

Secureworks®

Bringing it All Together- Simple Tools to Manage Threats and Risk Responsibly



Ryan Alban, CISSP | GISP
Sr. Manager,
Global Solution Leads
Secureworks

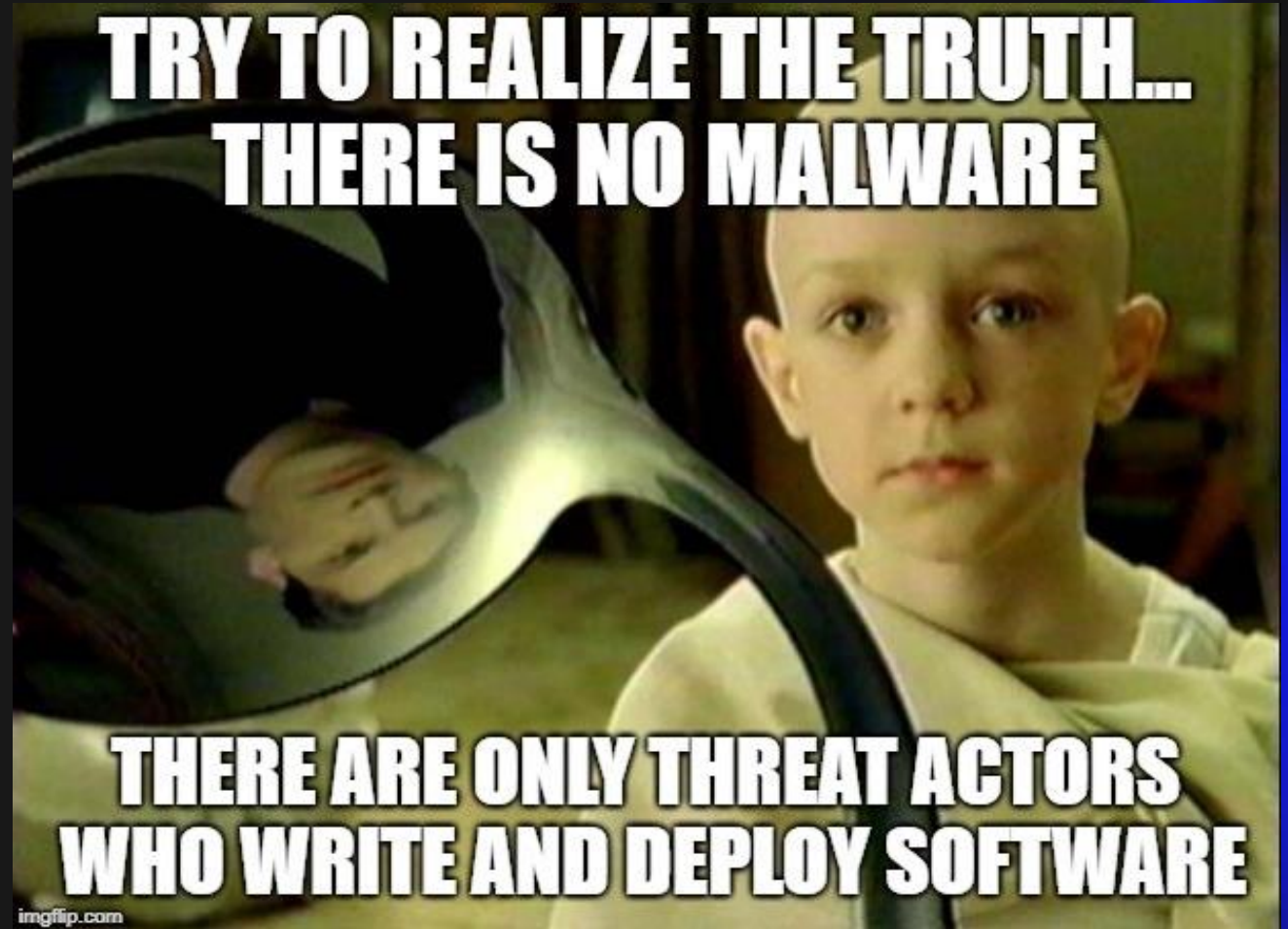




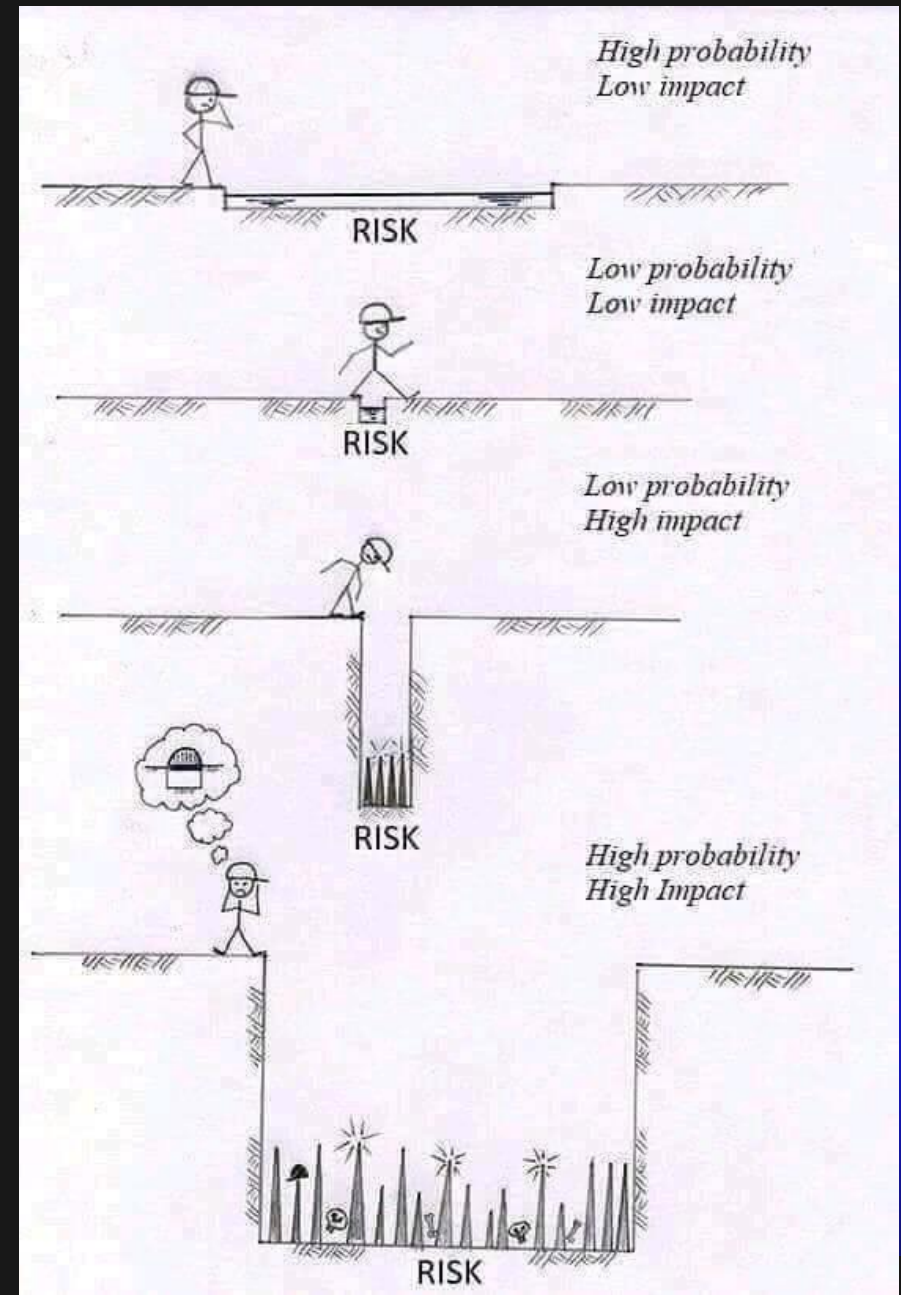
Today's Topics

- Threat Intelligence + Risk Management -> Action
- Brief (threat) Briefing
- Plotting Threat Impact
- Lather, Rinse, & Repeat
- (while having fun)

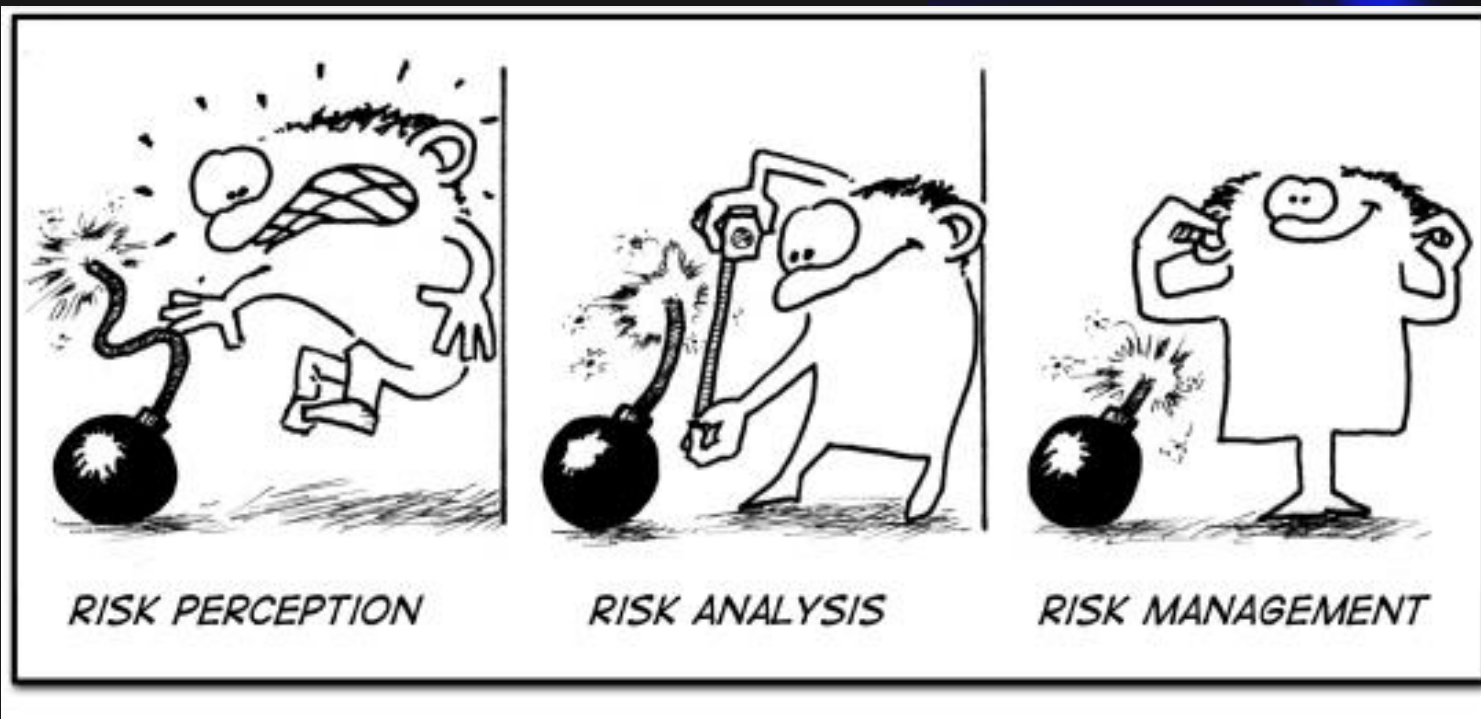
Without Threat Intelligence, you don't understand what you are defending against.



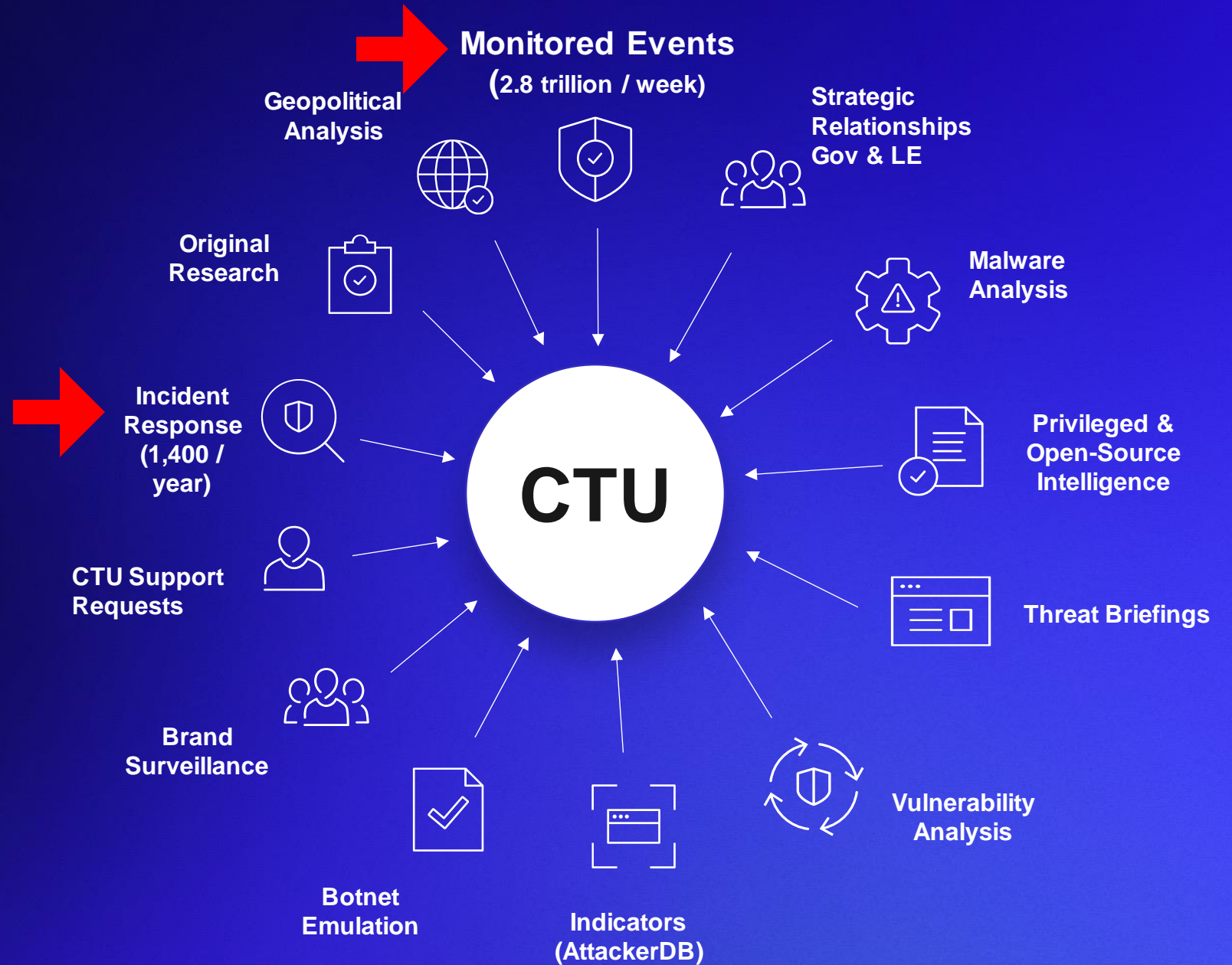
**Without
Risk Management,
you don't
understand
what you
are protecting.**



**Without
Action, you
are not doing
your job.**



Intelligence Collection



Incident Response Data



Organized Crime Threat Actors

Financially motivated cybercriminals are looking for a payday, plain and simple.



This cryptocurrency miner is exploiting the new Confluence remote code execution bug

By Charlie Osborne | 22 September 2021

The z0Miner cryptojacker is now weaponizing a new Confluence vulnerability to mine for cryptocurrency on vulnerable machines.



Data for 700M LinkedIn Users Posted for Sale in Cyber-Underground

By Tara Seals | 28 June 2021

After 500 million LinkedIn enthusiasts were affected in a data-scraping incident in April, it's happened again – with big security ramifications.

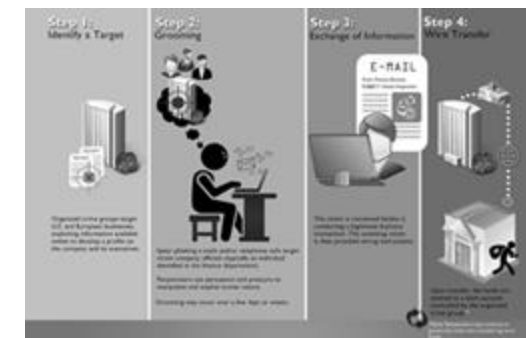


DARKReading

FBI: Business Email Compromise Cost \$1.8B in 2020

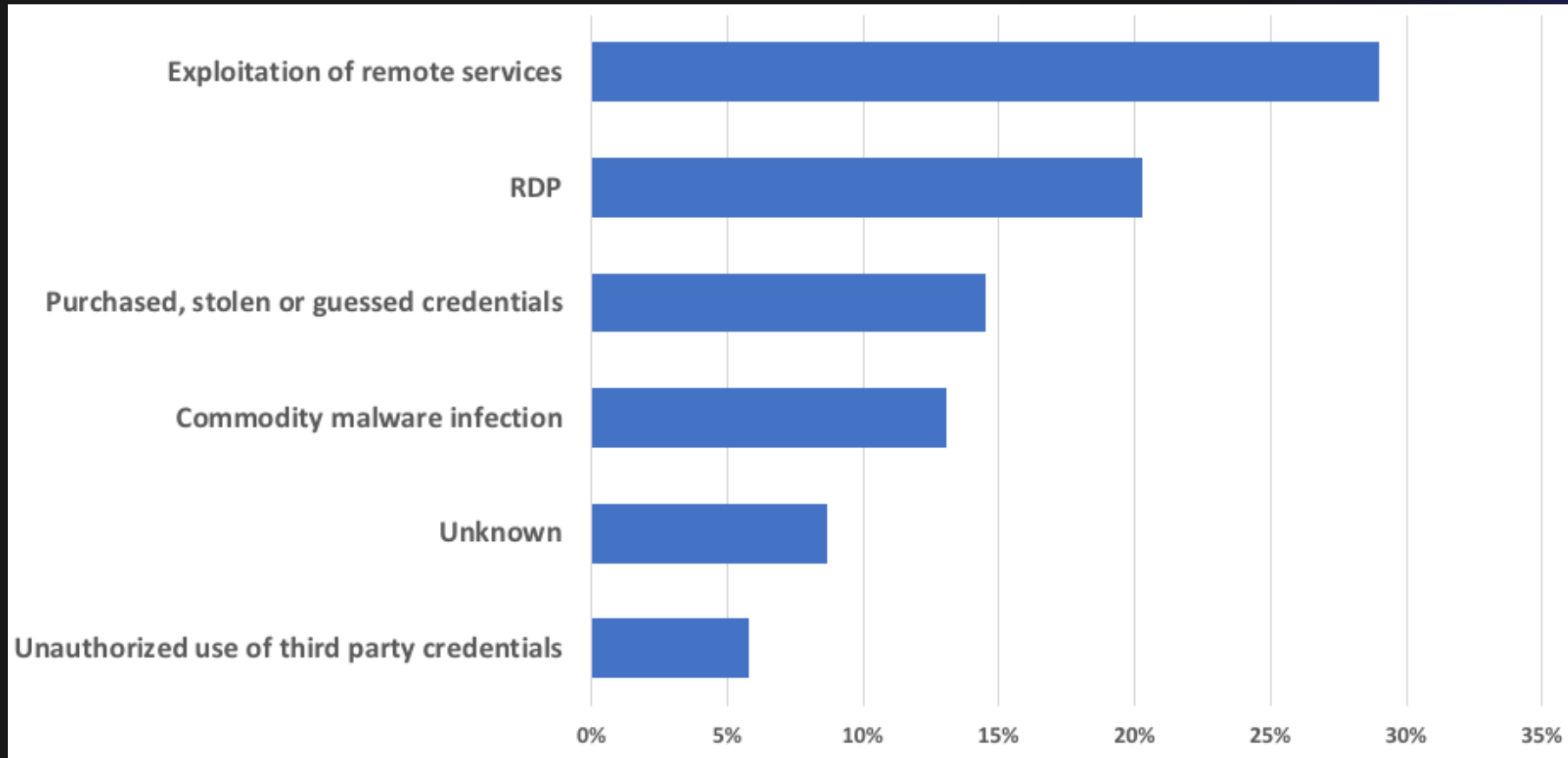
By Dark Reading Staff | 18 March 2021

Business email compromise (BEC) scams were the most expensive, with 19,369 complaints and adjusted losses of approximately \$1.8 billion.



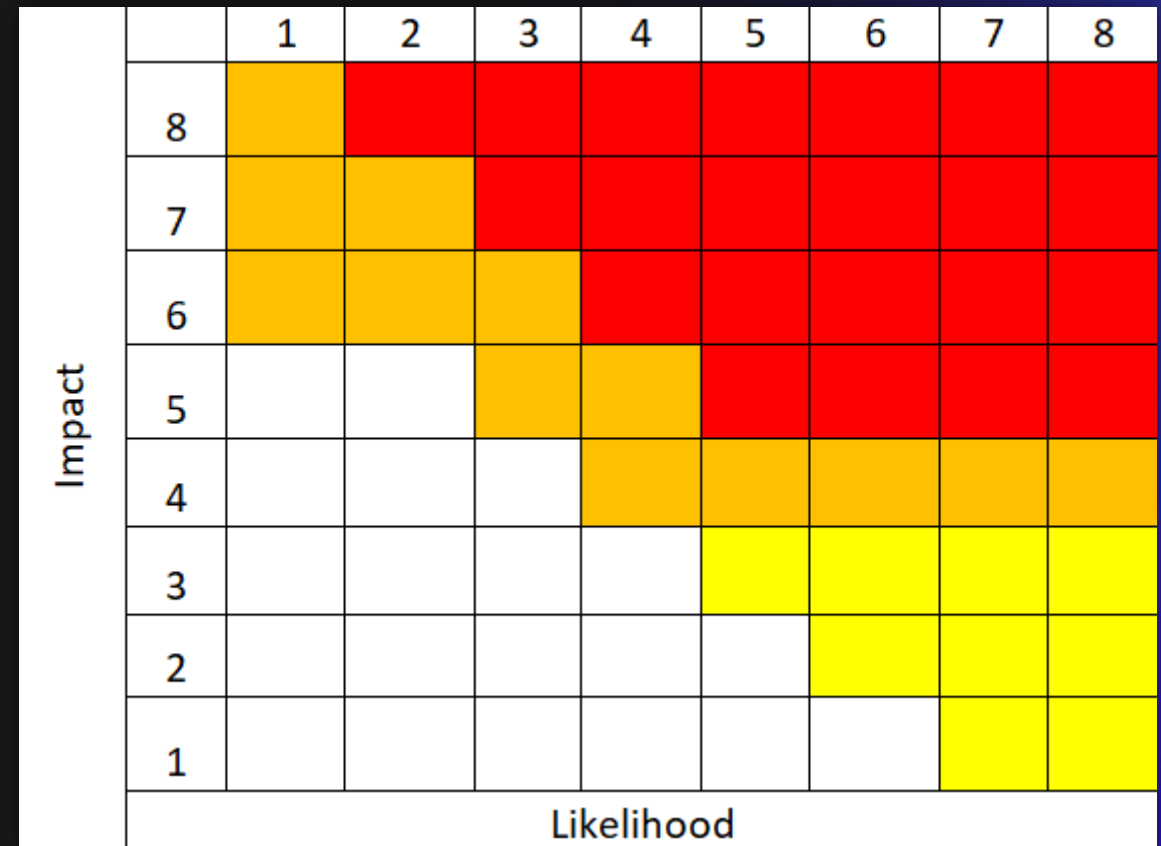
Ransomware Initial Access Vectors (IAV)

Most incidents occur due to a failure of security controls – 2021



Threat Heat Map – Where do you focus your resources?

- ① Post-intrusion ransomware
- ② Business Email Compromise
- ③ Nation State Espionage / IP Theft
- ④ Financially-motivated data theft
- ⑤ Cryptomining attacks
- ⑥ Nation State Destructive Attacks
- Ⓐ Commodity Remote Access Trojans
- Ⓑ Network Intrusions
- Ⓒ Critical Vulnerability Exploitation

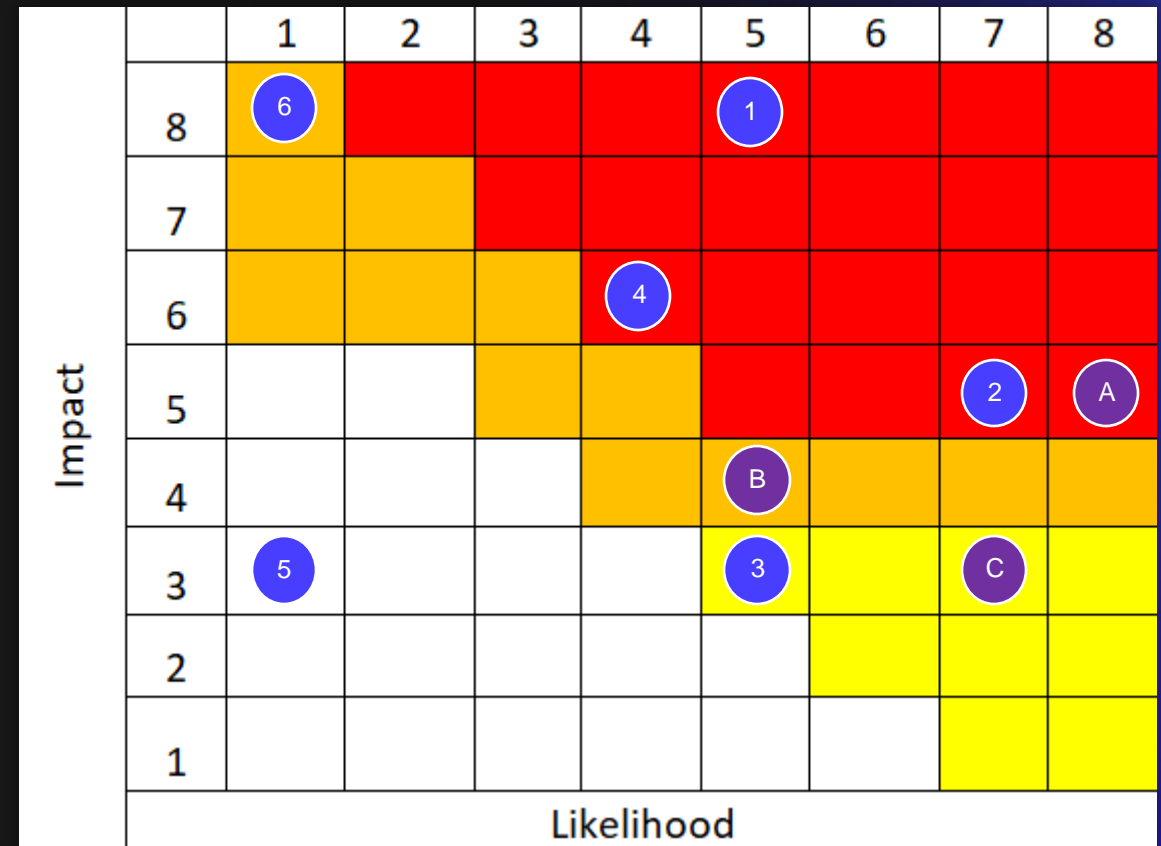


① = Core Threat

Ⓐ = Precursor to Core Threat

Threat Heat Map – Manufacturing

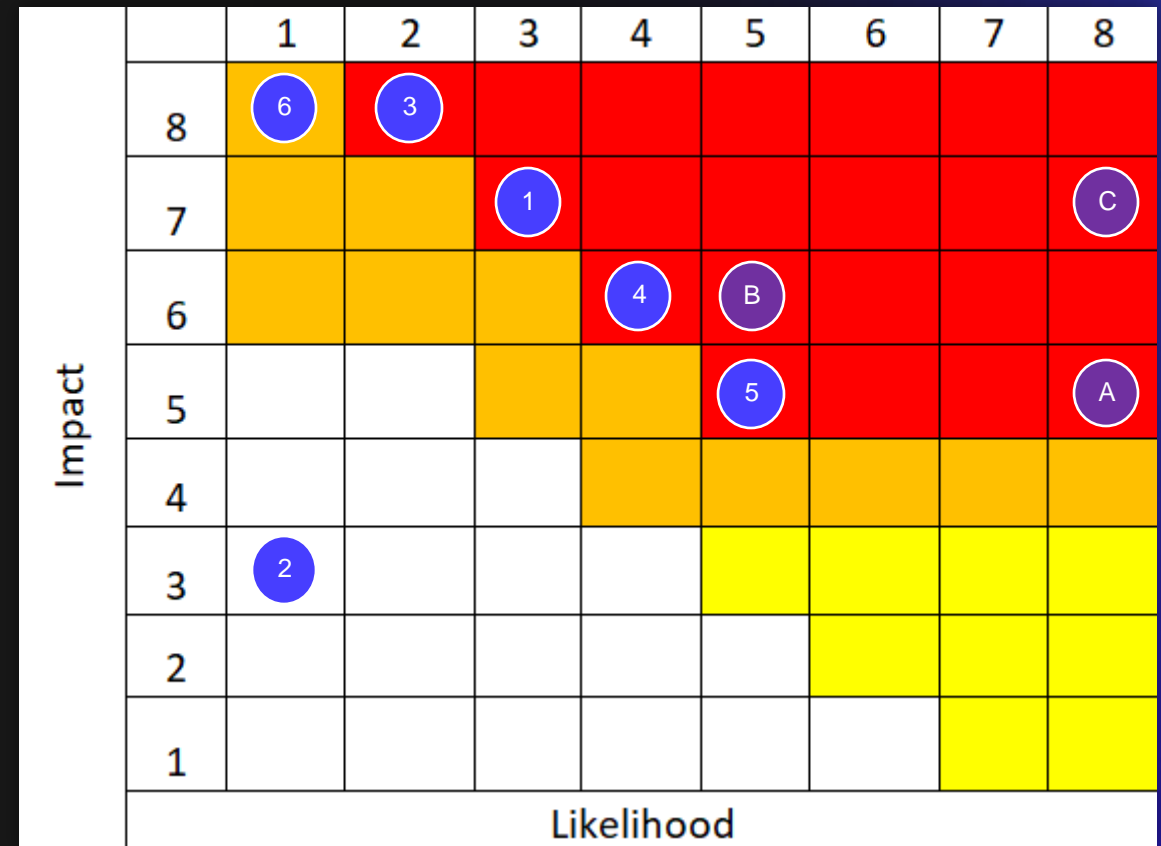
- 1 Post-intrusion ransomware
- 2 Business Email Compromise
- 3 Nation State Espionage / IP Theft
- 4 Financially-motivated data theft
- 5 Cryptomining attacks
- 6 Nation State Destructive Attacks
- A Commodity Remote Access Trojans
- B Network Intrusions
- C Critical Vulnerability Exploitation



● = Core Threat
 ● = Precursor to Core Threat

Threat Heat Map – Enterprise Software Company

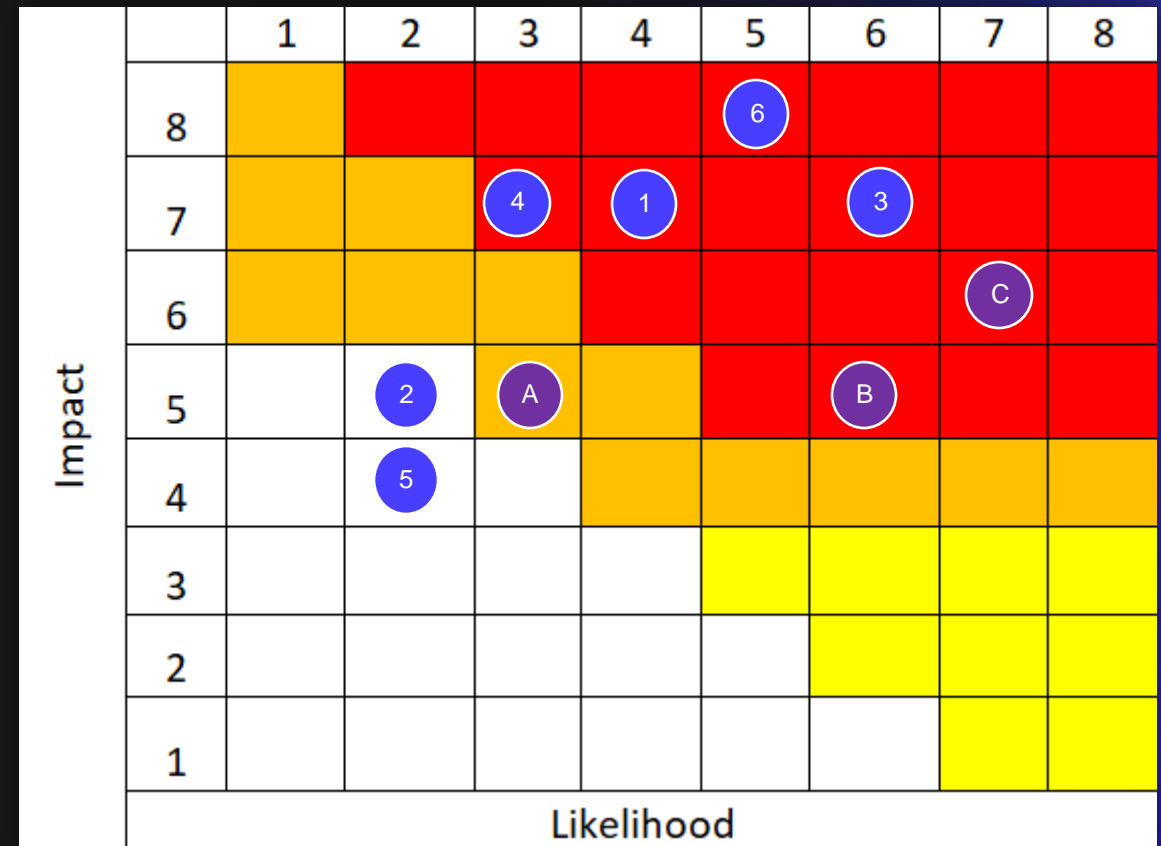
- 1 Post-intrusion ransomware
- 2 Business Email Compromise
- 3 Nation State Espionage / IP Theft
- 4 Financially-motivated data theft
- 5 Cryptomining attacks
- 6 Nation State Destructive Attacks
- A Commodity Remote Access Trojans
- B Network Intrusions
- C Critical Vulnerability Exploitation



● = Core Threat
 ● = Precursor to Core Threat

Threat Heat Map – DoD/Military Supplier/Contractor

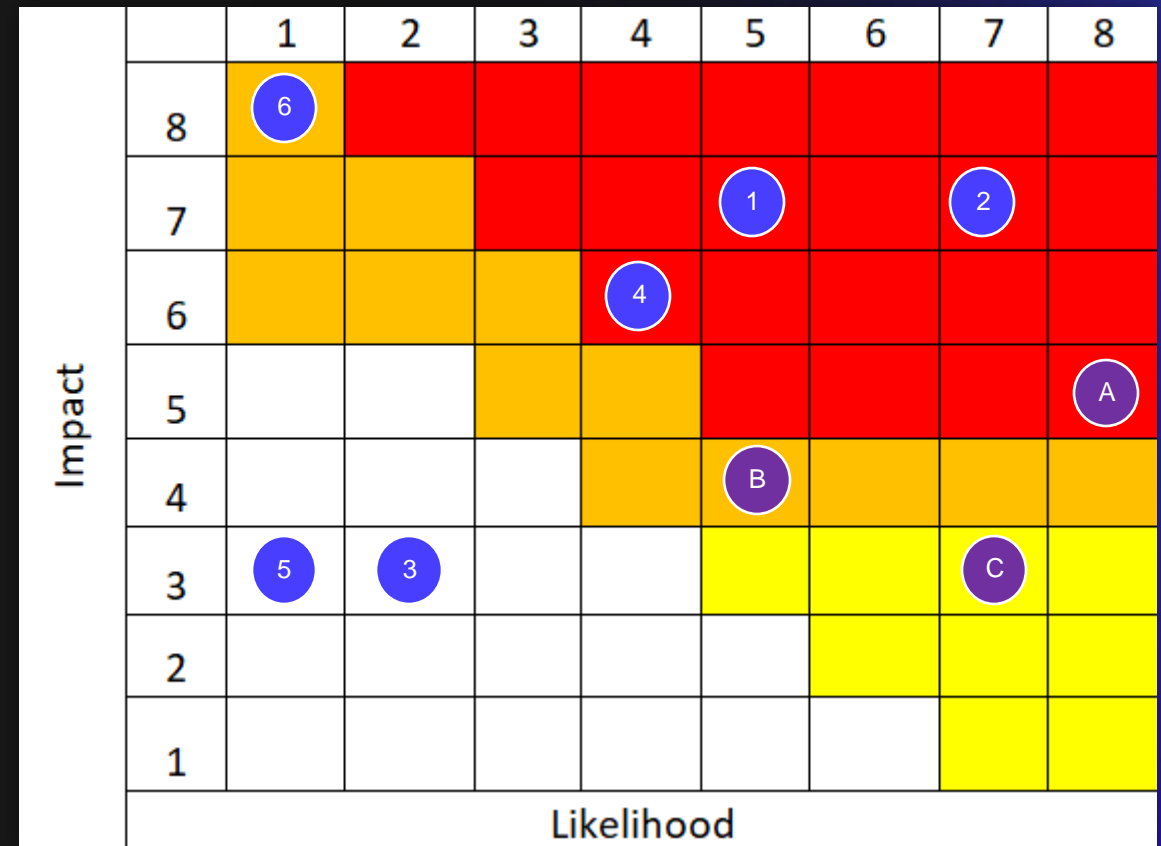
- 1 Post-intrusion ransomware
- 2 Business Email Compromise
- 3 Nation State Espionage / IP Theft
- 4 Financially-motivated data theft
- 5 Cryptomining attacks
- 6 Nation State Destructive Attacks
- A Commodity Remote Access Trojans
- B Network Intrusions
- C Critical Vulnerability Exploitation



● = Core Threat
 ● = Precursor to Core Threat

Threat Heat Map – Membership / Non-Profit Foundation

- 1 Post-intrusion ransomware
- 2 Business Email Compromise
- 3 Nation State Espionage / IP Theft
- 4 Financially-motivated data theft
- 5 Cryptomining attacks
- 6 Nation State Destructive Attacks
- A Commodity Remote Access Trojans
- B Network Intrusions
- C Critical Vulnerability Exploitation




= Core Threat


= Precursor to Core Threat

Priority Intelligence Requirements

- 1 Post-intrusion ransomware
- 2 Business Email Compromise
- 3 Nation State Espionage / IP Theft
- 4 Financially-motivated data theft
- 5 Cryptomining attacks
- 6 Nation State Destructive Attacks
- A Commodity Remote Access Trojans
- B Network Intrusions
- C Critical Vulnerability Exploitation

		1	2	3	4	5	6	7	8
Impact	8	6							
	7			3		1			
	6								
	5				2	B			A
	4				4				
	3							C	
	2						5		
	1								
			Likelihood						

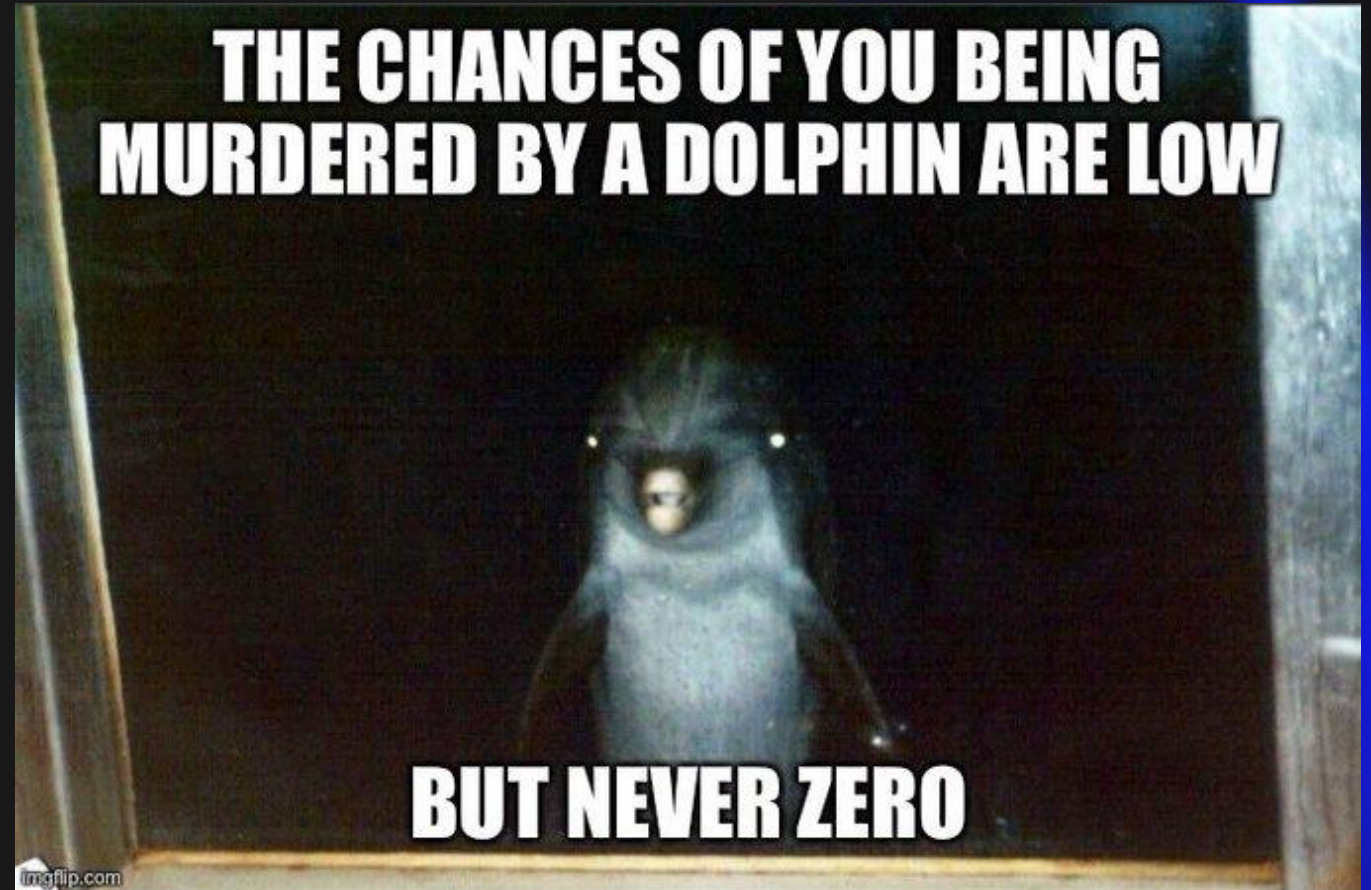
 = Core Threat

 = Precursor to Core Threat

Using a Heatmap to Support Your Security Program

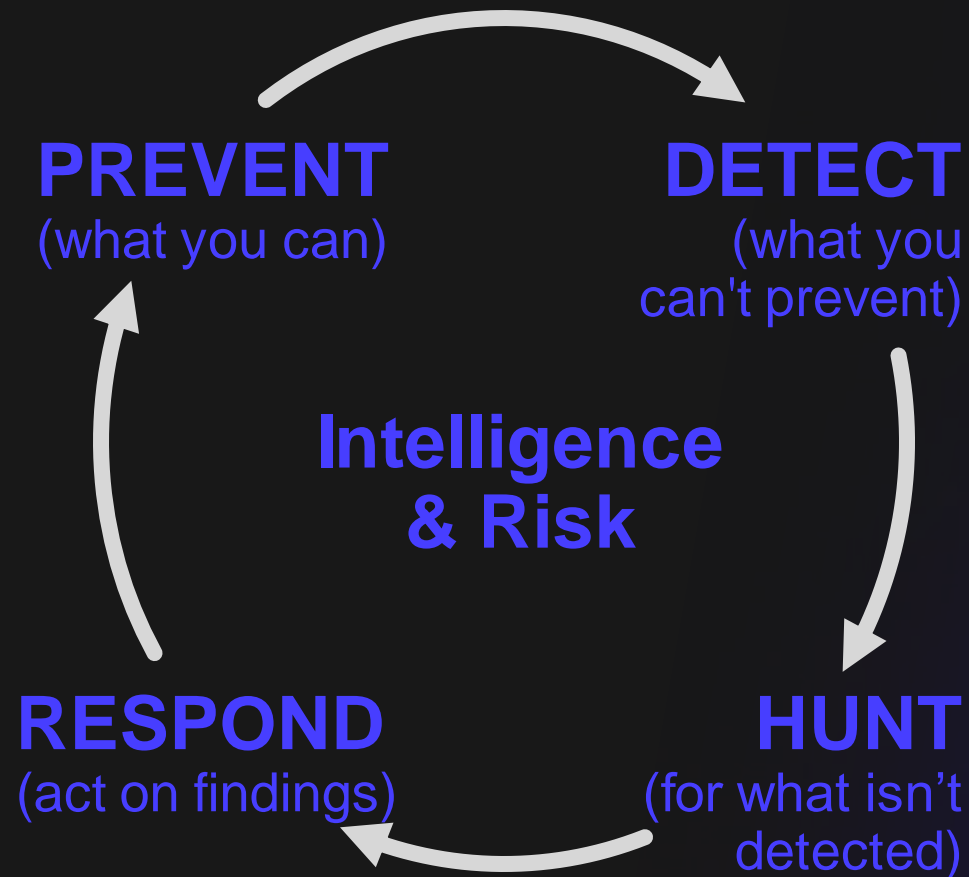
- Every organization is different. Risk Management is not, “one-size fits all.”
- Reasonable people can (and should) disagree or have a different view.
- The conversations this enables is more important than the “final version” or having the “right answer.”
- Use these conversations to build relationships and support for your program.
- The threat landscape, threat-actor methods, and your organization’s attack surface will change (and so should this map).

That's great,
now what do I
do about the
risk posed by
these threats?



Cyber Defense Cycle

Prevention, Detection, and Response



Cyber Defense Cycle

Prevention, Detection and Response

- You can't prevent everything.
- All prevention will fail or be circumvented.



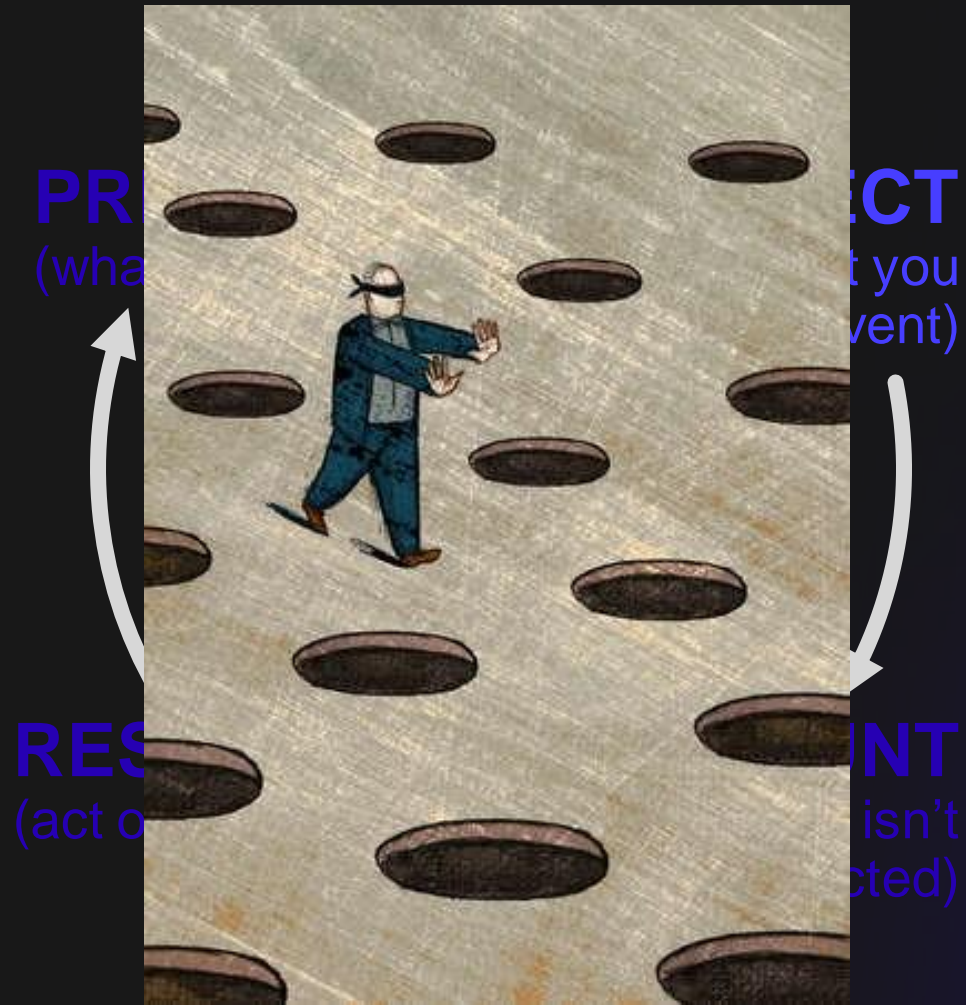
(act on findings)

(for what isn't detected)



Cyber Defense Cycle

Prevention, Detection and Response



- Requires visibility (SIEM / EDR / XDR) and someone to watch it (SOC).
- No such thing as perfect vision.

Cyber Defense Cycle

Prevention, Detection and Response



- Proactive exploration for undetected threats / vulnerabilities / assets.
- Not all hunting is effective; drive hunting into Detect objectives when possible.

Cyber Defense Cycle

Prevention, Detection and Response

- You must ACT to reduce risk and impact.
- Implement changes.



Cyber Defense Cycle

Prevention, Detection and Response

- Asset Management
- Patch Management
- Vulnerability Management
- Antivirus
- Secure Baseline Configurations

- Prepare and rehearse IR Plans
- Contain threats
- Evict/Eradicate Threat Actors
- Lessons learned: Could I prevent?
Could I detect sooner?

PREVENT
(what you can)

DETECT
(what you can't prevent)

**Intelligence
& Risk**

RESPOND
(act on findings)

HUNT
(for what isn't detected)

- Collect and Observe telemetry
- Apply intelligence to detect known threats
- Advanced analytics to identify suspicious behaviors
- Emphasize areas without Prevention controls.

- Proactive exploration for threat activity.
- Context-aware detectors to automatically uncover hard to detect threats
- Emphasize areas of Prevention and Detection gaps.

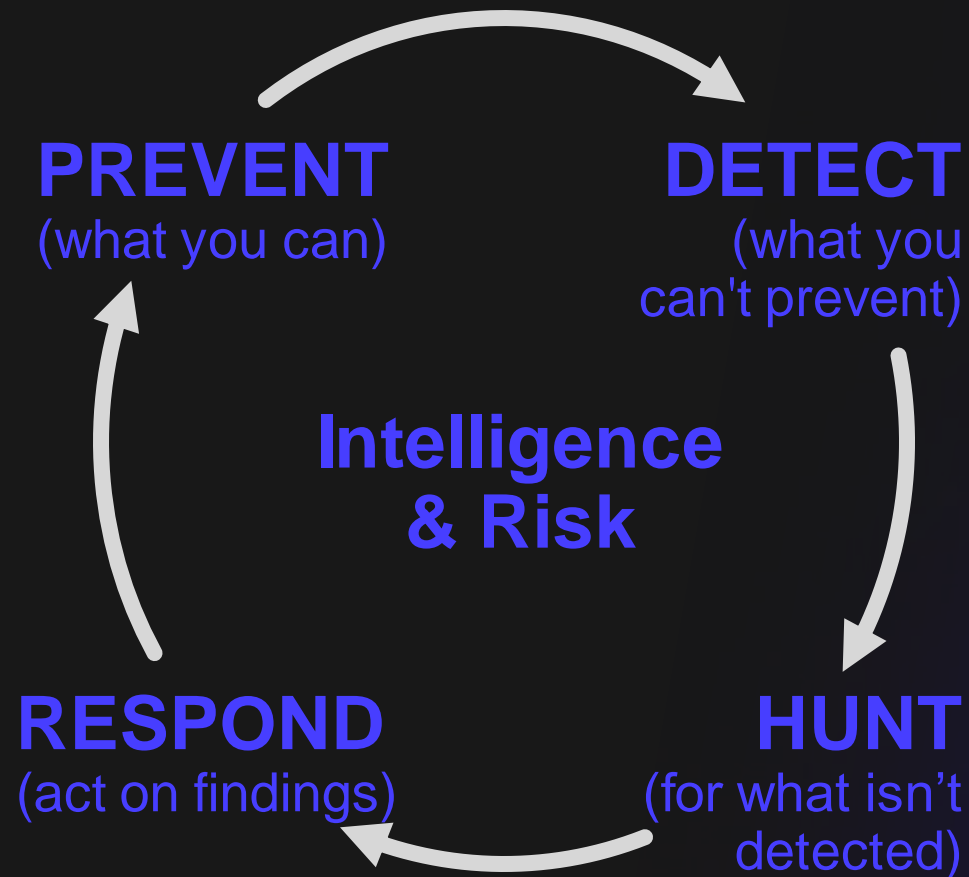
Log4j being exploited by nation-states

- Log4j vulnerabilities have been taken advantage of by nation-state actors
- Microsoft warned in December that nation state groups would target this vulnerability
- Threat actors aligned with Iran and China have been identified utilizing this vulnerability

Remove for Distribution

Cyber Defense Cycle – log4j / log4shell vulnerability

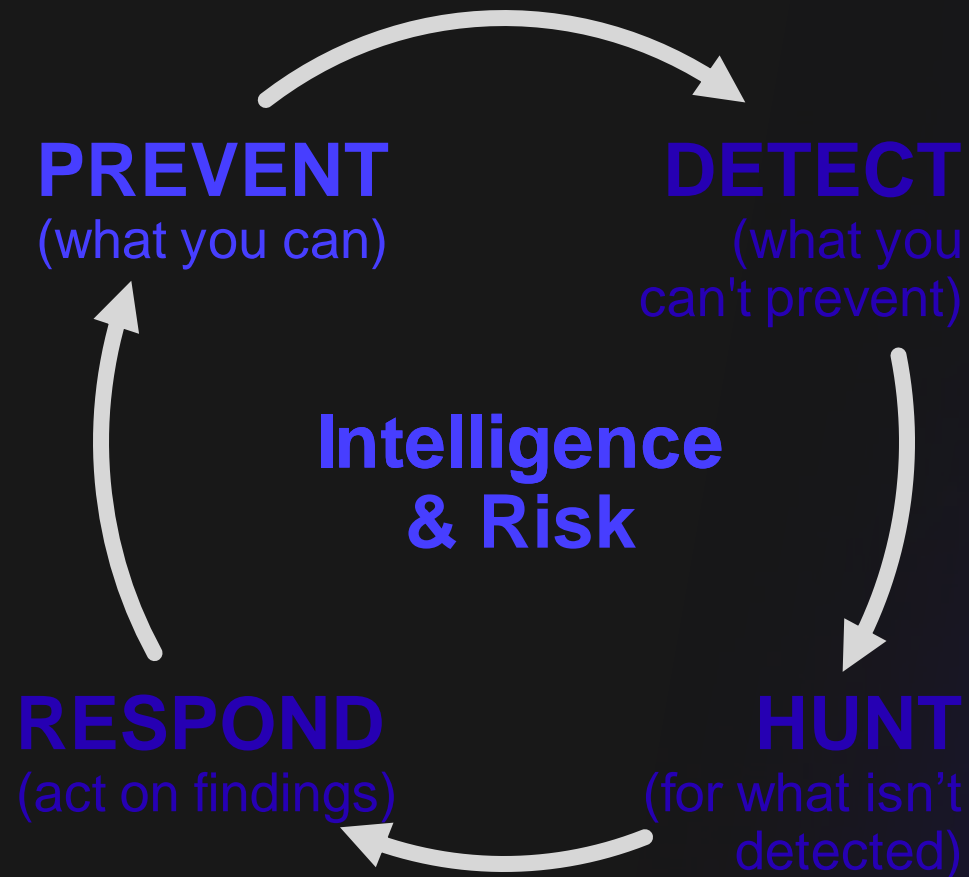
Prevention, Detection and Response



Cyber Defense Cycle – log4j / log4shell vulnerability

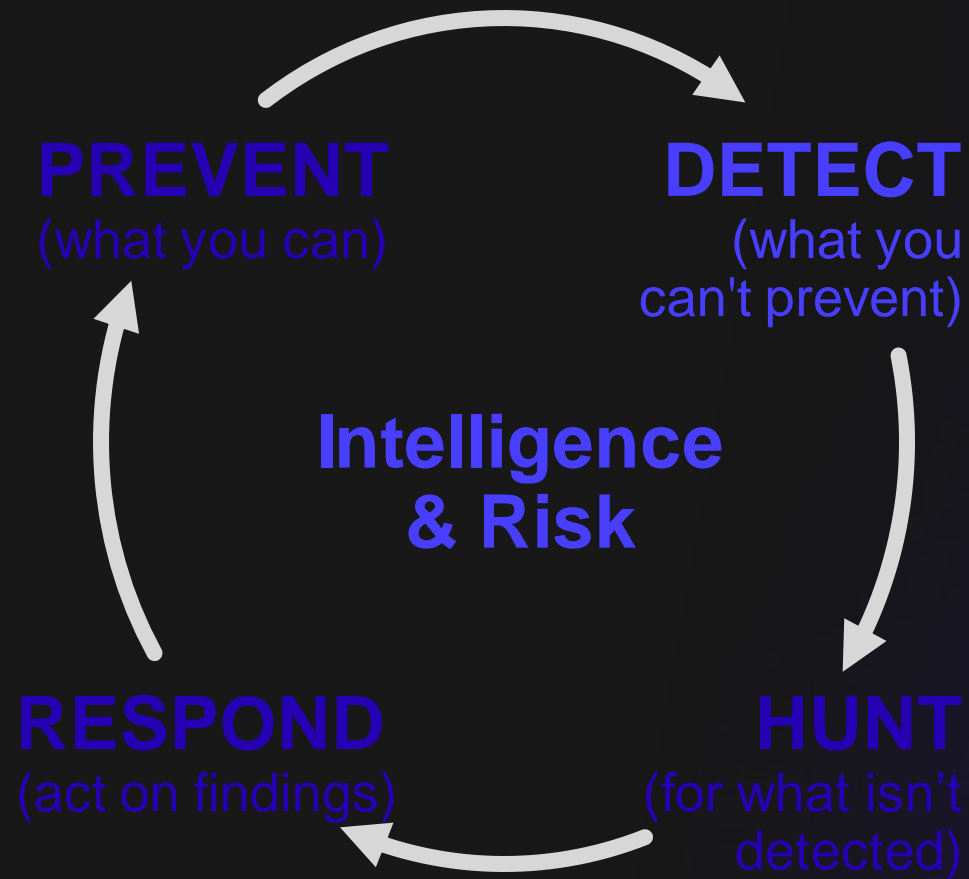
Prevention, Detection and Response

- You cannot prevent 0-day vulnerabilities or their exploitation



Cyber Defense Cycle – log4j / log4shell vulnerability

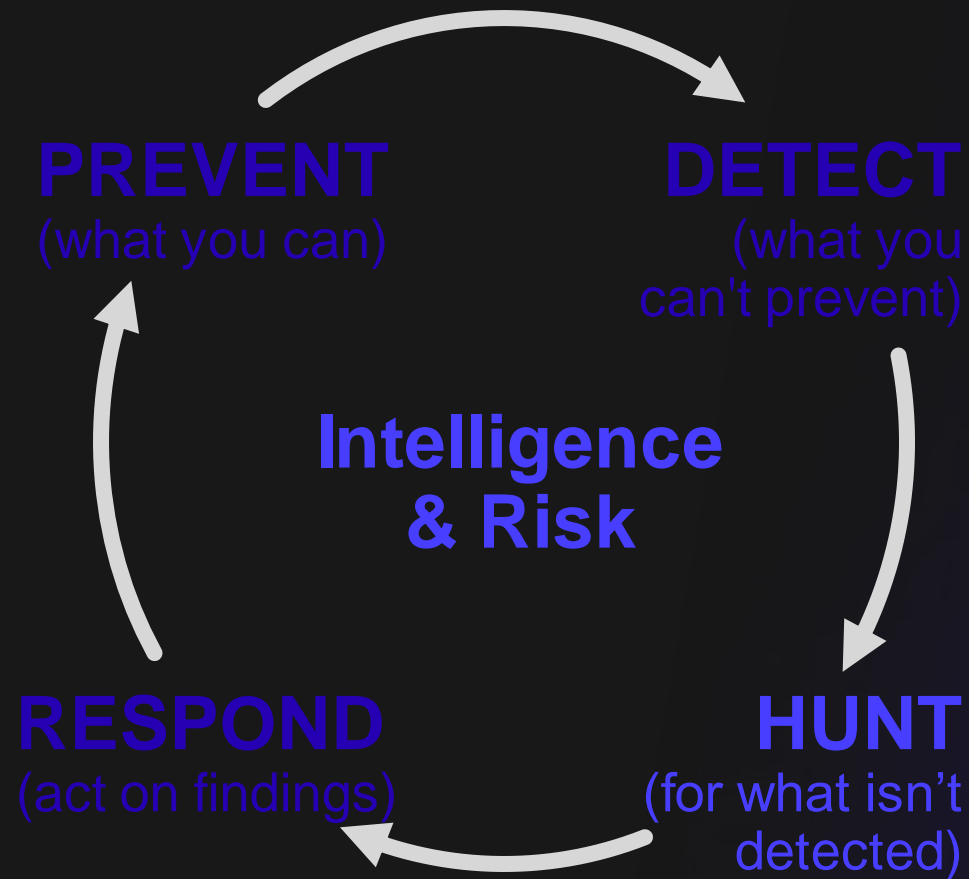
Prevention, Detection and Response



- Software Inventories / Software Bill of Materials
- Vulnerability Scanning
- You might detect post-exploitation activity

Cyber Defense Cycle – log4j / log4shell vulnerability

Prevention, Detection and Response

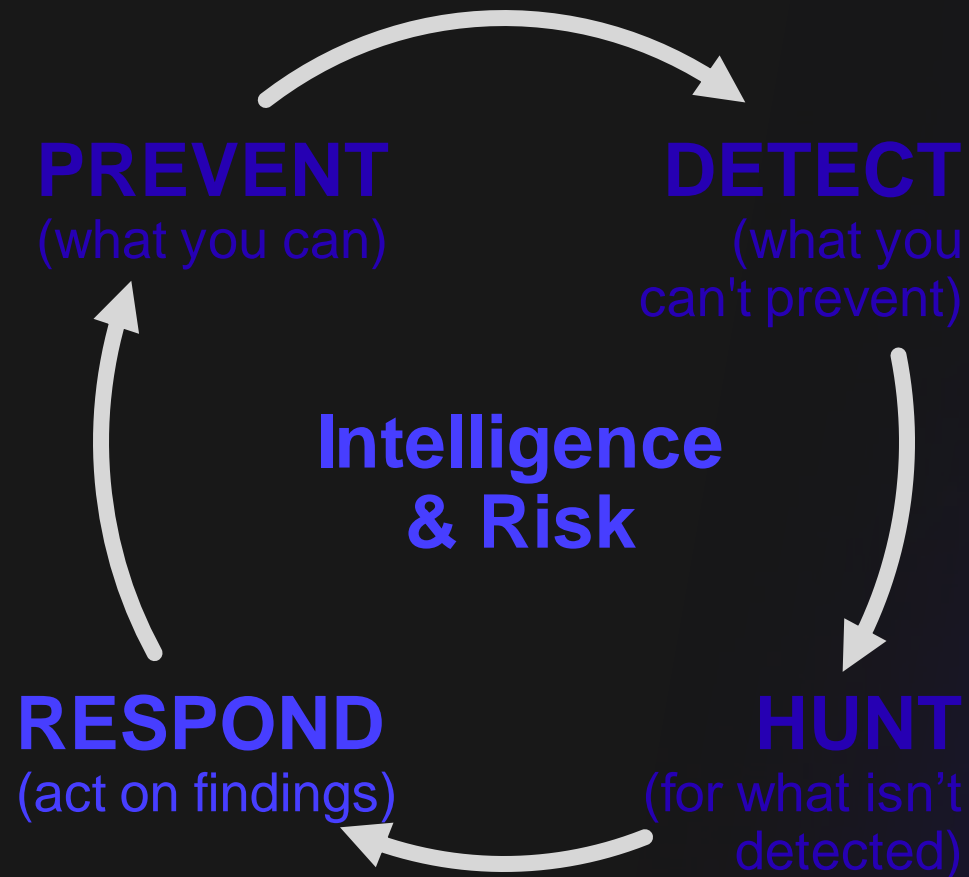


- Ask vendors and partners for known impact.
- Use open-source exploitation / testing tools on suspected assets.

Cyber Defense Cycle – log4j / log4shell vulnerability

Prevention, Detection and Response

- Deploy software updates.
- Implement WAF / NIPS countermeasures.
- Change configuration defaults.
- Deploy the 2nd patch ...and 3rd patch...



Remote code execution in Log4j (CVE-2021-44228)

- Scan and exploit utilised in conjunction with the Log4j vulnerability
- Exploitation was thought to be relatively trivial, and proof of concept code exists, including various workarounds for basic mitigations
- Successful exploitation would give a threat actor the ability to execute code remotely
- Apache has released version 2.17.1 to address all of the vulnerabilities

Remove for Distribution

Secureworks®

Products

Services

Why Secureworks

Partners

Blog > Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?

RESEARCH & INTELLIGENCE

Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?

Although Log4j vulnerability CVE-2021-44228 continues to be a serious threat, evidence suggests that the ability to remotely execute code is not as trivial as originally thought.

FRIDAY, DECEMBER 17, 2021

BY: COUNTER THREAT UNIT RESEARCH TEAM

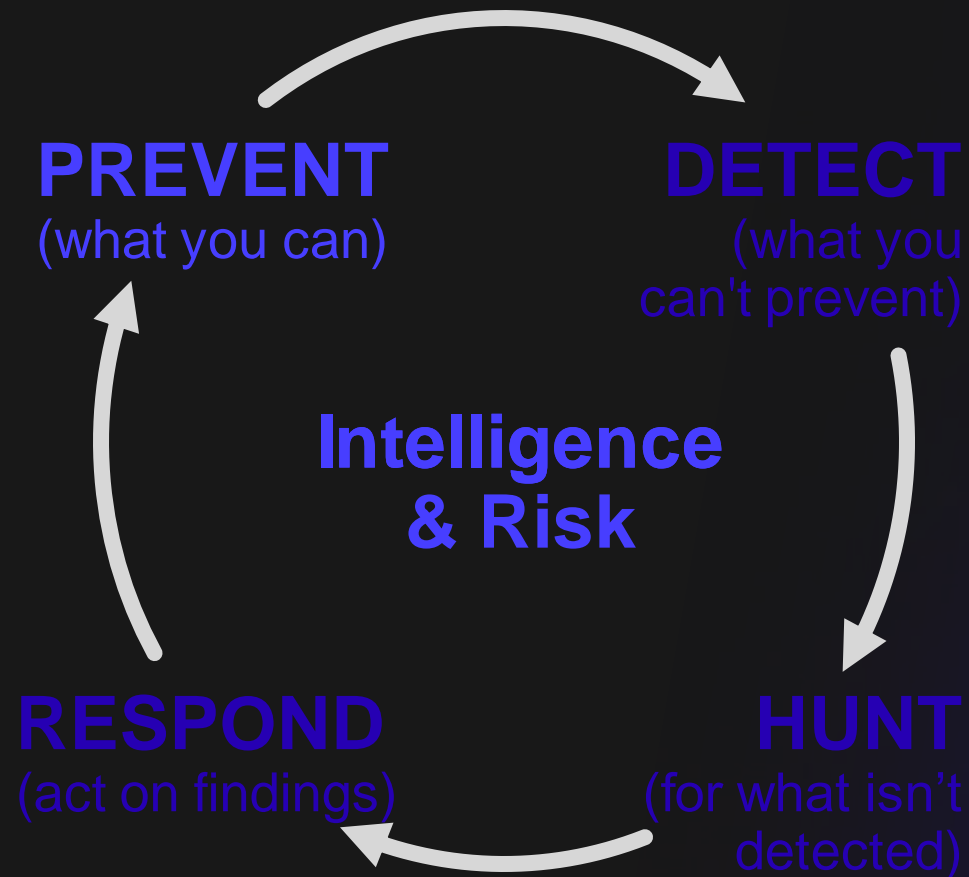


Since December 9, 2021, organizations have been working hard to understand their exposure to Log4j remote code execution vulnerability CVE-2021-44228 (also known as Log4Shell) and mitigate associated risks, either through patching or workarounds. Secureworks® Counter Threat Unit™ (CTU) researchers provided an [update](#) of the threat on December 15, but the situation has been evolving rapidly.

Cyber Defense Cycle – log4j / log4shell vulnerability

Prevention, Detection and Response

- Future exploitation attempts will fail as the vulnerability is closed.



Secureworks®

Thank You
