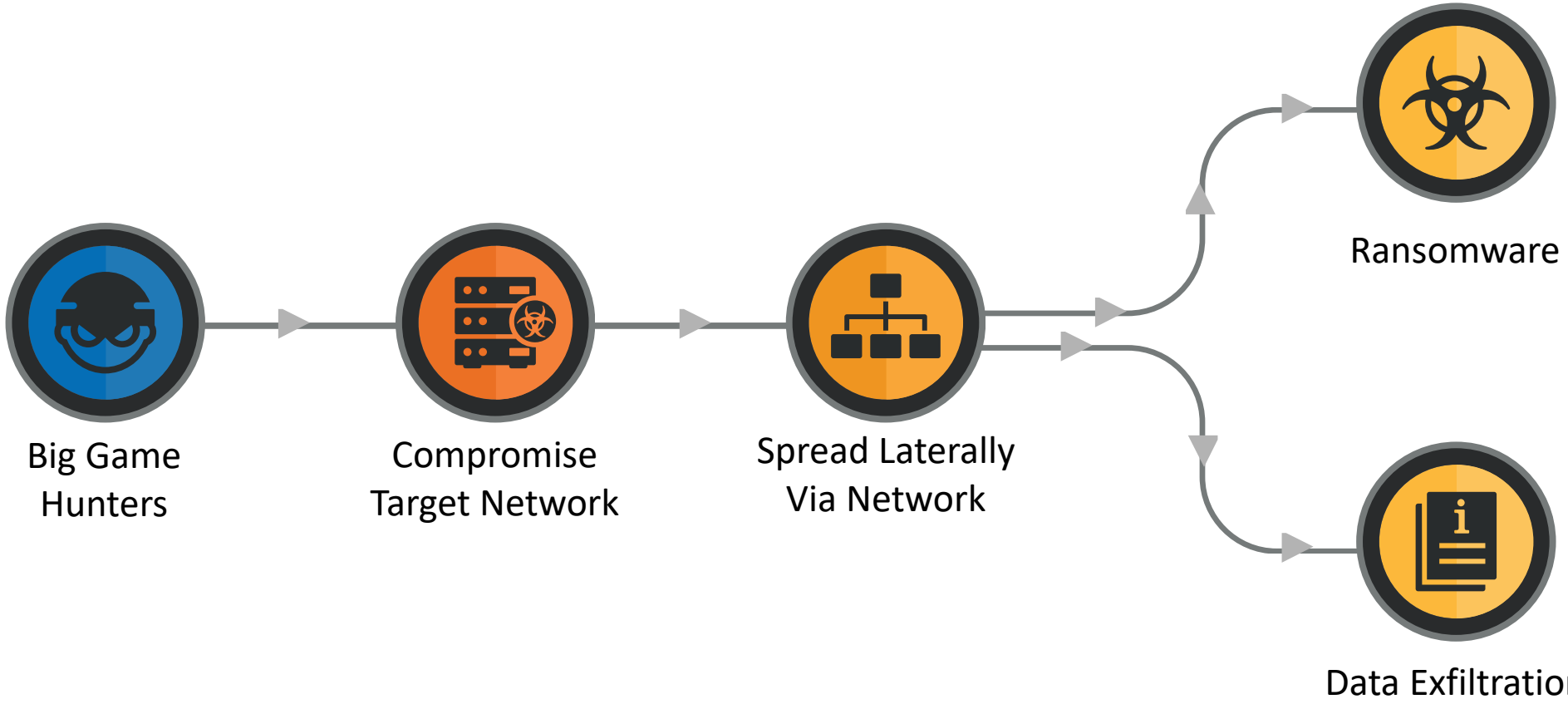
Processes

- Use of 0-day to compromise Exchange servers.
- Can be used for ongoing espionage and immediate information retrieval
- Once criminals get involved it is difficult differentiate

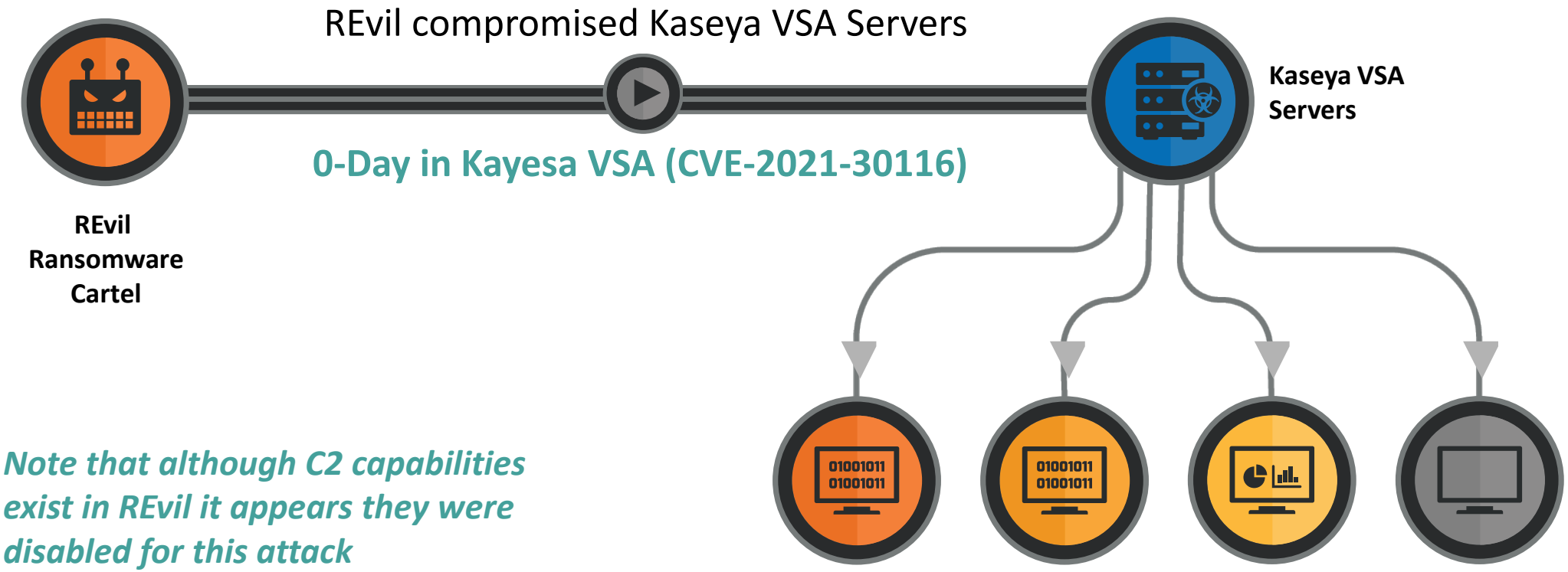
RSAConference2022

Ransomware Cartels

Big Game Hunting



Kaseya Overview



Note that although C2 capabilities exist in REvil it appears they were disabled for this attack

Summary

- Key things Nation States and sophisticated actors are targeting
  - Trust
  - Remote Access
  - Supply Chain
  - Weaponized Exploit Markets
  - Critical Infrastructure
  - Foundations of Internet

RSAConference2022

Lessons Learned

Insights from our work in the field

RSAConference2022

Essential controls (the basics)

Summary

- Talos has identified a number of basic controls that are applicable to the majority of incidents that we have responded to.
- In August 2021 Talos was also able to further validate these approaches due to the leaked ransomware playbook used by the Conti ransomware group

- Implement MFA
- Centralized logging
- Limit Windows tools to trusted accounts
- Network Segmentation
- Patch/Remediate vulnerable systems and software

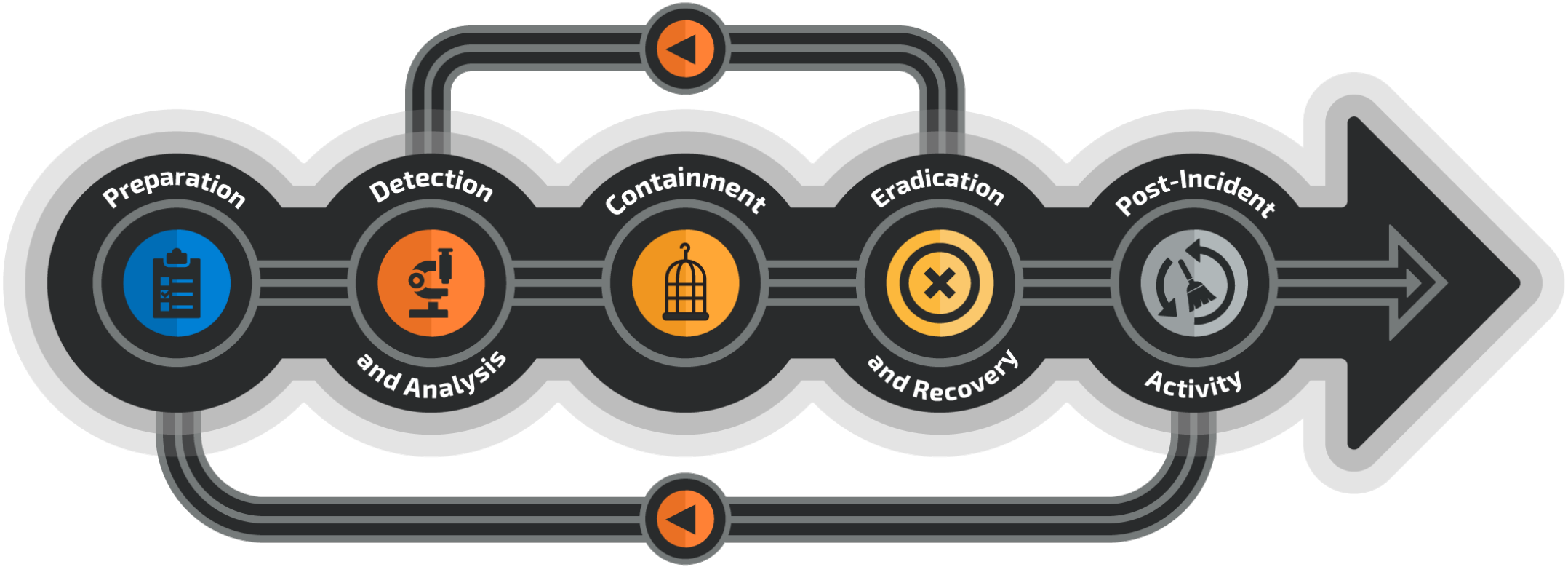
RSAConference2022

Creating a Defender-Friendly Infrastructure

Creating a Defender-Friendly Infrastructure

1. Develop your environment to allow for response
2. Understand your assets, risks and blind spots
3. Know where your logs are retained, how to access them, and how long they are retained
4. Know how to deploy tools rapidly and the impact and processes involved

Incident Response Process



Preparation

- Understand what questions you will need to answer, in the event of an incident or investigation

- Plan for how to access, preserve, analyze, and draw conclusions from your evidence
- Test and practice

- Validate and update processes such as containment and remediation strategies

- **Goal:** Have tools, knowledge and skills ready to act upon the event of an incident.

Detection and Analysis

- Plan for comprehensive monitoring, prioritizing known attack methods and critical systems

- Create and test the triage and escalation process, what information is needed to escalate, who should receive the escalation?

- Define what role can declare an incident, and what that entails

- **Collect and archive data that might be related to the situation**
  - Network logs
  - Endpoint logs
  - System events
  - Scheduled tasks
  - Security software events
  - Disks images
  - Memory captures

Containment

- Understand your assets, what function they provide, and their criticality - So you understand the impact of containment

- Develop multiple methods for containment, your first option may not work or may not be available

- Consider automated containment methods for very high-fidelity alerts or critical alerts

- **Can the incident be isolated?**
  - If the incident can be isolated, what steps will be taken to isolate?
  - If not, work with the owners to resolve the problem.
  - Are the affected systems isolated from non-affected systems?

Containment

- Understand how to manage enterprise-wide password resets, including across service accounts
- Determine what criteria would be needed to remove a device from containment
- Plan for deployment of enterprise settings or control changes, which are often needed to complete containment

- Have backups been created to protect critical data?
- Have copies of infected machines been made for forensic analysis?

Eradication and Recovery

- Prepare for methods of conducting enterprise-wide eradication steps
- Establish what your risk threshold is for rebuilding or attempting to recover a compromised system
- Understand how your backup infrastructure works, how frequent backups are captured, and what the process is for restoration

- Remove malicious software
- Deny the adversary access to the environment
- Remove/remediate known entry points
- Remove the presence of the adversary from the environment

Post Incident Activity

- Capture recommendations and track these as projects
- Hold an internal debrief to review the lessons learned and action items
- Document any process improvements needed, based on the lessons learned, test new controls and optimizations

- Capture recommendations to prevent future threats
- Analysis of the incident and overall actions
- Identify areas of weakness

Summary

Consider the threats that you are concerned about – how would you respond to an attack using those TTPs?

- Do you know what questions to ask?
- Do you have the logs or the telemetry to answer the questions?

Preparing for Defense

Initial Access

- Email inspection
- Log retention
- Monitoring
- Alerting

User Actions

- DNS Logs
- Netflow
- Endpoint security solution
- SYSMON
- PowerShell logging

Account Compromise

- MFA
- Authentication events
- Creation or modification of groups

Privilege Escalation

- Microsoft LAPS
- Monitor privileged accounts
- Alert on GPO modification

Lateral Movement

- Network segmentation
- Remove or restrict SMB
- Monitor for unexpected traffic

Encryption of data

- Ensure critical data is backed up regularly
- Secure backups
- Test data restore process

RSAConference2022

How do we evolve defenses

Things are escalating how do we stay secure??

Test and improve

Perform periodic tabletop tests using either recent incidents that your team has handled or recent incidents from the news or other sources to test your team.

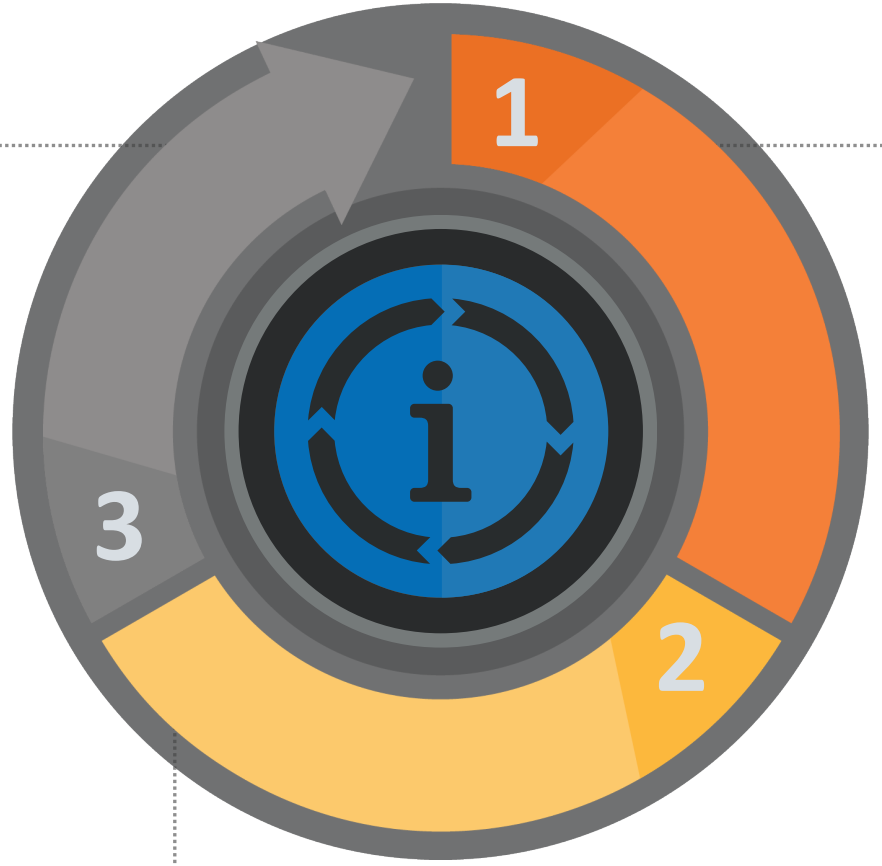
Are there different tools, capabilities, or telemetry you require to have a successful outcome?

Does your IR Plan cover all of what you need to be successful for this specific type of incident?

Much better to find out during a scheduled test vs. during an incident

Do you have the right team members or roles identified to address the issues or risks with this type of incident?

Apply Intelligence



- Develop alerts and detections based on information from reputable threat intelligence sources.
- When there are new tools, attack methods, or techniques, verify that your team captures the logs that are needed to detect and investigation these threats.

Train the team on what these alerts mean and how to handle them, update playbooks and IR plans as needed

Use tools like the Mitre ATT&CK matrix and navigator to better understand current techniques, detection opportunities, and mitigations

Stay Connected and Up To Date

Spreading security news, updates, and other information to the public.

White papers, articles & other information
talosintelligence.com

ThreatSource Newsletter
cs.co/TalosUpdate

Talos Blog
blog.talosintelligence.com

Social Media Posts
Twitter: @talossecurity

Instructional Videos
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity