THROUGH THE EYES OF THE ADVERSARY

THE SYNTHESIS OF THREAT INTELLIGENCE & THREAT HUNTING OPERATIONS

SPEAKER

JEN AYERS

VP, OverWatch and Security Response

- Over 20 years of cybersecurity experience
- Serves more than 20% of the Fortune 500
- Multiple roles both as a service provider as well as working in industry

SPEAKER

JASON RIVERA

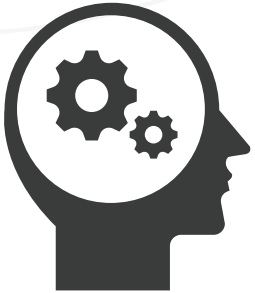
Director: Global Threat Intelligence Advisors

- 13+ years experience in threat intelligence
- Experience building threat intel programs for Fortune 500 companies and large government agencies.
- Former US Army Intelligence Officer at NSA & US Cyber Command

EXECUTIVE SUMMARY

THE CHALLENGE

On the other side of the most advanced attacks are intelligent, motivated, and highly capable human beings

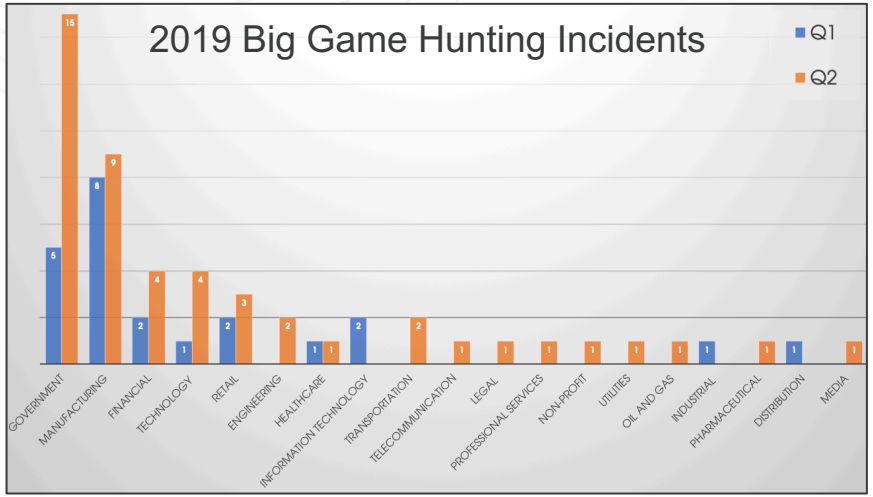


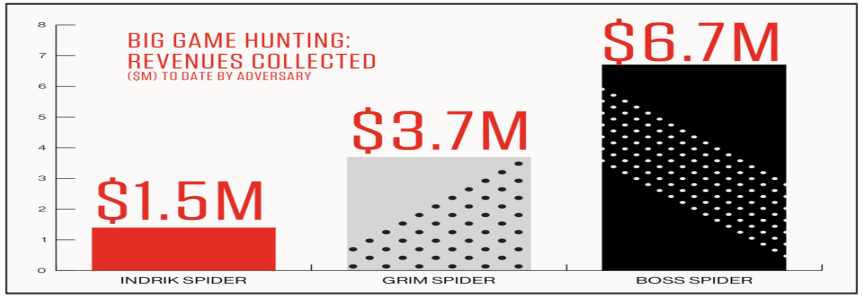
The adversary is intelligent enough to estimate your defenses and to creatively conceive of ways to bypass them

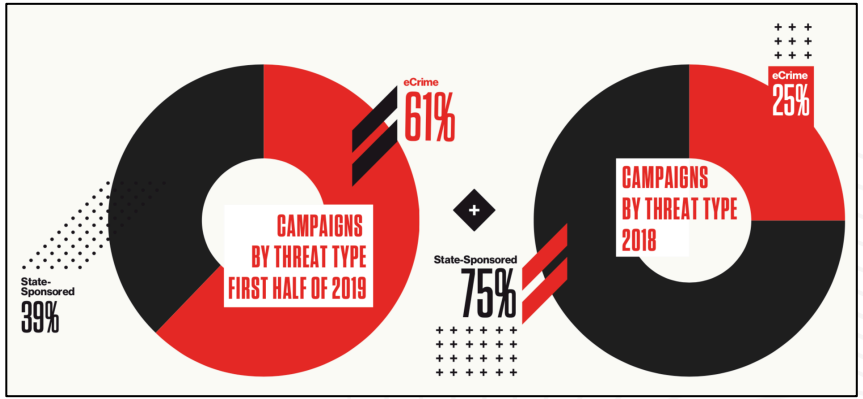
The adversary is sufficiently motivated, either financially, ideologically, or by nationalism, and is willing to do what it takes to achieve their objectives

The adversary is highly capable, and has a wealth of tools, personnel, experience & resources at their disposal

THE ADVERSARY IS SUCCEEDING AT HIGHER RATES THAN EVER BEFORE







FALCON

KEY OBSERVATIONS

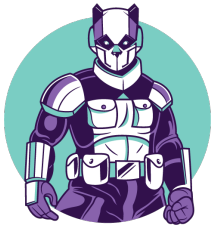
OBSERVATION 1

Flexibility & Creativity

WICKED SPIDER

Target: Financial

Technique: Remote RDP login with **stolen credentials.** Establish foothold



WICKED PANDA

Target: Telecom

Technique: Use **common Microsoft admin tools** to download implants, bypassing detection

VELVET CHOLLIMA

Target: Academic

Technique: **Spearphishing** to deliver malicious Chrome extensions

CLOCKWORK SPIDER

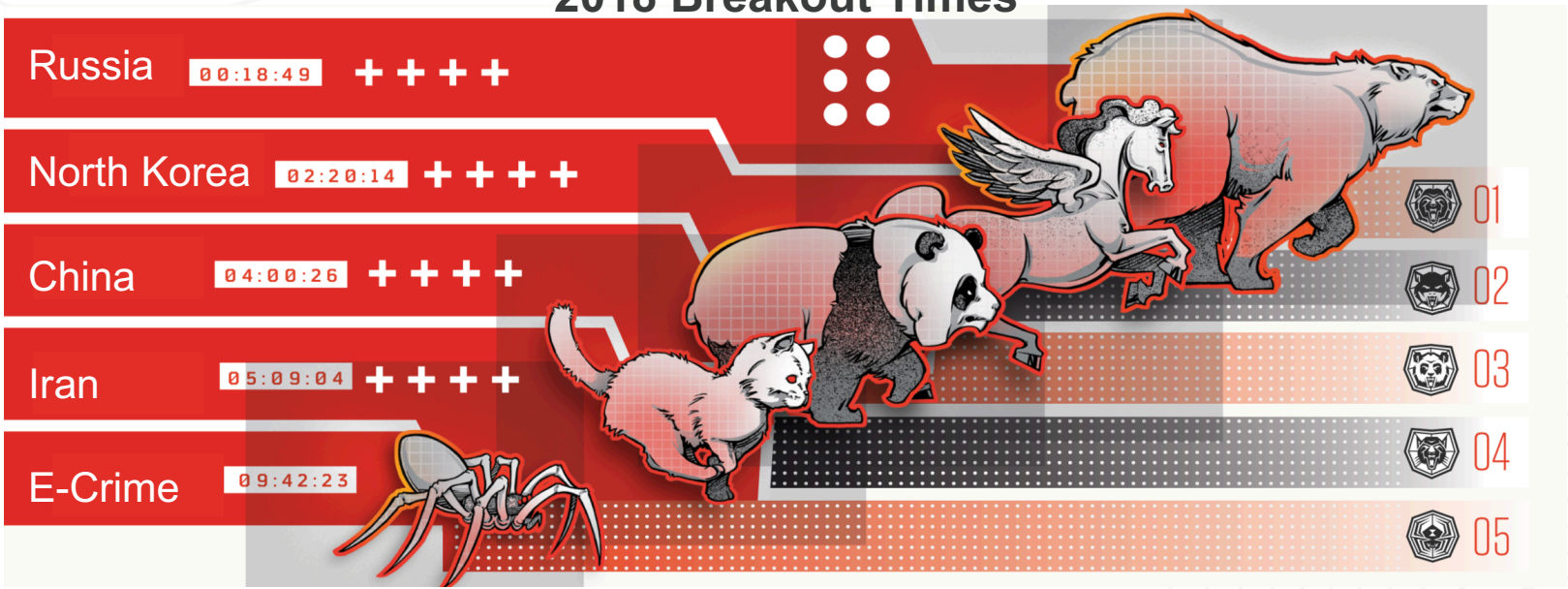
Target: Opportunistic

Technique: Install **custom root certificate** on victim to support man-in-the-middle network monitoring

OBSERVATION 2

Speed & Agility

2018 Breakout Times



FALCON

HOW TO SEE THROUGH THE EYES OF THE ADVERSARY

FALCON

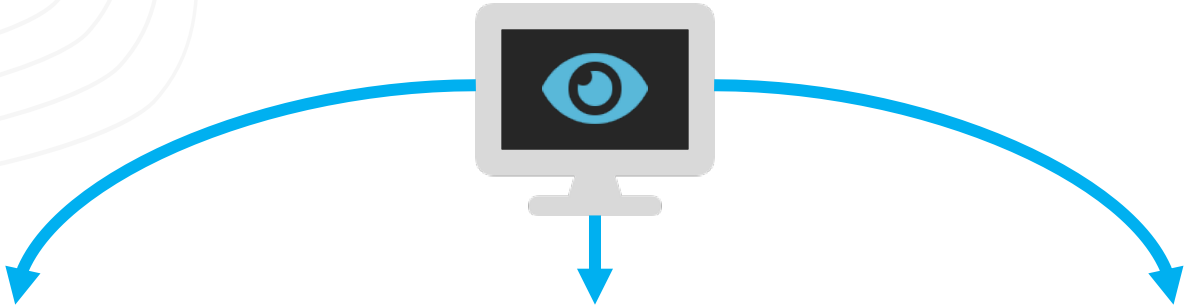
SO… WHAT IS AN “ADVERSARY”?

The adversary is a person or group of people who seek to harm our interests.

Ourselves

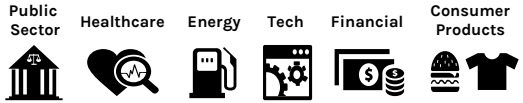
The Adversary

HOW CAN WE CONCEIVE OF OURSELVES?



Strategic

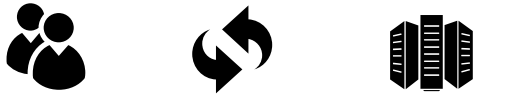
Industry



What things of value do you have that the adversary wants to target?

Operational

Critical Assets



What people, processes, and technologies will the adversary target?

Tactical

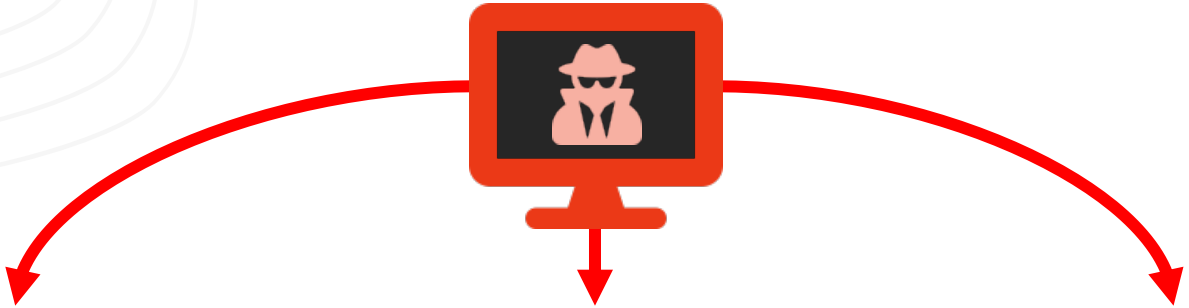
Access Vectors

	Physical		Human		Digital
	Supply Chain		Social Engineering		Internal to Network
	Comms Infrastructure		Coercion		External to Network
	Close Access		Business Transaction		Lateral Movement

How will the adversary gain entry into your organization?

FALCON

HOW CAN WE CONCEIVE OF THE ADVERSARY?



Strategic

Motive

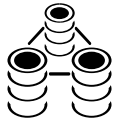
Intent

What are the underlying conditions that contribute to motive & intent?

Operational

Capability

Infrastructure



What capabilities do they possess, how do they work, & what infrastructure will those capabilities come from?

Tactical

TTPs

What TTPs will the adversary execute in order to gain access?

THE CYBER THREAT LANDSCAPE

Ourselves

The Adversary

Strategic

Public Sector | Healthcare | Energy | Tech | Financial | Consumer Products

Motive

Intent

Operational

Critical Assets

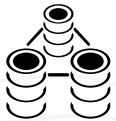
People

Processes

Technology

Capability

Infrastructure



Tactical

Access Vectors

	Supply Chain		Social Engineering		Internal to Network
	Comms Infrastructure		Coercion		External to Network
	Close Access		Business Transaction		Lateral Movement

TTPs

FALCON

SO HOW DO WE FIGHT BACK?

THREAT HUNTING & THREAT INTELLIGENCE

Ourselves

Public Sector | Healthcare | Energy | Tech | Financial | Consumer Products

People | Technology

The Adversary

Motive | Intent

Capa… | …cture

TTPs

Strategic

Operational

Tactical

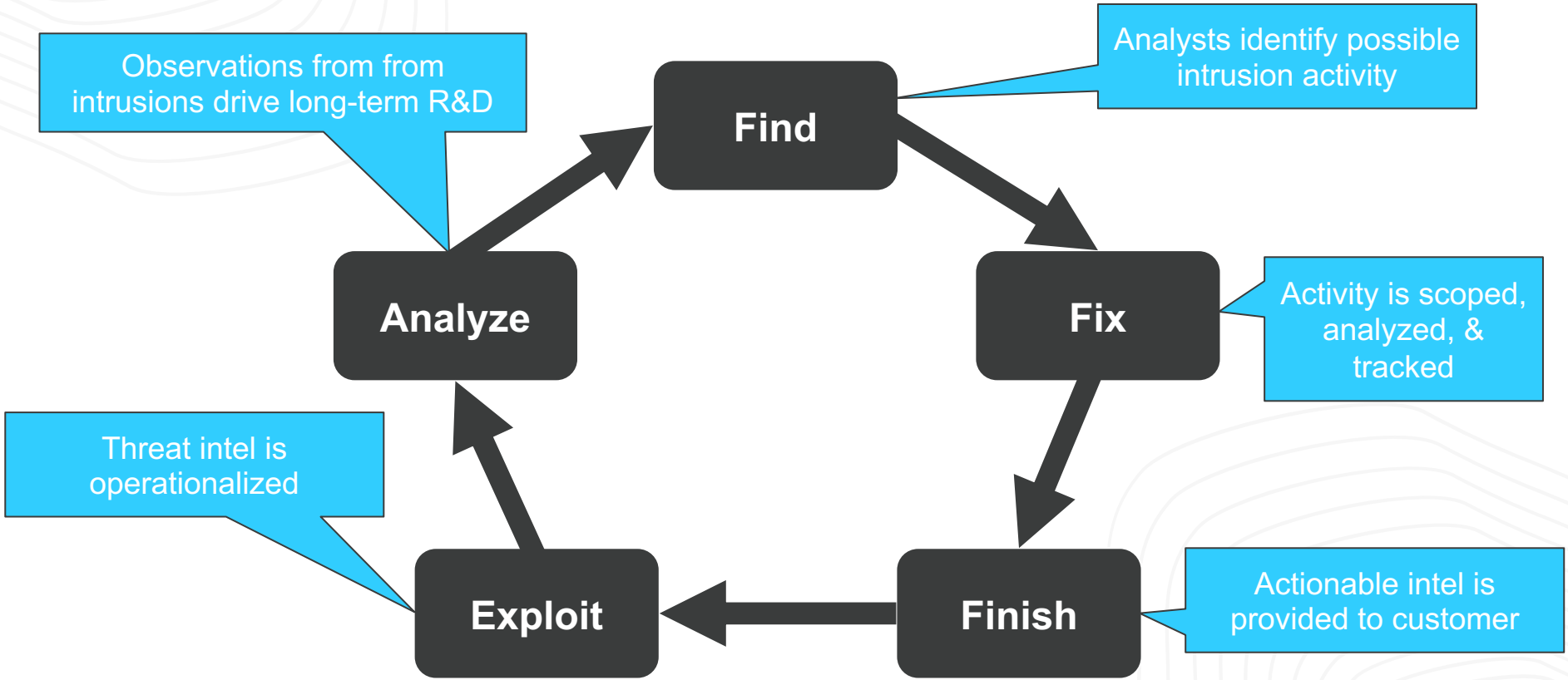
	Supply Chain		Social Engineering		Internal to Network
	Comms Infrastructure	$	Coercion		External to Network
	Close Access		Business Transaction		Lateral Movement

Threat Hunting

Threat Intelligence

FALCON

OPERATIONALIZING THREAT HUNTING



FALCON

ENABLING ELEMENTS

ENVIRONMENT

- Asset Inventory
- Classification of Data & Assets

Process

- Speed
- Context
- Baselining

Technical

- Host Visibility
- Network Awareness
- Enterprise Search
- Threat Intelligence

TECHNICAL CAPABILITIES FRAMEWORK

Capability	Minimum	Preferred
Host-level activity awareness	• Centralized log aggregation	• Real-time EDR
Network-level awareness	• Transaction logging (Proxy/FW) • Netflow	• NIPS • PCAP • SSL inspection
Enterprise Log Search	• On-demand triage scripts • Clean asset / application inventory	• Centralized aggregation of data (searchable) • Event correlation
Threat Intelligence	• Ad-hoc, open sourced research • Primary tactical	• Subscription to reputable source • Information sharing • Integrated tactical, strategic and operational

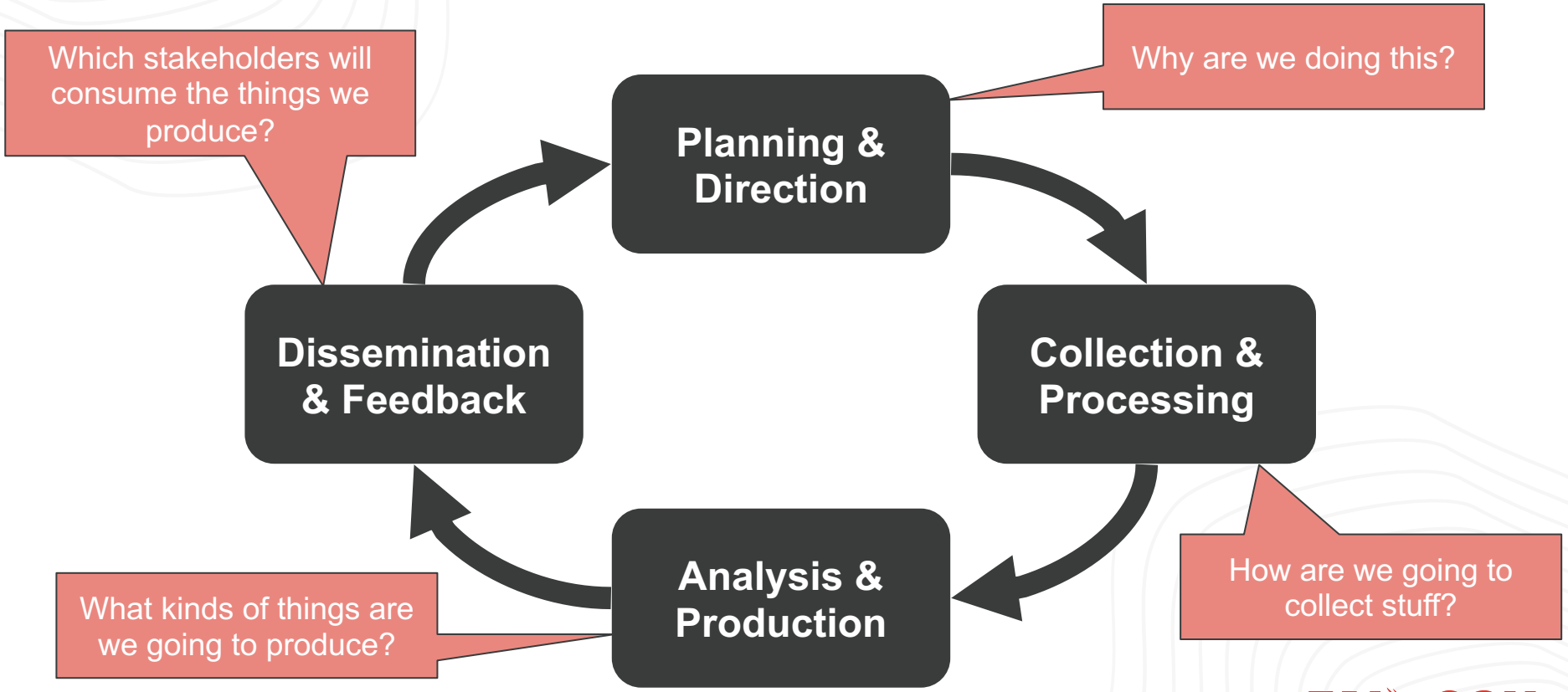
A NO-COST STARTING POINT

Logs (Network, Event Logs, DNS, AD Logs, DHCP, etc.)

LOG TYPES	LOG SOURCE	RETENTION PERIOD
Requests	DNS Logs	3 months
Applications, Security & System	Windows Event Logs	12 months
Access	Web Proxy Logs Firewall Logs	6 months
Authentication	Active Directory Remote Access Authentication Logs	6 months

https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm
www.crowdstrike.com/blog/the-importance-of-logs/

OPERATIONALIZING THREAT INTELLIGENCE



FALCON

INTELLIGENCE LIFECYCLE STEPS 1 & 2

Process	Goal	Desired Outcome
Planning & Direction	Use your estimate of the cyber threat landscape to develop your hypotheses, which then serve to define your mission through PIRs. Understand who will benefit from cyber threat intelligence, your stakeholders, what their intel requirements are and how to fulfill them.	• Cyber Threat Landscape • Priority Intelligence Requirements
Collection & Processing	Identify the inventory of existing threat intelligence sources within your environment (historical and real time). Collect from these trusted sources and external providers to satisfy PIRs, then de-duplicate, prioritize, normalize, and correlate raw threat data in an indicator / reporting storage solution (such as a SIEM, TIP, or Wiki).	• Collection Plan • Information Gaps

INTELLIGENCE LIFECYCLE STEPS 3 & 4

Process	Goal	Desired Outcome
Analysis & Production	Contextualize threat intelligence through enrichment and correlation within your enrichment. Produce human-readable or machine-readable products that are relevant, and predictive.	• Analytic Products • Production Cadence
Dissemination & Feedback	Deliver timely and actionable intelligence products to your teams and technologies to stay aware of significant or emerging threats and inform decision-making. Receive feedback in order to further refine the intelligence lifecycle in pursuit of fulfilling PIRs and other cybersecurity information objectives.	• Stakeholder Consumption 1. Tactical 2. Operational 3. Strategic • Stakeholder Feedback

HOW TO SERVE THREAT HUNTING & THREAT INTEL STAKEHOLDERS

Let's imagine them as being kinda like a race car driving team…

TACTICAL

STAKEHOLDERS:
- Security Engineers
- SIEM
- Firewall
- Endpoints
- IDS/IPS

"Mechanic"

Focused on enhancing automated defenses, optimizing visibility, and achieving high states of situational awareness and efficacy throughout the enterprise.

OPERATIONAL

STAKEHOLDERS:
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Threat Hunters
- Threat Intelligence

"Race Car Driver"

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STRATEGIC

STAKEHOLDERS:
- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

"The Owner"

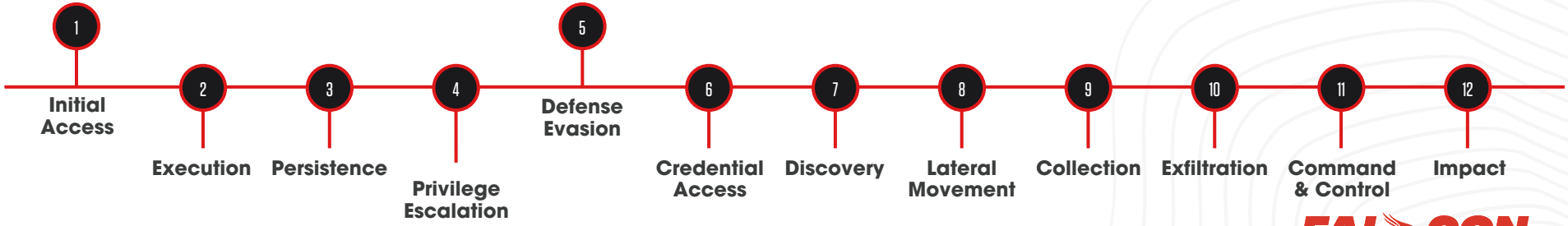
Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making.

FALCON

WHAT DOES THIS LOOK LIKE IN ACTION?

CASE STUDY: BIG GAME HUNTING

- Increased global activity by ECrime actor GRIM SPIDER
- Targeted ransomware deployment (Big Game Hunting)
  - Goal: Get deep access to network, deploy ransomware broadly, PROFIT!
- Initial access via targeted phishing email with macro-enabled MS Word doc
  - Obfuscated PowerShell script deploys modular malware TrickBot



FALCON

CYBER THREAT LANDSCAPE: BIG GAME HUNTING

Ourselves

The Adversary

Public Sector | Healthcare | Energy | Tech | Financial | Consumer Products

Financial Resources

Strategic

Motive

Criminal

Intent

Extortion

Data Theft

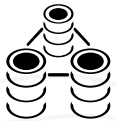
Fraud

Critical Assets

Operational

Capability

Infrastructure



People

Processes

Technology

Access Vectors

Tactical

	Supply Chain		Social Engineering		Internal to Network
	Comms Infrastructure		Coercion		External to Network
	Close Access		Business Transaction		Lateral Movement

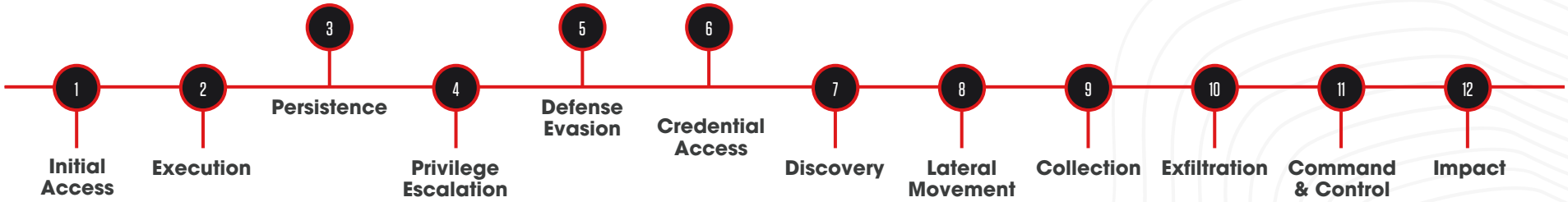
TTPs

Spear Phishing

FALCON

CASE STUDY: BIG GAME HUNTING

- Additional tools downloaded and deployed
  - Trickbot modules for recon and id theft
  - PowerShell Empire framework
- Leveraged scheduled tasks, services, and masqueraded file names to attempt to blend in
  - Tasks and services: `WinDotNet, GoogleTask, Sysnetsf, ControlServiceA, Updater`
  - Files, directories: `WinDefrag, NetSocket`
- TrickBot module `pwgrab64` sets registry key `UseLoginCredential = 1` resulting in creds stored in plaintext memory, accessible to cred dumping tools
- Collected creds for mail clients, web browsers, FileZilla, WinSCP, PuTTY, VNC, RDP



CYBER THREAT LANDSCAPE: BIG GAME HUNTING

Ourselves

The Adversary

Financial Resources

Strategic

Motive

WizardSpider

Intent

Extortion

Data Theft

Fraud

Critical Assets

Operational

Capability

Infrastructure

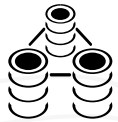
People

PowerShell

Processes

Technology

TrickBot



Access Vectors

Tactical

	Supply Chain		Social Engineering		Internal to Network
	Comms Infrastructure		Coercion		External to Network
	Close Access		Business Transaction		Lateral Movement

Spear Phishing

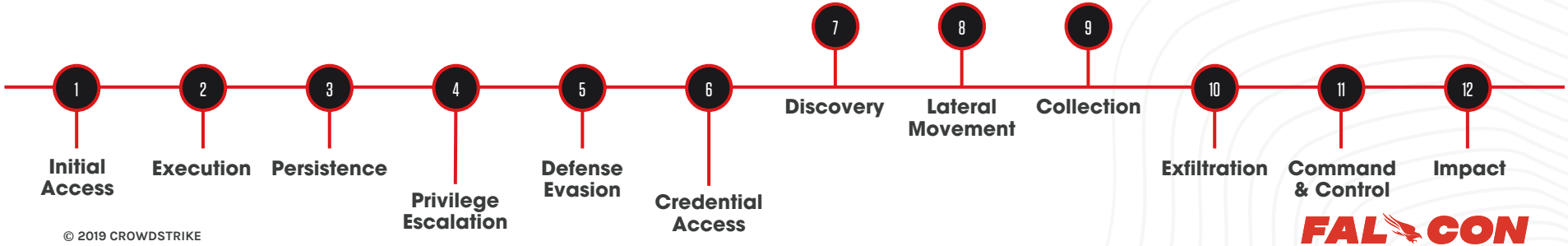
TTPs

FALCON

CASE STUDY: BIG GAME HUNTING

- Trickbot modules `networkdll` and `psfin`
  - Collects local system and network data via WMI, LDAP, and command line
  - Hunts for financial and Point-of-Sale systems
- Hunting for admin credentials

- First lateral movement can happen within hours of initial access
- Tools: `PsExec.exe`, TrickBot `shareDll` module
- Achieving admin access can take days to months



FALCON

CYBER THREAT LANDSCAPE: BIG GAME HUNTING

Ourselves

The Adversary

Financial Resources

Strategic

Motive

Wizard Spider

Intent

Extortion

Data Theft

Fraud

Critical Assets

Operational

Capability

Infrastructure

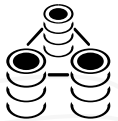
Admin Creds

PowerShell

System & Network Data

Financial & POS Systems

Trickbot



People

Processes

Technology

Access Vectors

Tactical

TTPs

	Supply Chain		Social Engineering		Internal to Network
	Comms Infrastructure		Coercion		External to Network
	Close Access		Business Transaction		Lateral Movement

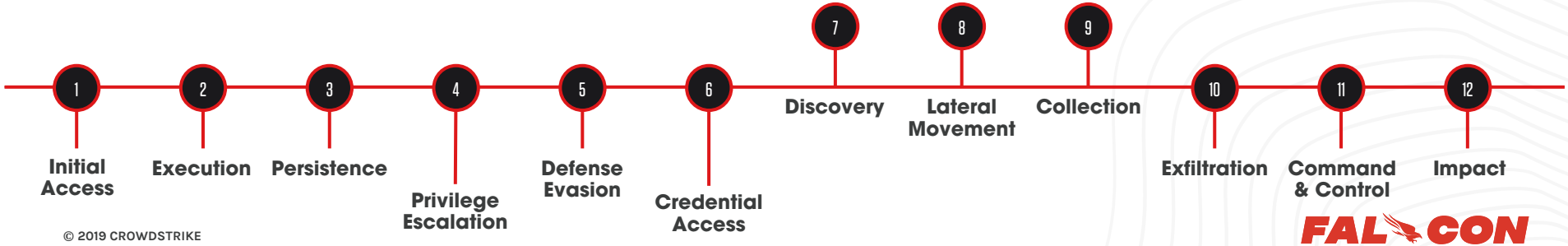
Spear Phishing

FALCON

CASE STUDY: BIG GAME HUNTING

- Trickbot modules `networkdll` and `psfin`
  - Collects local system and network data via WMI, LDAP, and command line
  - Hunts for financial and Point-of-Sale systems
- Hunting for admin credentials

- First lateral movement can happen within hours of initial access
- Tools: `PsExec.exe`, TrickBot `shareDll` module
- Achieving admin access can take days to months



FALCON

CYBER THREAT LANDSCAPE: BIG GAME HUNTING

Ourselves

Financial Resources

The Adversary

Strategic

Motive

Wizard Spider

Intent

Extortion

Data Theft

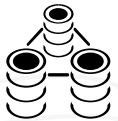
Fraud

Operational

Capability

Trickbot

Infrastructure



Critical Assets

Admin Creds

People

PowerShell

Processes

System & Network Data

Financial & POS Systems

Technology

Tactical

Access Vectors

	Supply Chain		Social Engineering		Internal to Network
	Comms Infrastructure		Coercion		External to Network
	Close Access		Business Transaction		Lateral Movement

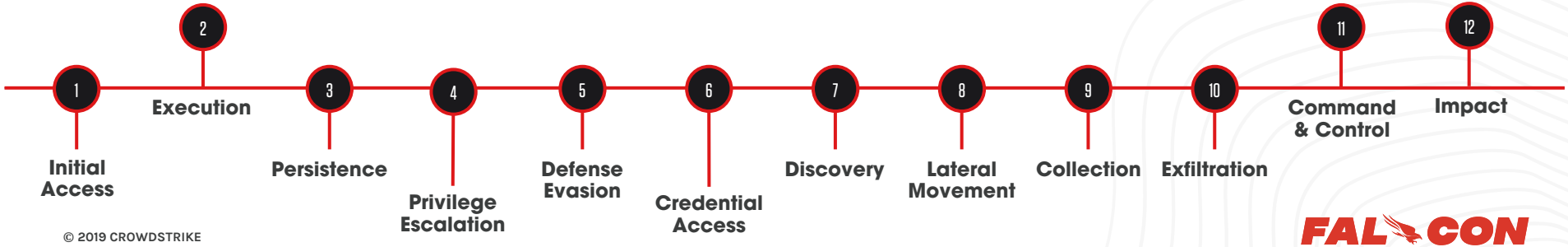
TTPs

Spear Phishing

FALCON

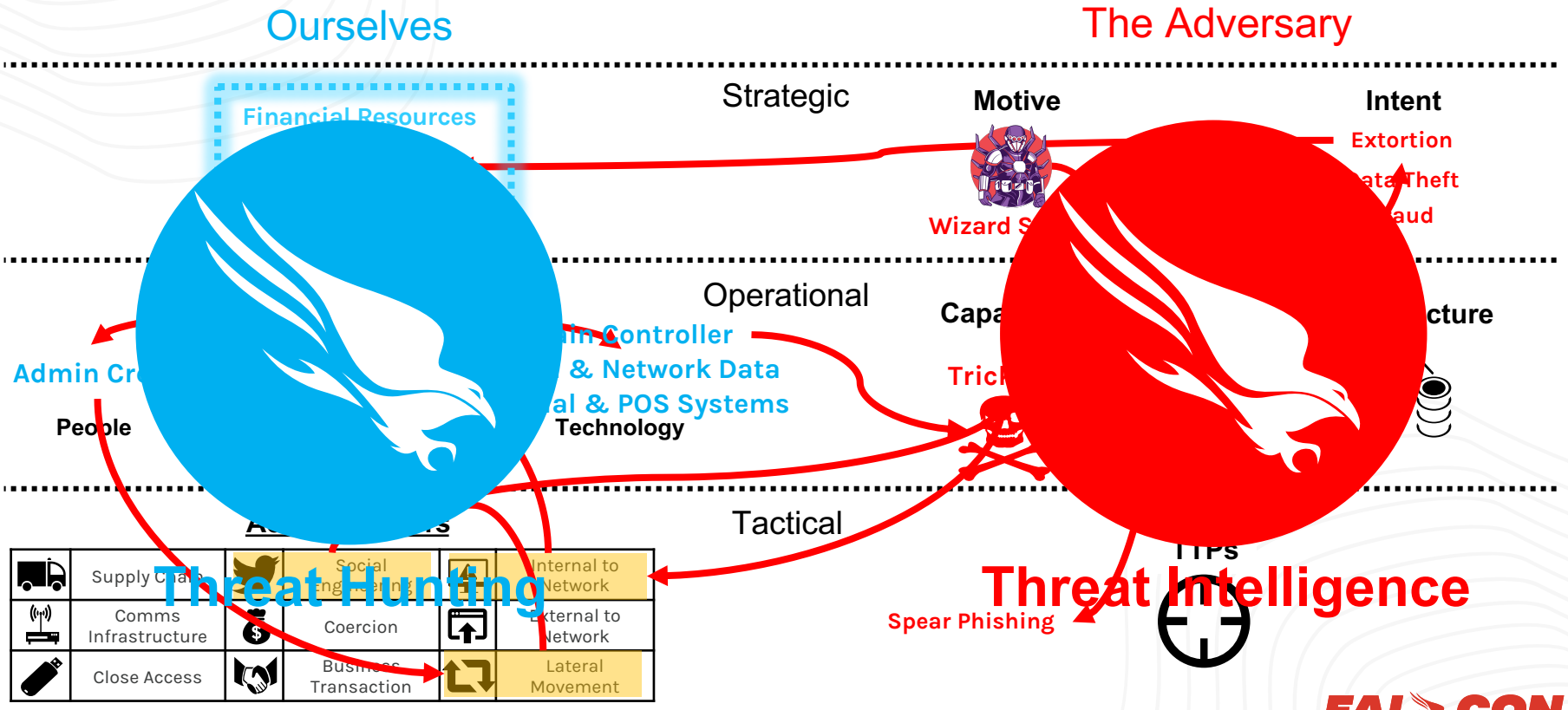
CASE STUDY: BIG GAME HUNTING

- Leverage domain admin and Domain Controller as staging ground
- Stage Ryuk ransomware and deploy to targets via PsExec
  - Noisy operation, so speed is of the essence at this point
  - 3-8 hours to deploy globally



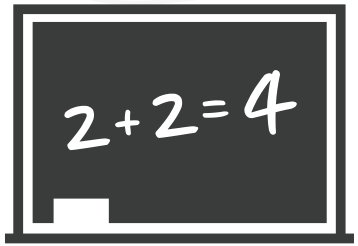
FALCON

CYBER THREAT LANDSCAPE: BIG GAME HUNTING



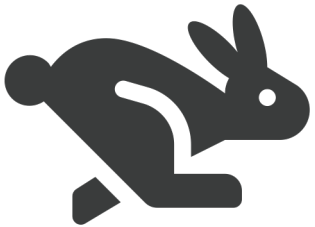
RECOMMENDATIONS

A proactive mindset and a little bit of planning go a long way



The fundamentals still matter – continue to enforce basic security hygiene

Look beyond malware: strengthen defenses against modern attack



Survival of the fastest: accept the 1-10-60 challenge

Look to partners to help solve the skills shortage

THANK YOU.

ANY QUESTIONS?