Developing your TI strategy

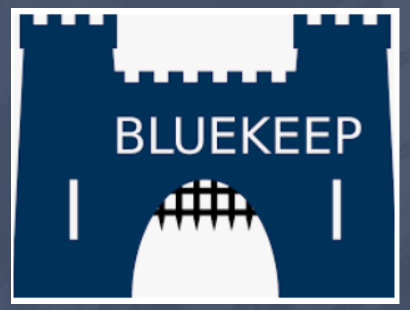
December 2020 – **Cyber Ireland Zero to Hero TI Series**

Eoin Carroll - Sr Vulnerability Researcher & Principal Engineer
McAfee ATR (Advanced Threat Research)

McAfee Confidential

About me @w3knight

Critical Industry Vulnerabilities



Next Generation Technology

Advanced Threat Research & Defense

Semi-Conductor Electronic Engineer Medical Device Electronic Engineer Defensive & Offensive Security Roles

Cisco CCNA MSc Network & Security (CIT)

2000 2007 2009 2011 2020

Threat Intelligence/Defensible Security Architecture

DRAGOS PRODU

Robert M. Lee

Chief Executive Officer

SEC530: Defensible Security Architecture and Engineering

CIS. Center for Internet Security®

Recorded Future®

ATT&CK®

INTEL471

THE BEST OF TAOSECURITY BLOG

VOLUME 1

MILESTONES, PHILOSOPHY AND STRATEGY, RISK, AND ADVICE

RICHARD BEJTLICH

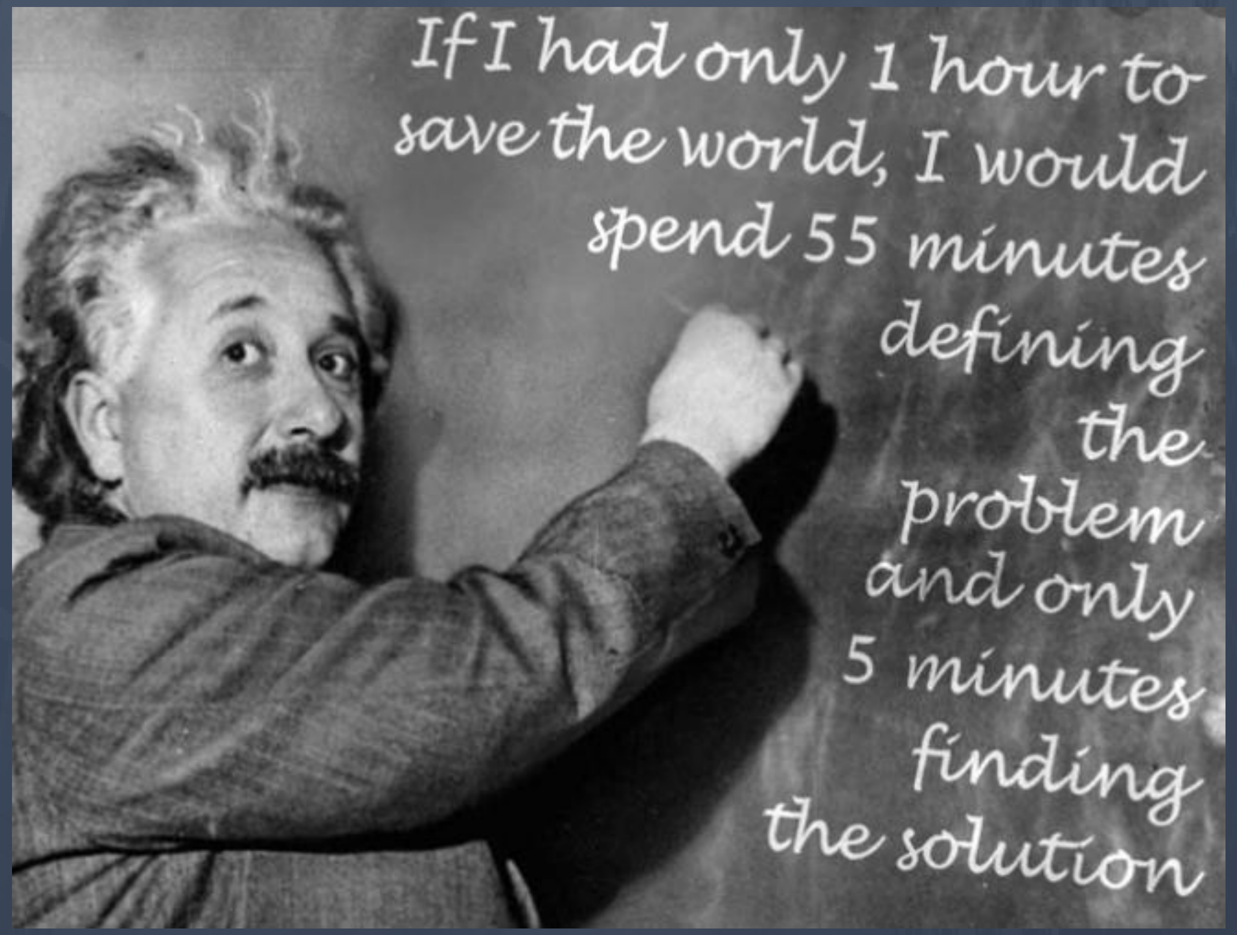
NIST National Institute of Standards and Technology U.S. Department of Commerce

Todays Learning Objectives

- Why do we need Threat Intelligence
- Threat Intelligence Strategy and Requirements
- Active Defense (consuming vs generation)
- Prioritizing Vulnerabilities
- Active Defense Tools

Why do we need Threat Intelligence

- Understand real credible threats relative to our Business
- Assess our exposure relative to active adversaries
- Stay one step ahead of our adversaries by understanding their motives, capabilities and opportunities (Proactive not Reactive)
- Drive and prioritize Defensible Security Architecture

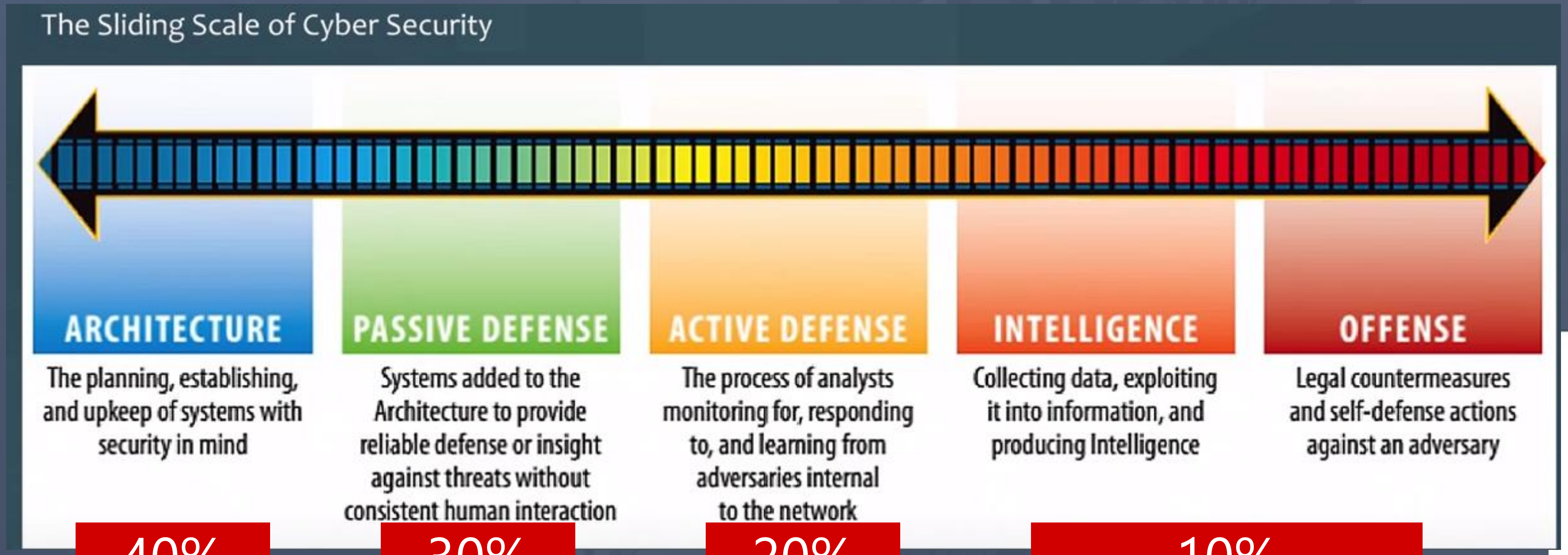


If I had only 1 hour to save the world, I would spend 55 minutes defining the problem and only 5 minutes finding the solution

Threat Intelligence Strategy and Requirements

- Start at Policy level and the Threat Intelligence requirements of the business stakeholders (Business assets of value to attacker)
- Situational awareness - know your own environment and adversaries in your Threat Model relative to your business
- Need to build on a strong Security Architecture, SOC and IR infrastructure capabilities
- Consumer vs Generating (consumer readily available TI)
- Intelligence must meet the requirements of business stakeholders consuming

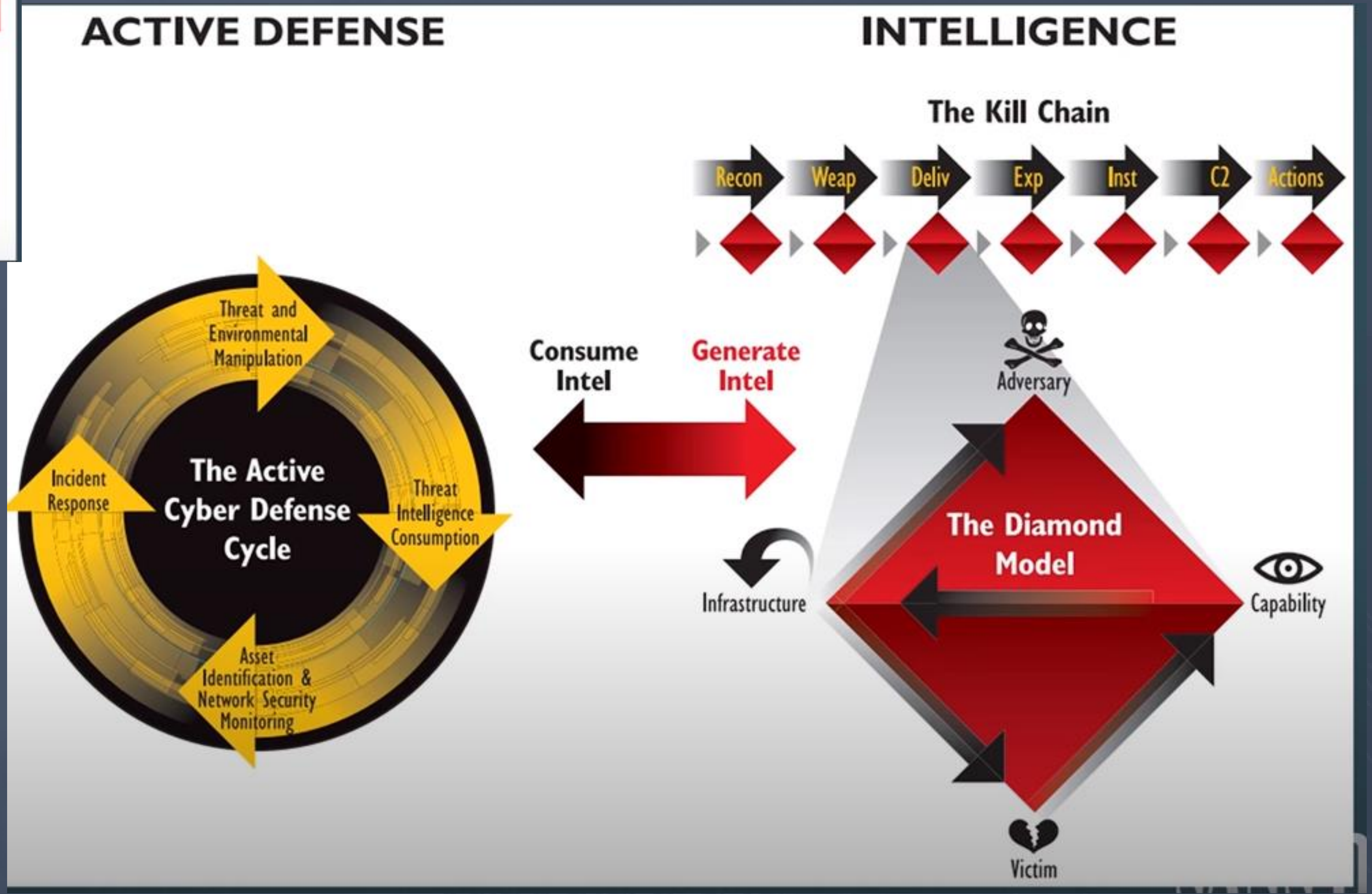
Active Defense (consuming vs generation)


The Sliding Scale of Cyber Security
ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

40% 30% 20% 10%

- Motives
- Capabilities
- Opportunity

The bigger picture IoA (Campaigns vs IoC)



Digest Threat Intelligence → Extract TTPs → Map to MITRE ATT&CK → Emulate Adversary Threat Hunting → Close Defense Gaps

Knowing When to Consume Intelligence and When to Generate It - CTI SUMMIT 2017
https://www.youtube.com/watch?v=cW7Z9Vqsgk0

McAfee

Active Adversaries and how they are getting in and operating

1988 - Morris Worm

2001 – Code Red Worm

2003 – Blaster Worm

2004 – Sasser Worm

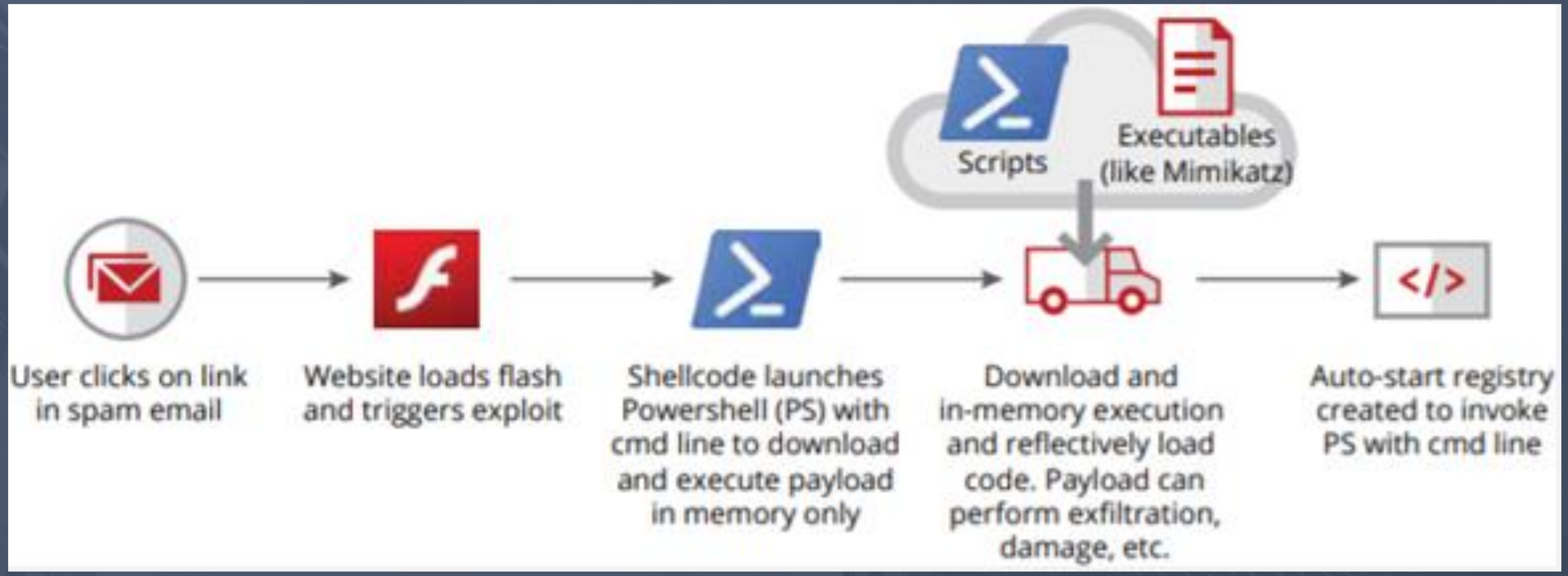
2017 – Eternalblue (MS17–010)

2019 – Bluekeep (CVE- 2019-0708)

2020 - SMBGhost (CVE-2020-0796)

2020 - SIgRed (CVE-2020-1350)

2020 - Bad Neighbor (CVE-2020-16898)



Scripts

Executables (like Mimikatz)

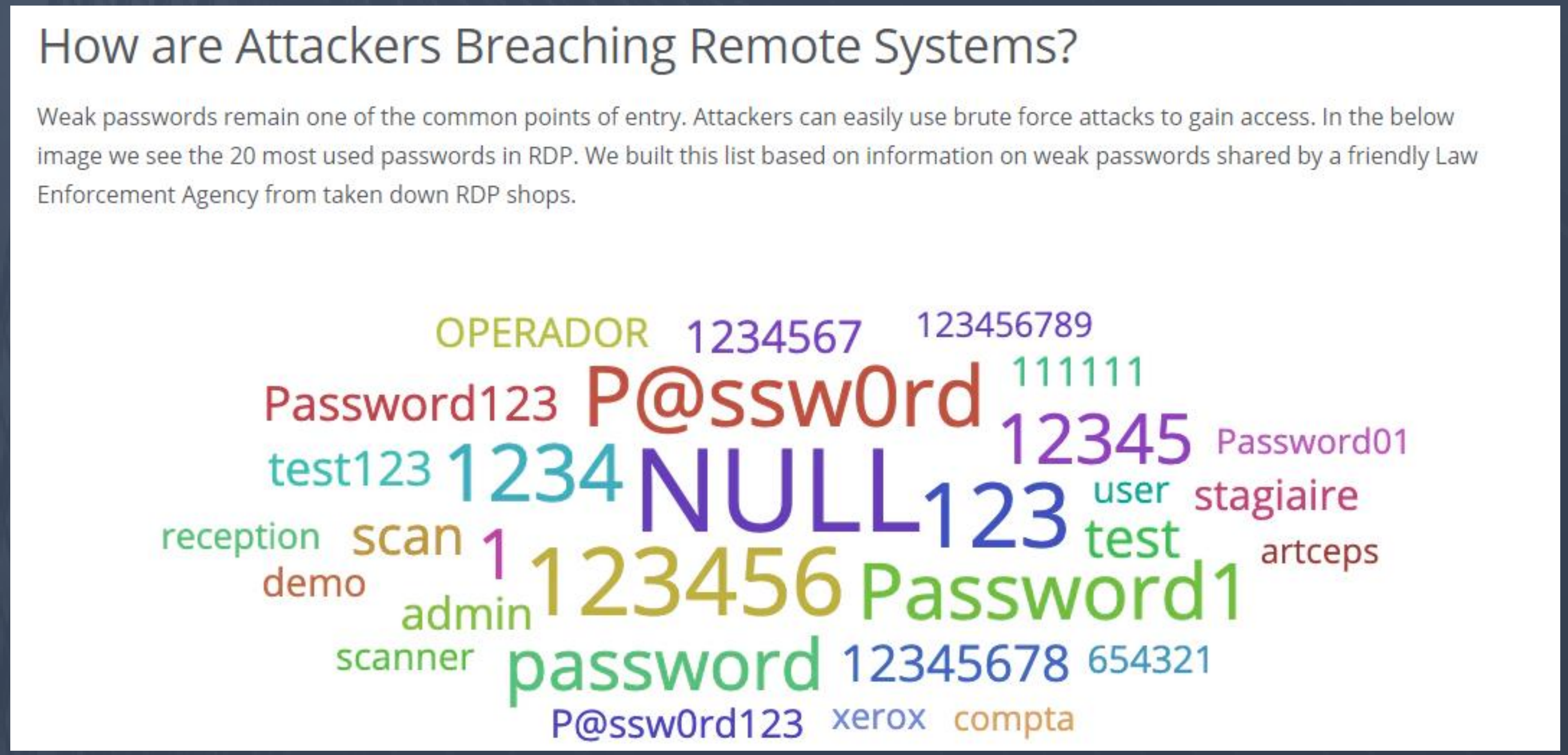
User clicks on link in spam email

Website loads flash and triggers exploit

Shellcode launches Powershell (PS) with cmd line to download and execute payload in memory only

Download and in-memory execution and reflectively load code. Payload can perform exfiltration, damage, etc.

Auto-start registry created to invoke PS with cmd line

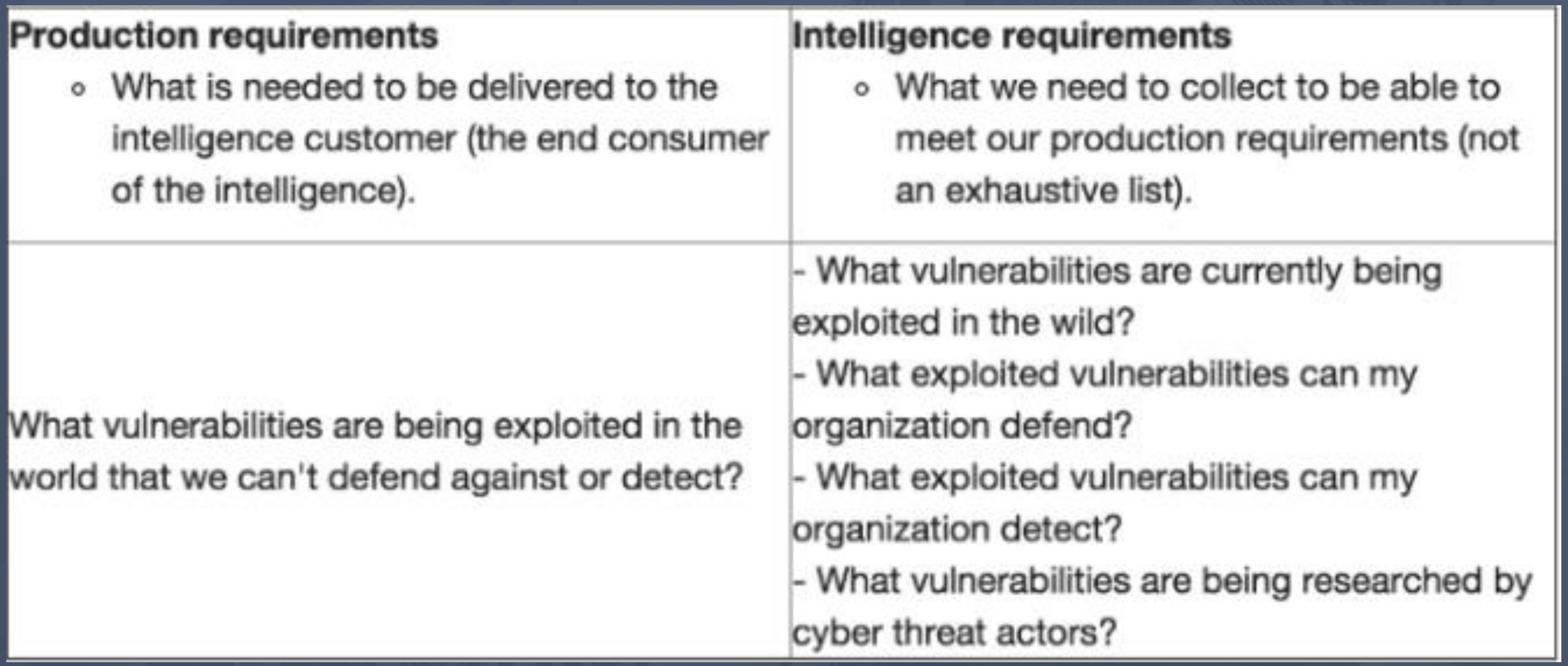


How are Attackers Breaching Remote Systems?

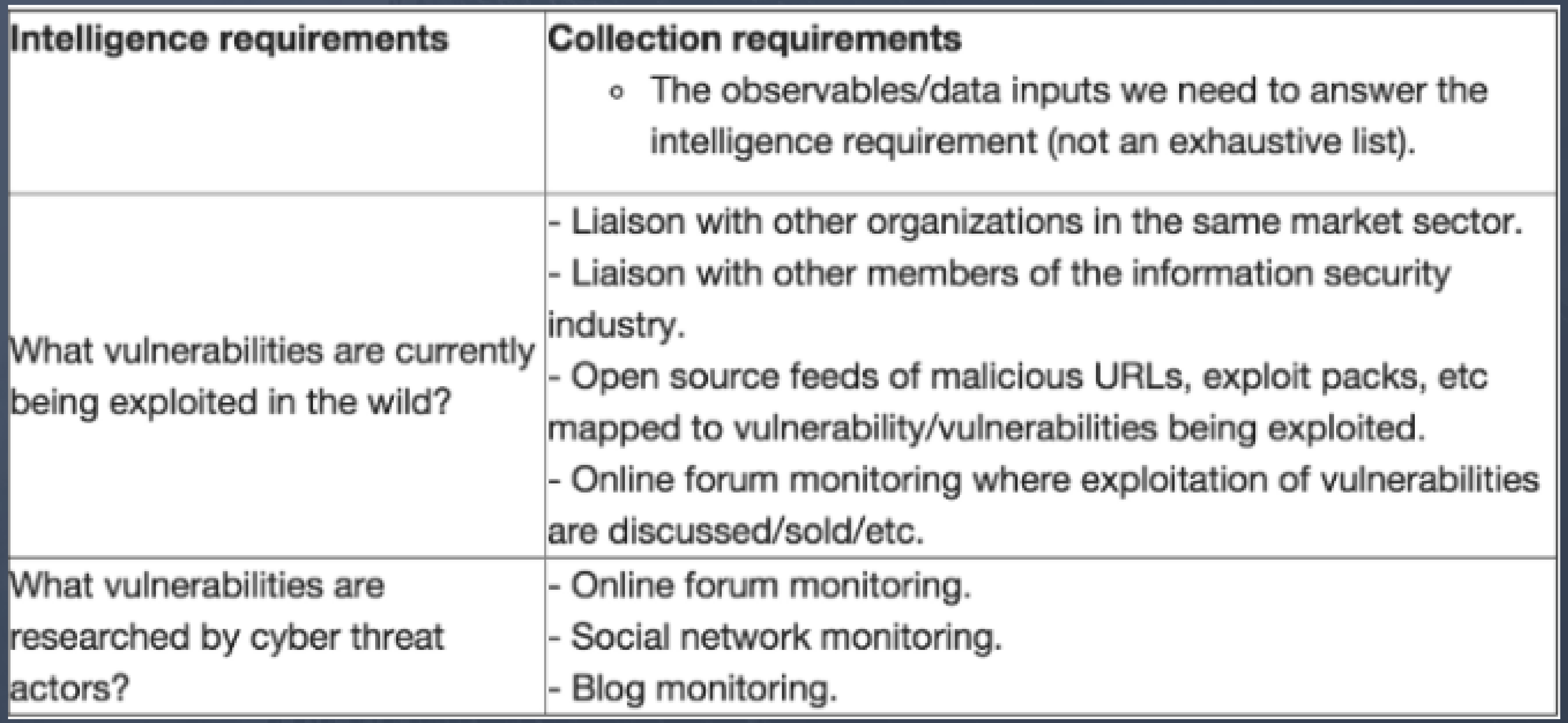
Weak passwords remain one of the common points of entry. Attackers can easily use brute force attacks to gain access. In the below image we see the 20 most used passwords in RDP. We built this list based on information on weak passwords shared by a friendly Law Enforcement Agency from taken down RDP shops.

Threat Intelligence Requirement

The CISO/CSO (Chief Information Security Officer) of your organization wants to know of any vulnerabilities that are being exploited in the wild that your organization can’t defend against or detect



Production requirements ○ What is needed to be delivered to the intelligence customer (the end consumer of the intelligence).	**Intelligence requirements** ○ What we need to collect to be able to meet our production requirements (not an exhaustive list).
What vulnerabilities are being exploited in the world that we can't defend against or detect?	- What vulnerabilities are currently being exploited in the wild? - What exploited vulnerabilities can my organization defend? - What exploited vulnerabilities can my organization detect? - What vulnerabilities are being researched by cyber threat actors?



Intelligence requirements	**Collection requirements** ○ The observables/data inputs we need to answer the intelligence requirement (not an exhaustive list).
What vulnerabilities are currently being exploited in the wild?	- Liaison with other organizations in the same market sector. - Liaison with other members of the information security industry. - Open source feeds of malicious URLs, exploit packs, etc mapped to vulnerability/vulnerabilities being exploited. - Online forum monitoring where exploitation of vulnerabilities are discussed/sold/etc.
What vulnerabilities are researched by cyber threat actors?	- Online forum monitoring. - Social network monitoring. - Blog monitoring.

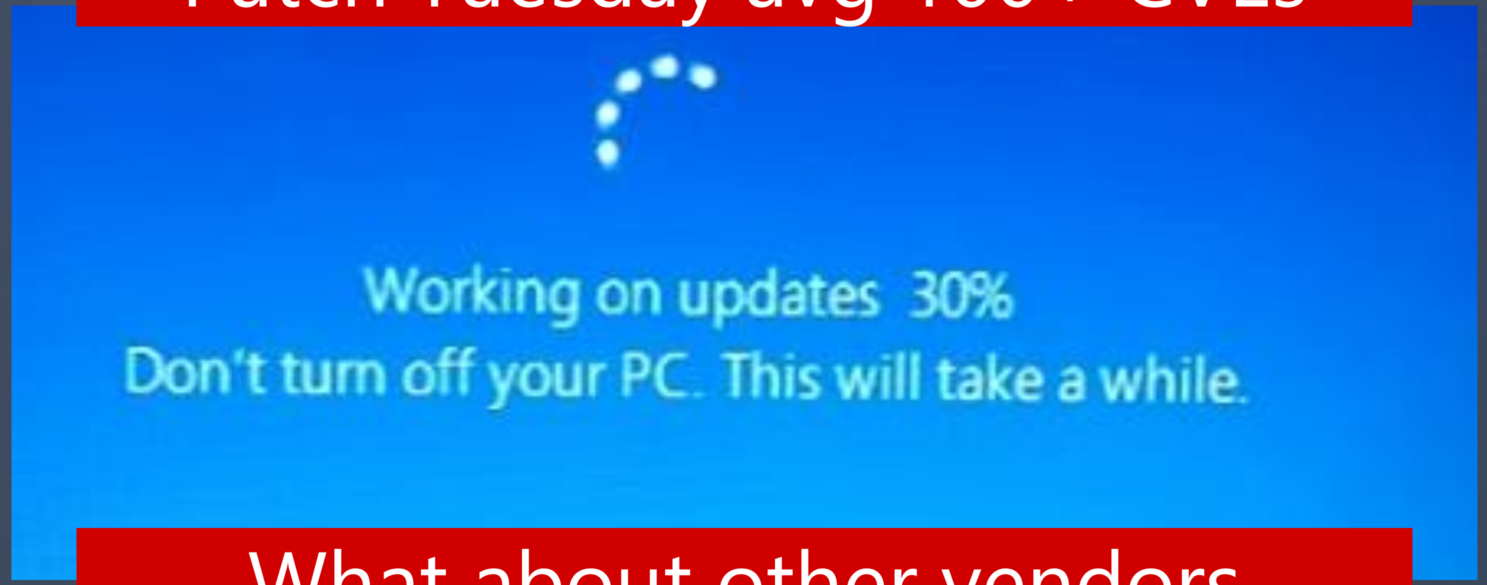
Cyber threat intelligence requirements: What are they, what are they for and how do they fit in the intelligence cycle
https://medium.com/@markarenaau/cyber-threat-intelligence-requirements-what-are-they-what-are-they-for-and-how-do-they-fit-in-the-79441aeca032

Vulnerability Prioritization using Threat Intelligence

CVE-2020-17051: Remote kernel heap overflow in NFSv3 Windows Server

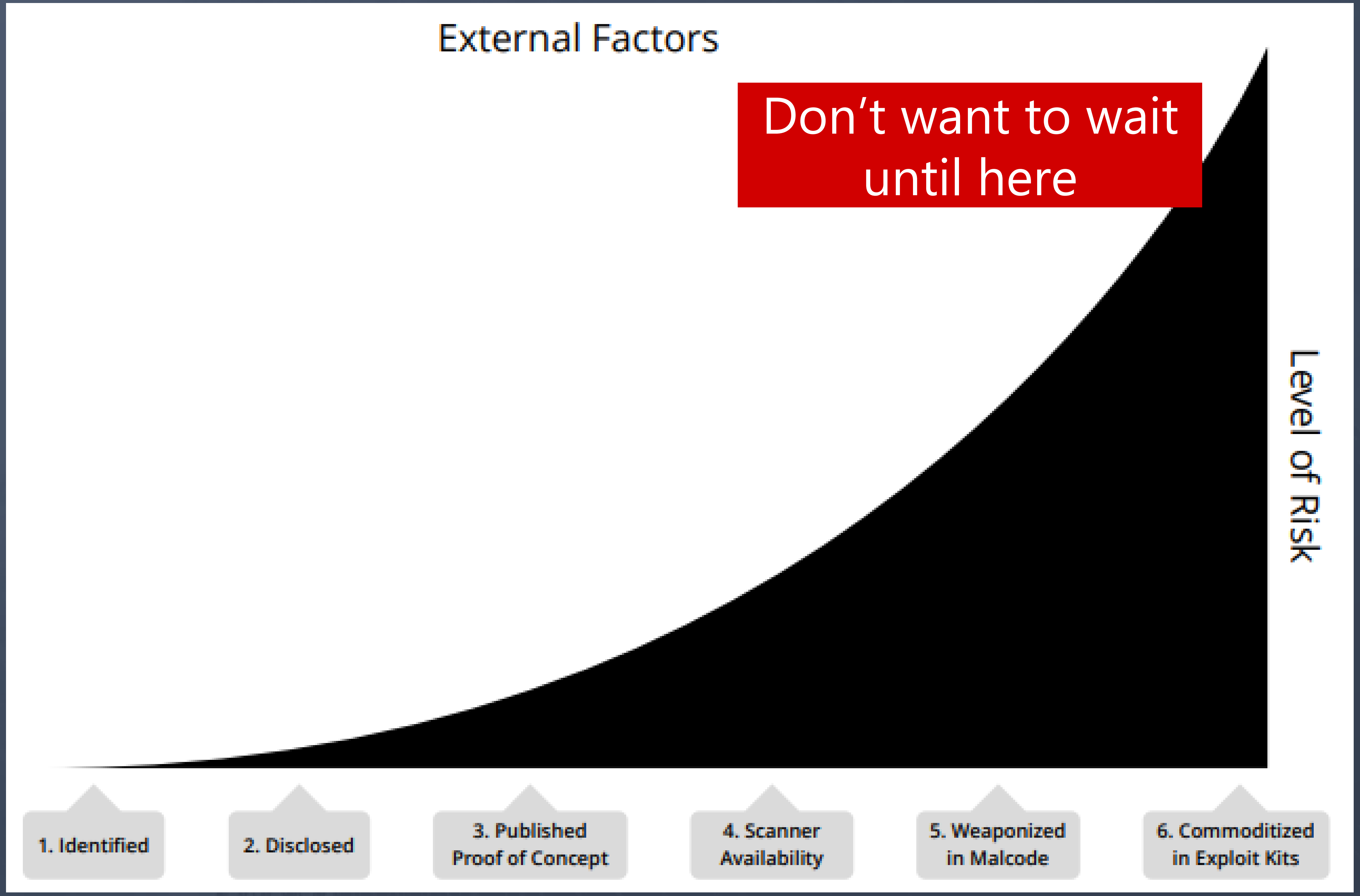
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cve-2020-17051-remote-kernel-heap-overflow-in-nfsv3-windows-server/

Patch Tuesday avg 100+ CVEs



Working on updates 30%
Don't turn off your PC. This will take a while.

What about other vendors



Don't want to wait until here

https://go.recordedfuture.com/book

Active Defense Tools

How to find C2 activity with Zeek and MITRE ATT&CK https://www.youtube.com/watch?v=oKwiyAHCZCE

Thank you.

McAfee™