



DEEPSEC

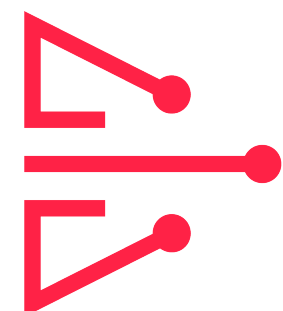
Micro Attack Simulations

Improving Cyber Resilience

Christian Schneider



Kevin Ott



**EXPLOIT
LABS**



Christian Schneider

@cschneider4711



Security Architect,
Whitehat Hacker & Trainer

Christian-Schneider.net



Kevin Ott

@kevin0x90



Senior Red Team Engineer
Exploit Labs GmbH

ExploitLabs.de



WHY WE'RE DOING THIS?

...



The Gap: Early-stage Organizations

Why traditional cybersecurity methods fall short for early-stage organizations

Resource Constraints

- › Limited staff dedicated to security
- › Budget constraints make full-scale Red Teaming costly

Low Maturity Level

- › Basic or nascent security controls
- › Lack of well-defined processes and documentation

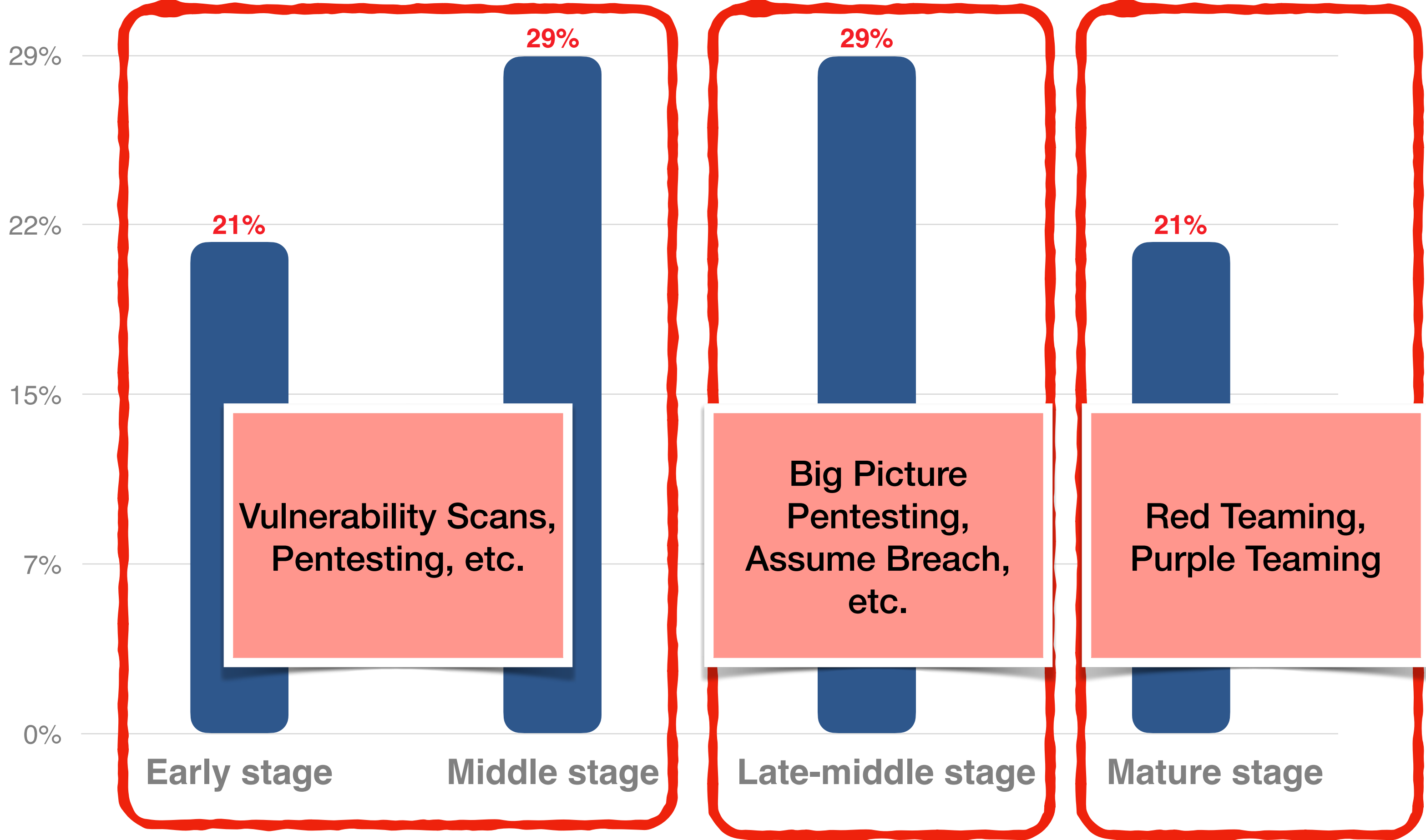
Skill Gap

- › May lack in-house expertise for advanced threat detection and mitigation
- › Limited experience in dealing with complex attacks

Time Sensitivity

- › Need quick wins to prove the ROI (Return on Investment) of security measures
- › Long periods for traditional Red Teaming might be impractical

How Organizations describe their Cybersecurity Maturity Levels



Classic 50:50 split with 50% of organizations below or at "Middle stage"

Source: "Cyber Resilient Organization Study 2021" by IBM based on Ponemon Institute Research Data
<https://www.ibm.com/resources/guides/cyber-resilient-organization-study/>



“Let’s be honest, most companies don't need a full blown red team, but still want to test procedures and reaction beyond traditional penetration testing.”

– *Unknown Source ;-)*



WHAT ARE MICRO ATTACK SIMULATIONS?

Targeting specific Security Controls



Focused, Feasible, Actionable

“Bite-sized Assessments”

Definition

- › Miniaturized and focused Red Team exercises
- › Targeting single or multiple specific security controls

Purpose

- › Quick validation of implemented controls
- › Identification of gaps in both technical and non-technical domains

Different Control Types

- › **Technical:** Firewalls, IDS/IPS, encryption, etc.
- › **Non-Technical:** Policies, escalation procedures, response playbooks

Applicability

- › Ideal for organizations with limited resources or expertise
- › A stepping stone to more comprehensive assessments

Trying to break specific Security Controls

Instead of a full-blown Red Team approach

- 01** | Identify security controls which are crucial to certain attack paths:
Usually via scenario-driven modeling approaches with different threat actors.
- 02** | Create attack simulations (esp. for “*Single Points of Failure*” Controls):
No need to test controls that the model states as not (yet) implemented.
Focus on implemented controls most relevant to withhold an attack path.
Stage test cases, with initial access defined as per control to test.
No need to “penetrate” from outside towards the specific object.
- 03** | Execute attack simulations:
Check expected outcome of a successful security control:
(*preventing access, stopping attack, triggering incident response processes, etc.*)
Incorporate Red Team style under-cover techniques when detective controls are tested.



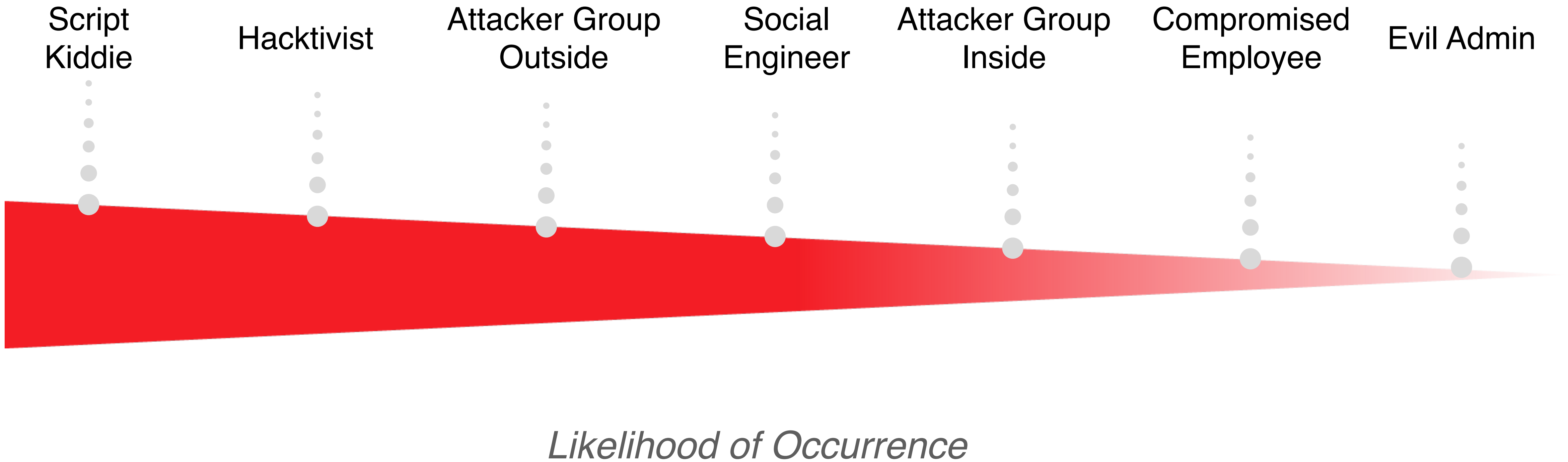
WHICH CONTROLS TO ATTACK?

Scenario-driven Attack-Tree Modeling



Define Threat Actors

Useful for Scenario-Driven Attack Paths



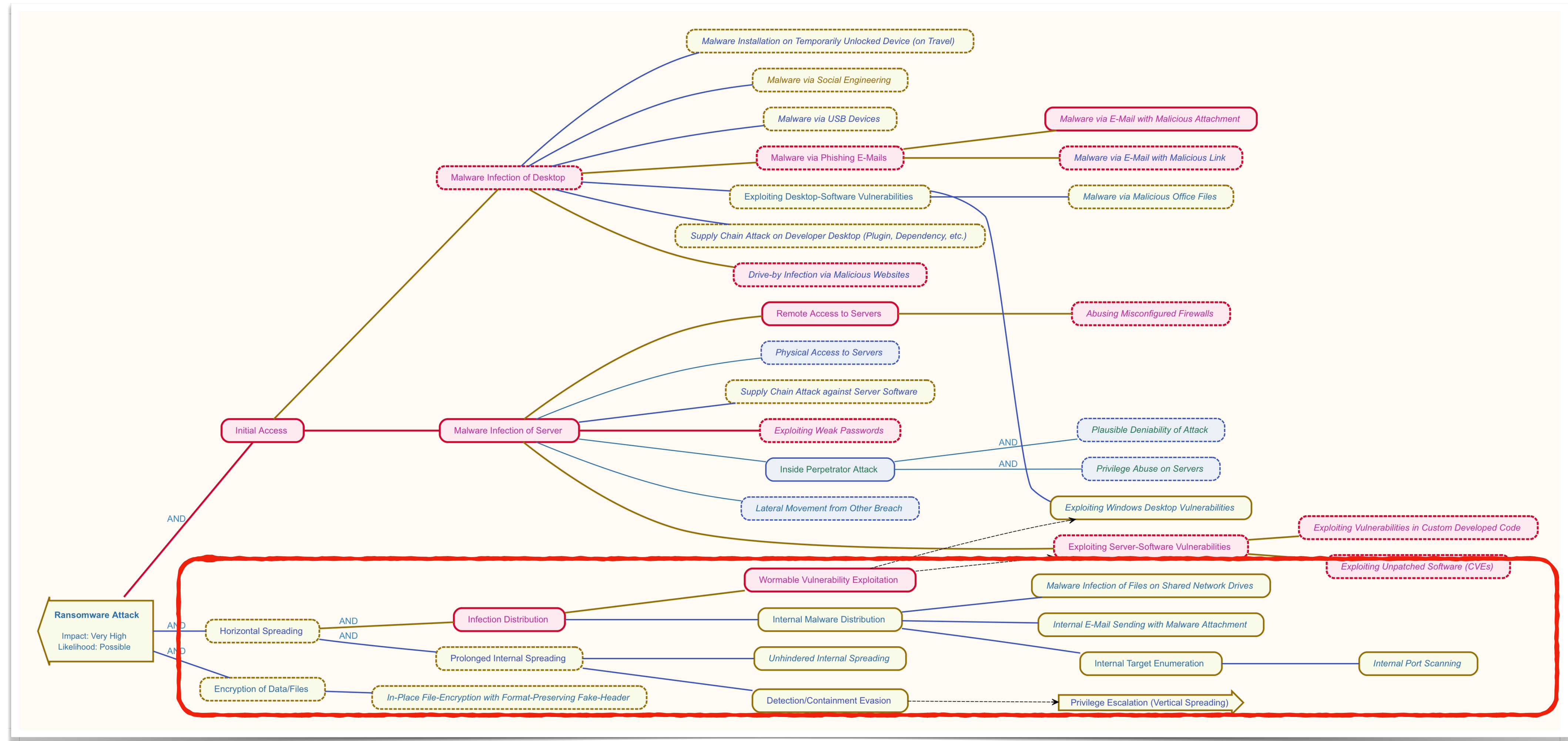
Define Attack Goals

With Impact on the Organization

Risk	<u>Impact</u>		ID	Title
<i>High</i>	Very High <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	A1	Ransomware Attack
<i>High</i>	Very High <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	A38	Sensitive Data Publication (Double Ransom)
<i>Medium</i>	High <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	A39	Access Brokerage

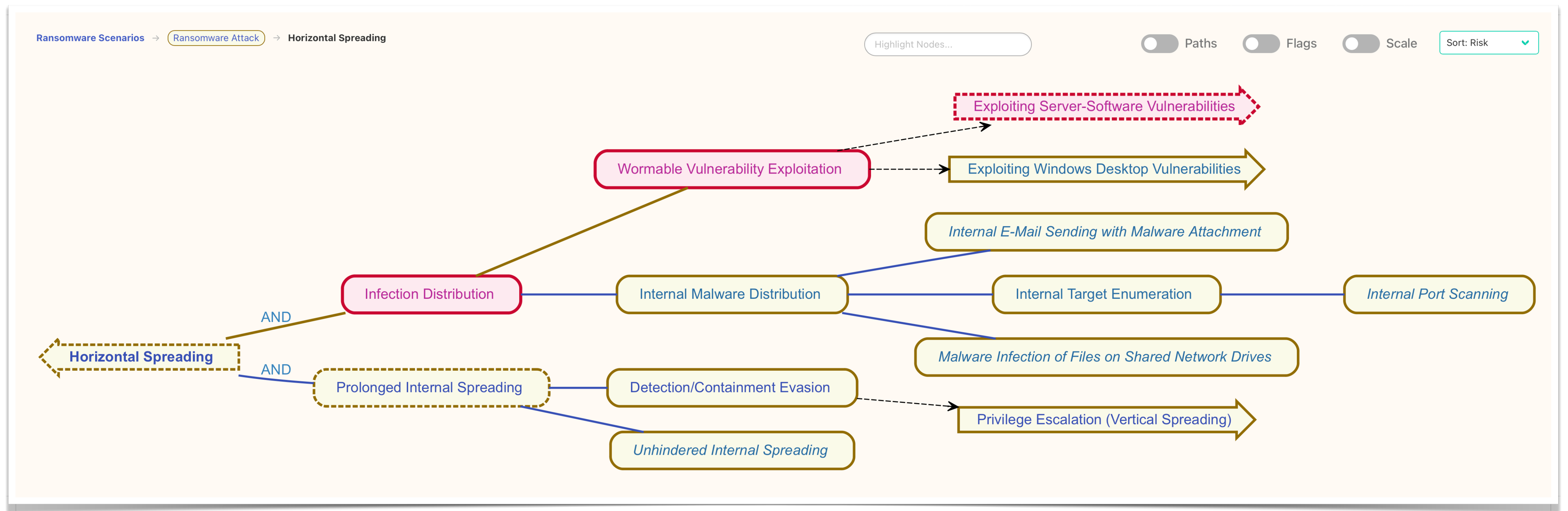
Define Attack Paths leading to Goals

OR / AND Connected



Define Attack Paths leading to Goals

OR / AND Connected



Assign Actors & Complexity

at the leafs of the tree to determine likelihood

Title	Controls	Children	<u>Actor</u>	Complexity	Likelihood
<i>1 × Actor: Hactivist</i>					
Malware via Phishing E-Mails	0 / 2	2 Sub	Hactivist	Ordinary	Likely
<i>4 × Actor: Attacker Group Outside</i>					
Drive-by Infection via Malicious Websites	0 / 2	0 Sub	Attacker Group Outside	Simple	Likely
Malware Installation on Temporarily Unlocked Device (on Travel)	0 / 1	0 Sub	Attacker Group Outside	Complex	Possible
Malware via USB Devices	0 / 1	0 Sub	Attacker Group Outside	Complex	Possible
Supply Chain Attack on Developer Desktop (Plugin, Dependency, etc.)	0 / 2	0 Sub	Attacker Group Outside	Very Complex	Unlikely

Add Security Controls to Nodes

The more towards the root, the more *generic* it is.
The more towards the leafs, the more *specific* it is.

Drive-by Infection via Malicious Websites 0 / 2 0 Sub Attacker Group Outside Simple Likely T ▼

Edit Controls Move Delete Duplicate

Visiting malicious websites can also lead to malware infections on desktops. These websites may contain malicious code or exploit kits that can infect a user's computer with malware without their knowledge.

Attack Paths

Propose Suggest

Flag

Add new or search existing Development Medium Add

Security Controls Flag

Direct Controls

- Remove Effect: High Browser Security Hardening
- Remove Effect: Medium Proxy-based Web Malware Filtering

Sub-Tree Controls

Propose Suggest

Attack Goals: Ransomware Attack Access Brokerage

Out-of-Scope

Different Controls have Different Effects

Useful for simulating which control combos should be challenged

The screenshot shows a web interface for managing security controls. At the top, there is a search bar with the placeholder text "Add new or search existing". To the right of the search bar are three dropdown menus: "Development", "Medium", and "Add". Below the search bar is a large light green panel titled "Security Controls". In the top right corner of this panel is a "Flag" button. Under the "Security Controls" heading, there is a section for "Direct Controls". This section contains two items, each with a "Remove" button and a dropdown menu for "Effect". The first item is "Browser Security Hardening" with an "Effect: High" dropdown. The second item is "Proxy-based Web Malware Filtering" with an "Effect: Medium" dropdown. A red rectangular box highlights the "Effect" dropdown menus for both items. Below the "Direct Controls" section is a section for "Sub-Tree Controls". At the bottom of the interface, there are two yellow buttons: "Propose" and "Suggest".

Define Validation Steps for Controls

Use these later as instructions for executing the Micro Attack Simulations...

Authentication-enforcing Web-Proxy

Operations

Medium

Preventive

Edit

Delete

Duplicate

An authentication-enforcing web-proxy is a security control that is used to enforce authentication of users before they are allowed access to the internet. It acts as an intermediary between the user's device and the internet, intercepting all requests made by the user and checking them against a set of authentication credentials. If the user is not authenticated, the web-proxy will deny access to the requested resources.

Attack Likelihood Reduction

Flag

• Medium Effect on: **Communication Channel via Web-Proxy**

Validation

- Conduct penetration testing to simulate real-world attacks and attempt to bypass the authentication-enforcing web-proxy.
- Perform vulnerability scanning to identify any potential weaknesses or misconfigurations in the implementation.
- Test the authentication mechanism by attempting to authenticate with both valid and invalid credentials.
- Monitor and analyze network traffic to ensure that all requests are being intercepted and checked by the web-proxy.
- Test the denial of access functionality by attempting to access resources without proper authentication and verifying that access is indeed denied.
- Review and validate the logging and auditing capabilities of the web-proxy to ensure that all relevant events are being logged for monitoring and forensic purposes.

Protection 1 • Level 3 • Effect 14 • ROI 1

Define Validation Steps for Controls

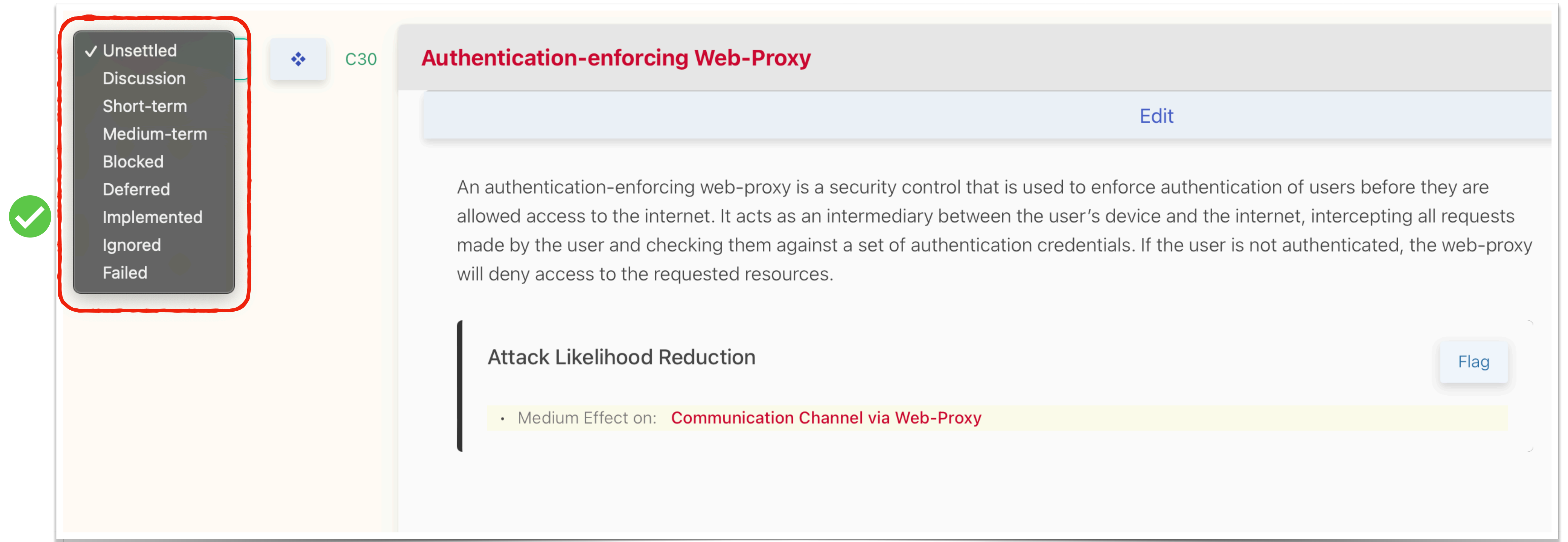
Making the execution of Micro Attack Simulations repeatable

Validation

- Use automated tools such as Microsoft's Active Directory Best Practices Analyzer (AD BPA) or third-party tools to scan and audit the Active Directory configuration.
- Manually review the configuration settings and compare them against industry best practices and security guidelines.
- Verify that the auditing and logging settings are correctly configured to capture relevant events and changes in the Active Directory environment.
- Ensure that the audit logs are being regularly monitored and reviewed for any suspicious activities or unauthorized changes.
- Test the effectiveness of the configuration audits by intentionally misconfiguring certain settings and verifying if they are identified during the audit process.
- Conduct periodic penetration testing or vulnerability assessments to identify any misconfigurations that might not be detected by the configuration audit alone.
- Regularly update and patch the Active Directory servers to address any known vulnerabilities or weaknesses that could be exploited by attackers.
- Document the results of the configuration audits and any steps taken to remediate identified issues.

State which Controls are Implemented

Used to simulate which controls are the “Achilles Heels” for an attack path



The screenshot shows a user interface for managing security controls. On the left, a vertical menu lists control states: Unsettled (checked), Discussion, Short-term, Medium-term, Blocked, Deferred, Implemented, Ignored, and Failed. A red box highlights this menu, and a green checkmark icon is positioned to its left. The main content area displays a control titled 'Authentication-enforcing Web-Proxy' with ID 'C30'. Below the title is an 'Edit' button. The control's description reads: 'An authentication-enforcing web-proxy is a security control that is used to enforce authentication of users before they are allowed access to the internet. It acts as an intermediary between the user's device and the internet, intercepting all requests made by the user and checking them against a set of authentication credentials. If the user is not authenticated, the web-proxy will deny access to the requested resources.' Below the description is a section for 'Attack Likelihood Reduction' with a 'Flag' button. A bullet point indicates a 'Medium Effect on: Communication Channel via Web-Proxy'.

✓ Unsettled
Discussion
Short-term
Medium-term
Blocked
Deferred
Implemented
Ignored
Failed

❖ C30

Authentication-enforcing Web-Proxy

Edit

An authentication-enforcing web-proxy is a security control that is used to enforce authentication of users before they are allowed access to the internet. It acts as an intermediary between the user's device and the internet, intercepting all requests made by the user and checking them against a set of authentication credentials. If the user is not authenticated, the web-proxy will deny access to the requested resources.

Attack Likelihood Reduction

Flag


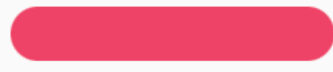
- Medium Effect on: **Communication Channel via Web-Proxy**

Find “*Single Points of Failure*” & Combos

Using Monte Carlo simulations of implemented controls

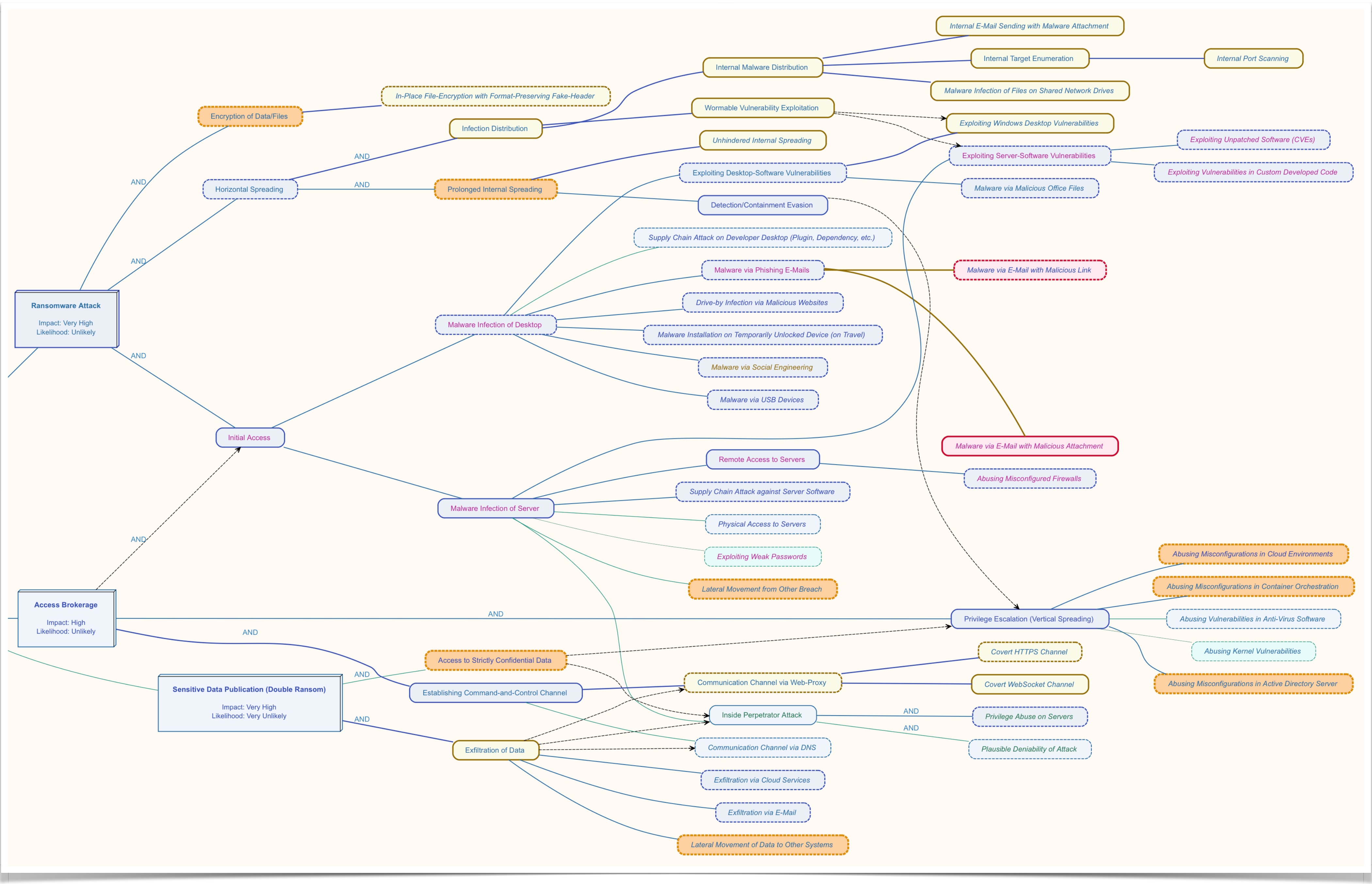
2 Controls (excluding *Singe Points of Failure*) with high **failure** score when part of a combination:

Based on 21606 checked combos (pairs of two and three). Click on controls to flag them for further inspection.

Flag	ID	Title	Kind	Effort	Status	Score	
🚩	C25	Backup and Recovery	Operations	Low	Implemented	100 %	
🚩	C5	Network Segmentation	Operations	High	Implemented	100 %	

4 **Singe Points of Failure**

- ▶ Cloud Service Hardening
- ▶ Container Hardening (OWASP CSVS, CIS-Benchmarks, etc.)
- ▶ Regular Active Directory Configuration Audits
- ▶ Resource-based Data Encryption of Strictly Confidential Data





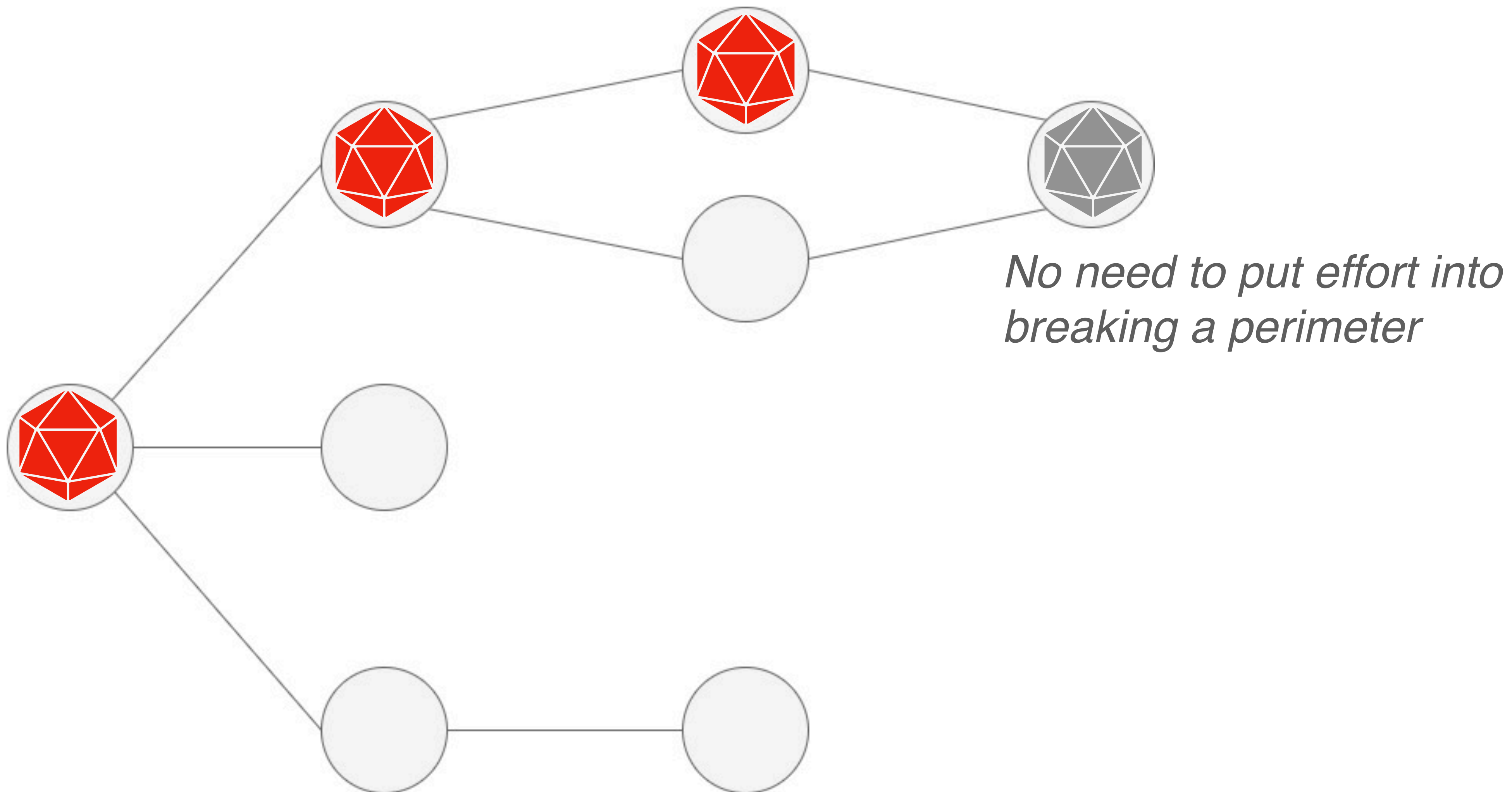
CREATING MICRO ATTACK SIMULATIONS

Trying to break the chosen Controls



Scenario-based Attack Path Selection

Choose which nodes to skip and which to attack



Example: Abuse of AD Misconfiguration

Objective

Assess vulnerability to attacks targeting misconfigured AD to control the domain controller. Test effectiveness of PAM solution.

Controls

AD security settings, Best Practices Analyzer scans, PAM tools and their sensitivity.

Micro Attack Simulation

Utilizing techniques from the SpecterOps paper on "ESCALATE" (ESC1), aggressively exploit known and potential Active Directory misconfigurations to seize control of the domain controller.

Attempt to move enduser accounts into privileged groups to challenge PAM tools and intrusion detection capabilities.

Example: Covert Communication Channels

Objective

Evaluate the ability to detect and block covert malware communication via WebSockets and DNS.

Controls

Network intrusion detection systems (NIDS), application-layer firewalls, DNS monitoring tools, Endpoint Protection (EDR/EPP).

Micro Attack Simulation

Deploy simulated malware (RAT, C2) using covert WebSocket and DNS channels from a compromised internal system to challenge the organization's detection and blocking capabilities.

Example: **Unhindered Ransomware Spreading**

Objective

Test the ability to detect custom-built advanced ransomware spreading from endpoints to servers.

Controls

Endpoint detection and response (EDR) solutions, ransomware detection, heuristic analysis tools.

Micro Attack Simulation

Run custom-built ransomware designed to stealthily encrypt files (while preserving headers) on selected endpoints and servers (to simulate lateral movement) in timed intervals (to simulate spreading).

Example: Insufficient Crisis Management

Objective

Evaluate the organization's response to ransomware mails and "*should've been detected*" indicators of compromise on servers.

Controls

Crisis management procedures, incident detection and alerting mechanisms.

Micro Attack Simulation

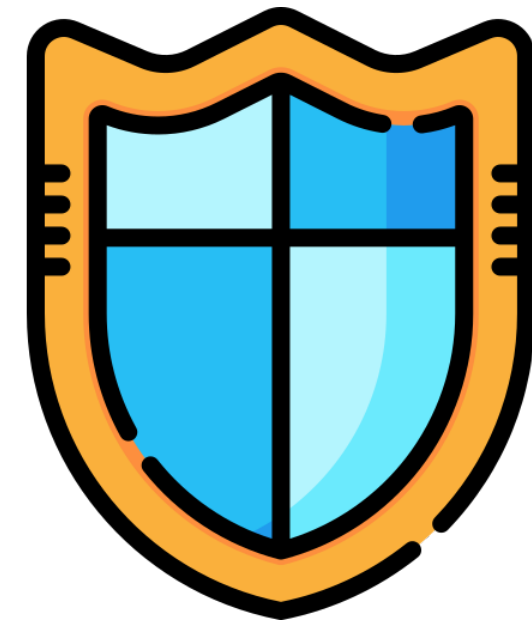
Deploy ransom notes, trigger high-severity indicators of compromise, and send ransom emails to official channels.

Include proofs of breach (data excerpts and/or dropping IoCs) to test tracing and incident escalation procedures.

Case Study — Involved Parties



White Team
(Crisis Management)



Blue Team
(SOC)



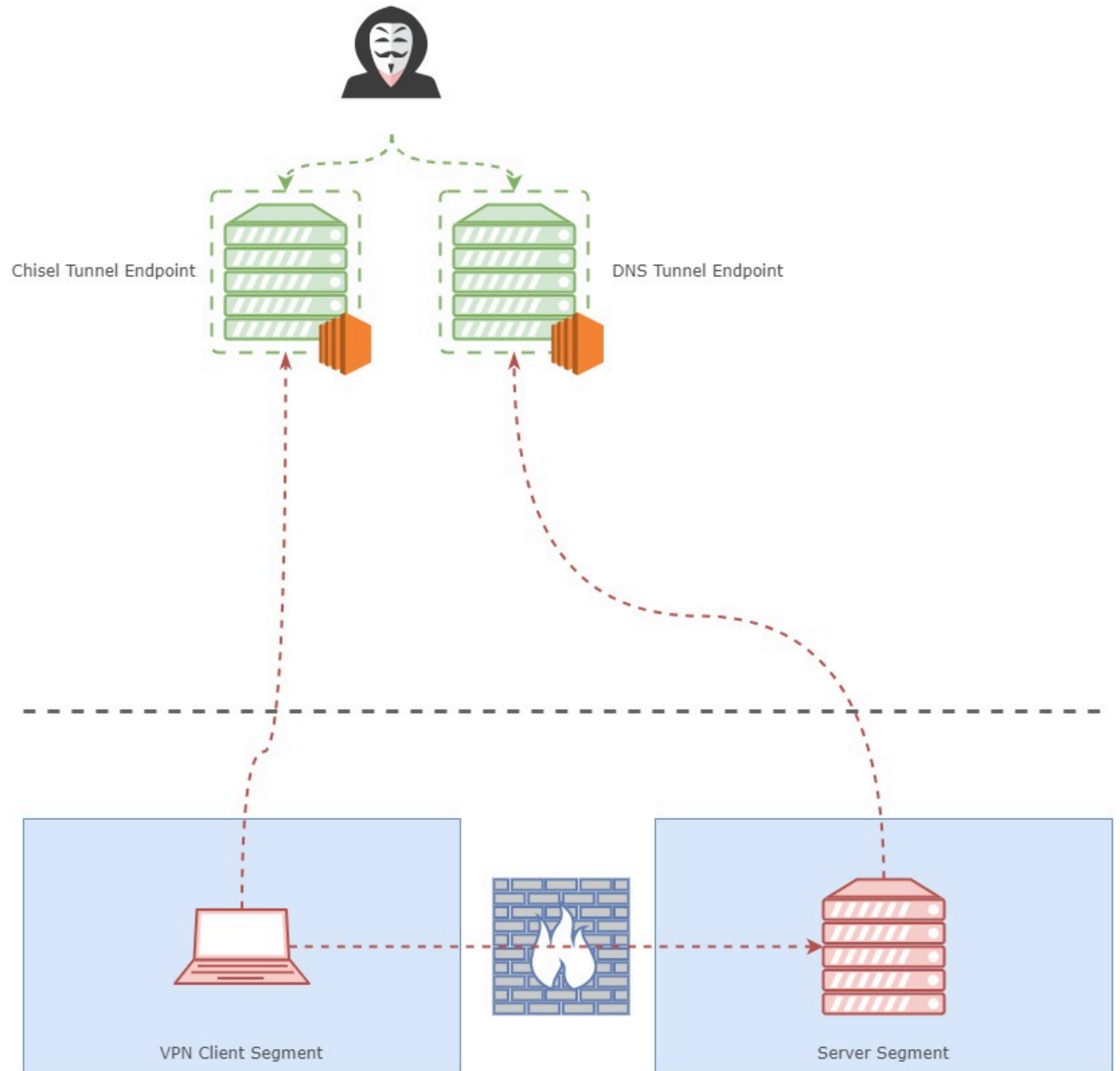
Data Protection Officer
(Public Contact)



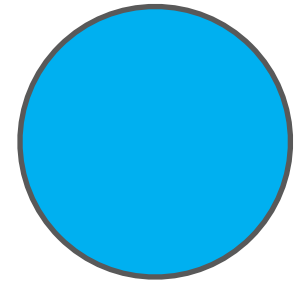
Red Team
(External)

Case Study: Attack Path Setup

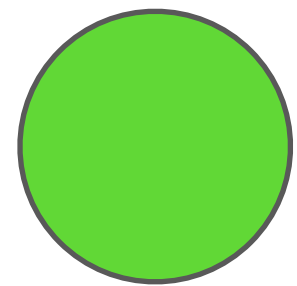
- Customized Chisel
(remove known network and file signatures)
- Custom developed DNS C2 endpoints in cloud
- Custom developed ransomware
- Access target server via VPN client
(as per scenario)



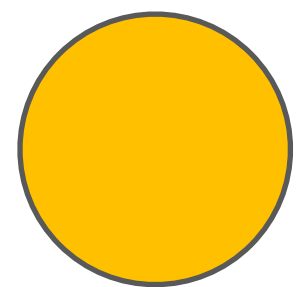
Case Study — Event Types in Timeline



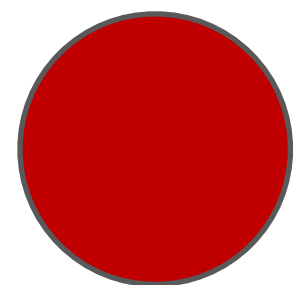
Context information in timeline.



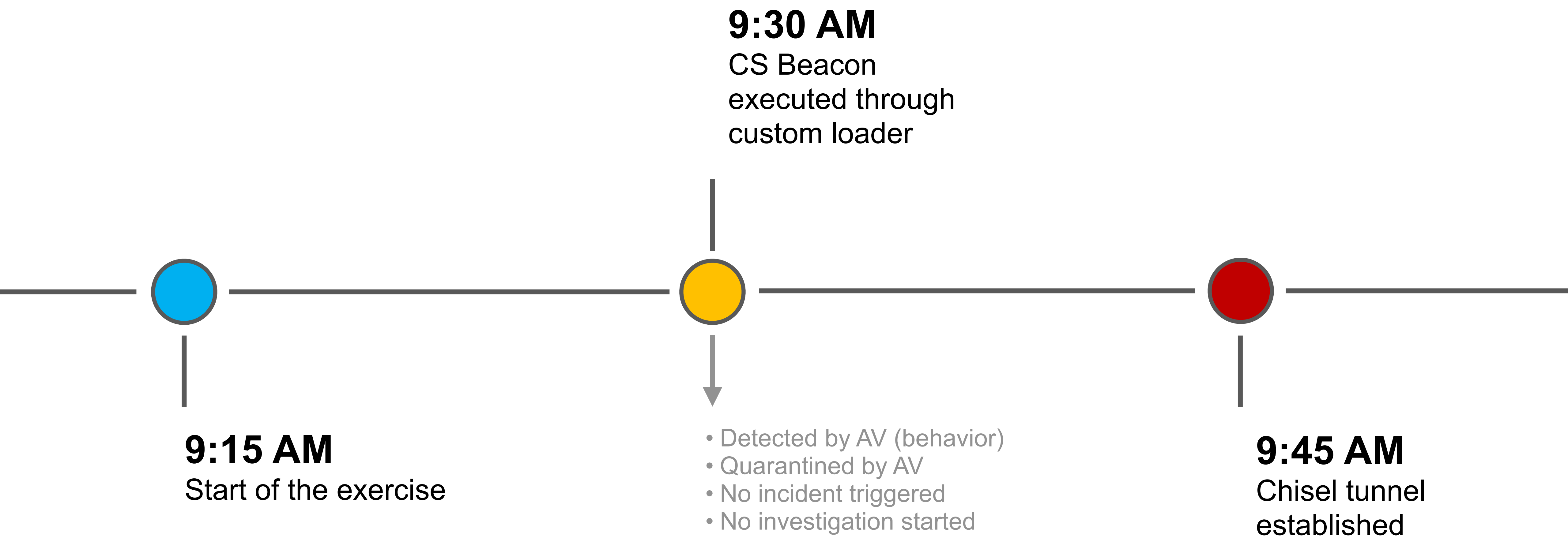
Event was detected and investigation was started.



Event was detected, but no investigation started.

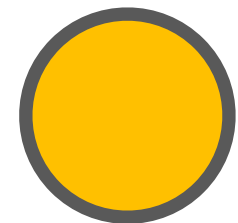


Neither detection nor investigation.



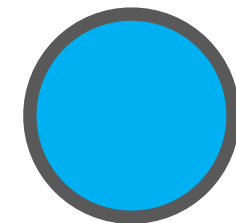
10:00 AM - 10:15 AM

Running all sorts of noisy
"ransomware-like" tools and
commands tunneled via
Chisel Server



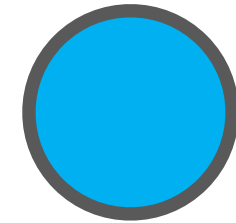
Port & Vuln Scans

- Alerted by AV as suspicious traffic
(Including Critical rated)
- No incident triggered
- No investigation started



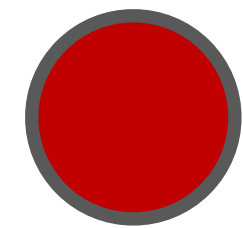
11:15 AM

Target servers *not*
accessible —
Executing AD enumeration



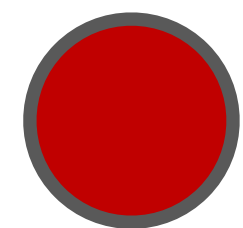
1:15 PM

Found critical
vulnerability allowing
us to compromise AD
(ESC1)



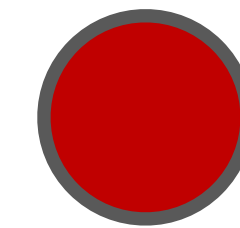
3:30 PM

Executed attack on AD (ESC1), becoming domain admin (global)



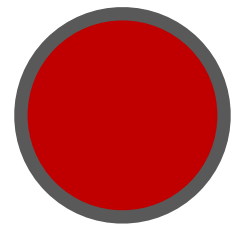
3:40 PM

Added our user to server admin group
(no monitoring on privileged groups)



3:45 PM

Accessed target server, bypassing PAM solution



3:57 PM

Ransomware executed on server, all files in directories encrypted on real TTPs like Salsa20 as algorithm

[2] Your data has been stolen and encrypted

From  LockBit Ransom <lockbit-ransom-4@protonmail.com>

☆ Nov 14, 2022

To



>>>>> Your data has been stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay, the sooner your company will be safe.

To get the encrypted data back, transfer 40000 \$ in Bitcoin to the following address:



If you are unsure how to acquire and transfer the require Bitcoin, follow the instructions here: <https://www.bitcoin.com/get-started/how-to-buy-bitcoin/>

>>>>> What guarantee is there that we won't cheat you

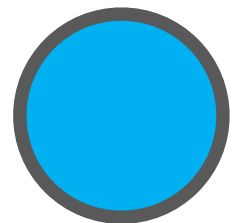
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group, and we want nothing more than money. If you pay, we will provide you with the encryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you the decryptor or delete your data after you pay, nobody will pay us in the future!

>>>>>>> You need to contact and decrypt one file for on tor darknet sites with your personal ID.



10 PM

first ransom e-mail to forwarded to incident responders on duty



4:45 PM

Second ransom e-
increased amount
75000 \$


We have Domain Admin in your Active Directory

From  LockBit Ransom <lockbit-ransom-4@protonmail.com>

☆ ↗ @ Nov 14, 2022

To



>>>>> We have Domain Admin in your Active Directory and bypassed your Privileged Access Management solution 

If you don't pay the ransom, we will sell the privileged accounts of your corporate server network to the highest bidder on a darknet auction. Your time is running up and the earlier you pay, the higher the chance that no attacker group will utilize this access foothold.

To stop our running auction, transfer 75000 \$ in Bitcoin to the following address immediately:



If you are unsure how to acquire and transfer the require Bitcoin, follow the instructions here: <https://www.bitcoin.com/get-started/how-to-buy-bitcoin/>

>>>>> What guarantee is there that we won't cheat you

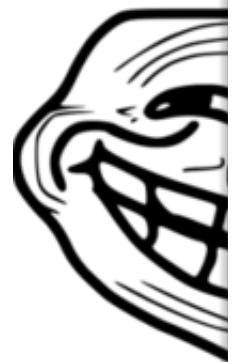
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group, and we want nothing more than money. If you pay, we will stop the running auction and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it.



PM
ts that the
real, still
ation, we
n full access

5:15

IR not
compr
and ac
mainta



enable_acco
Original user
Updated userA

Don't think you can stop us...

From  LockBit Ransom <lockbit-ransom-4@protonmail.com>

☆ ↗ @ Nov 14, 2022

To



Monday, November 14th, 2022 at 6:20 PM




We noticed you disabled our foothold ... Try again... ;)


We've re-enabled it ... Time is against you!



36.18 KB 2 files attached



 we-reenable.jpeg 13.67 KB

 and-are-still-in.jpeg 22.52 KB

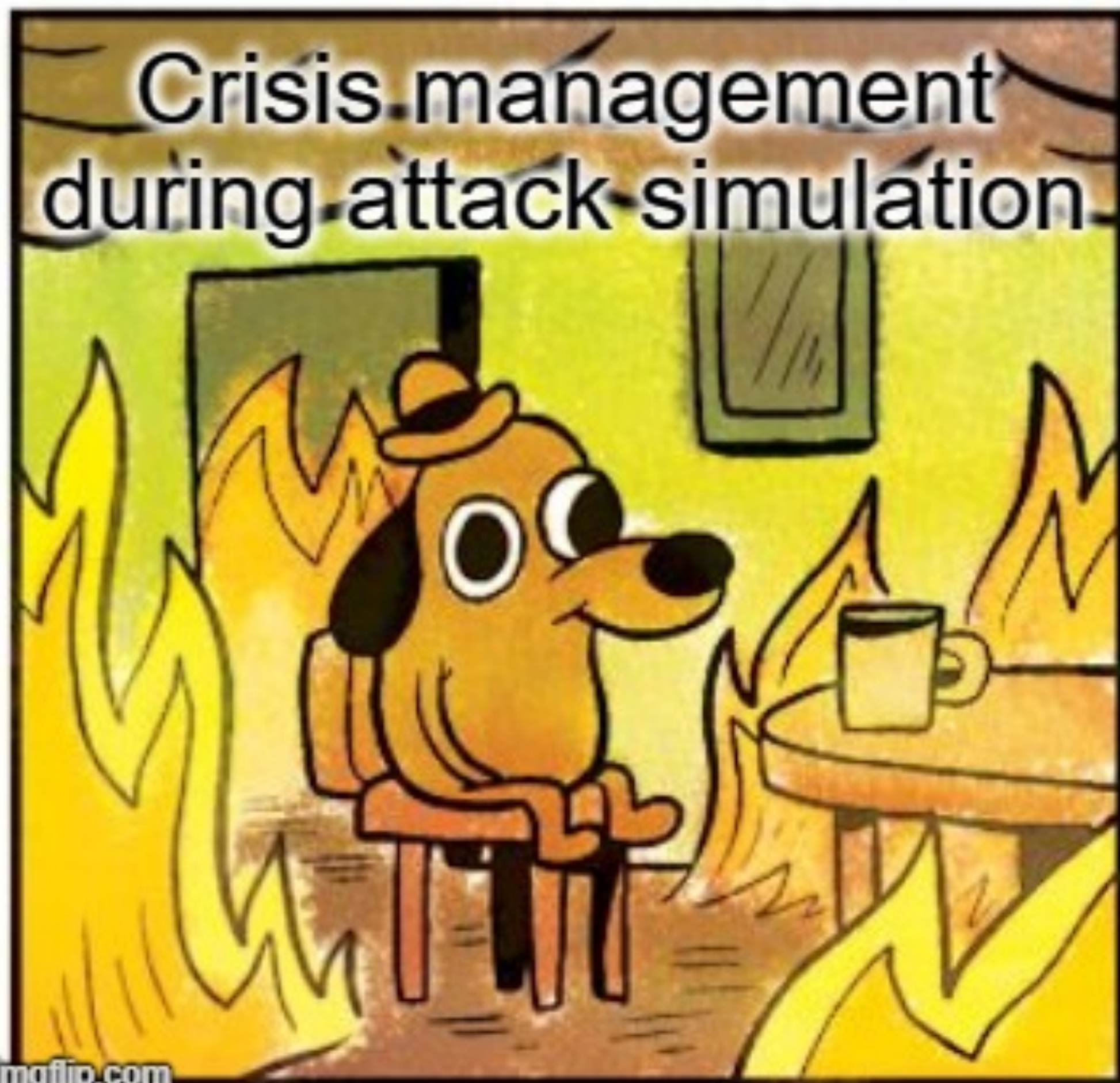


EXERCISE RESULTS

Post-mortem Analysis & Debriefing



Crisis management
during attack simulation



THIS IS FINE.



Post-mortem Analysis

- 01** | Logs from EDR, EPP, DNS, Proxy, AD, Windows-Eventlogs, IDS
Correlation with timing of Micro Attack Simulations
- 02** | Gap-Analysis to mark “failed” controls in the attack tree
Re-calculate the attack tree to reflect the holistic view
- 03** | Debriefing with the team(s)
Not a failure, but an opportunity to learn and improve



CONCLUSION

...



Comparison with Traditional Red Teaming

Both approaches have benefits and drawbacks, *but different ones...*

	Micro Attack Simulations	Traditional Red Teaming
<i>Scope</i>	Focused on specific controls or processes	Broad, covers multiple attack vectors
<i>Duration</i>	Shorter, often days to weeks	Longer, often weeks to months
<i>Cost</i>	Generally lower & less resources	Generally higher & more resources
<i>Complexity</i>	Lower complexity, less planning required	High complexity, extensive planning
<i>Skill Required</i>	May require specialized skills for specific controls	Requires diverse skill sets across multiple areas
<i>Objectives</i>	Validates specific security controls	Validates overall security posture
<i>Misses</i>	Interrelated operation of security controls	Potential weak points behind initial posture
<i>Impact on Ops</i>	Lower, less disruptive, less risk	Higher, more disruptive, more risk
<i>Realism</i>	May not fully simulate real-world attacks	Aims to closely simulate real-world attacks
<i>Output</i>	Detailed feedback on specific controls	General assessment of security readiness
<i>Reporting</i>	More straightforward, focused, enhanced with Tree	Comprehensive, in-depth
<i>Adaptability</i>	Easier to adapt (other actors or controls) and repeat	May require significant changes for each iteration

Offensive Security Landscape

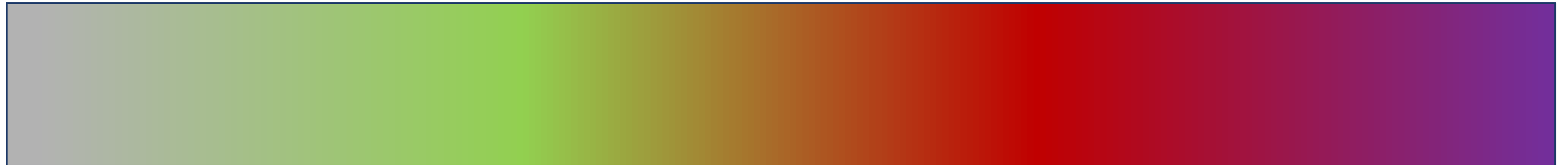
Where do Micro Attack Simulations fit in?

Vulnerability
Scans

VAPT

Red
Teaming

Purple
Teaming



Micro Attack Simulations

Simulate the Unsimulateable

Benefit of Micro Attack Simulations vs. Traditional Red Team Approach

ALERT

Malware Discovered in Popular NPM Package, ua-parser-js

Last Revised: October 22, 2021

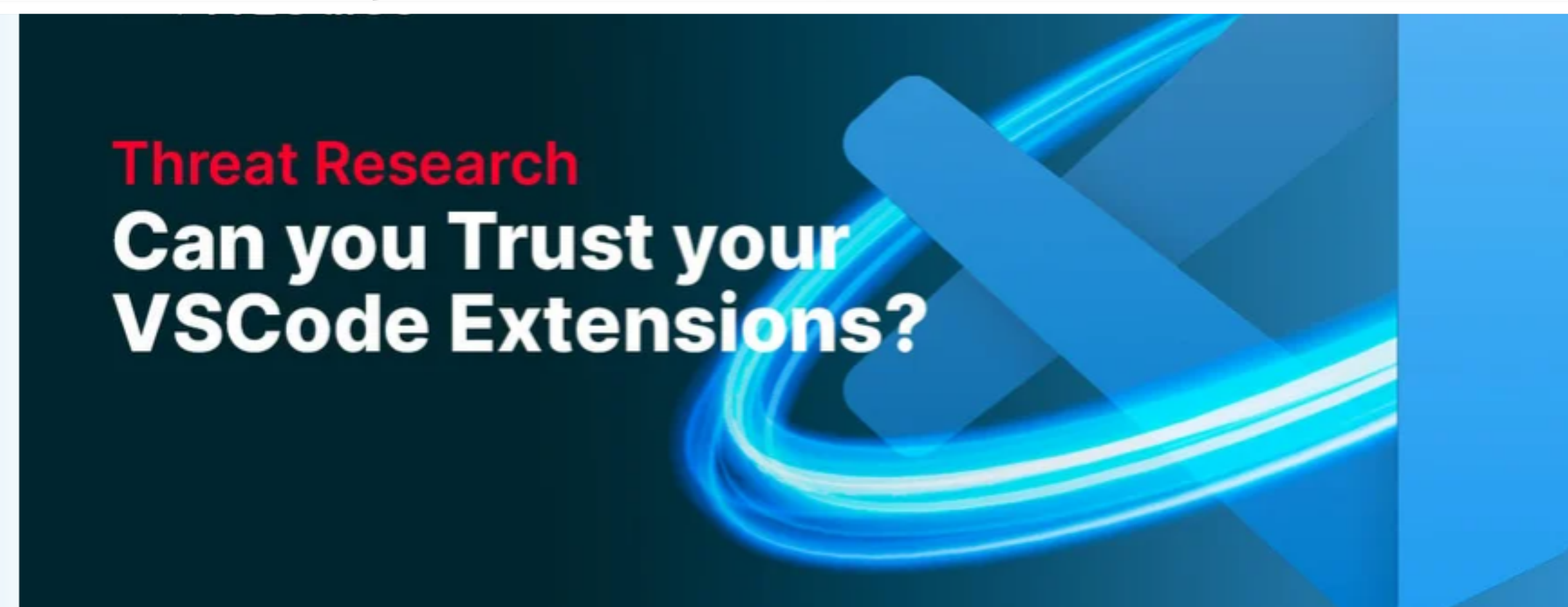


Versions of a popular NPM package named `ua-parser-js` was found to contain malicious code. `ua-parser-js` is used in apps and websites to discover the type of device or browser a person is using from User-Agent data. A computer or device with the affected software installed or running could allow a remote attacker to obtain sensitive information or take control of the system.

CISA urges users and administrators using compromised `ua-parser-js` versions 0.7.29, 0.8.0, and 1.0.0 to update to the respective patched versions: 0.7.30, 0.8.1, 1.0.1

For more information, see [Embedded malware in ua-parser-js](#).

<https://www.cisa.gov/news-events/alerts/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js>



Ilay Goldman, Yakir Kadkoda

January 06, 2023

Can You Trust Your VSCode Extensions?

Aqua Nautilus researchers have recently discovered that attackers can easily impersonate popular Visual Studio Code extensions and trick unknowing developers into downloading them. In original vulnerability

<https://blog.aquasec.com/can-you-trust-your-vscode-extensions>

Why opt for Micro Attack Simulations?

Gains & Advantages

Rapid Validation

- › Quick turnaround time for security assessments
- › Immediate insights for improvements

Cost-Efficiency

- › Less resource-intensive than full-scale Red Teaming
- › Offers high ROI for small to medium-sized organizations

Tailored Approach

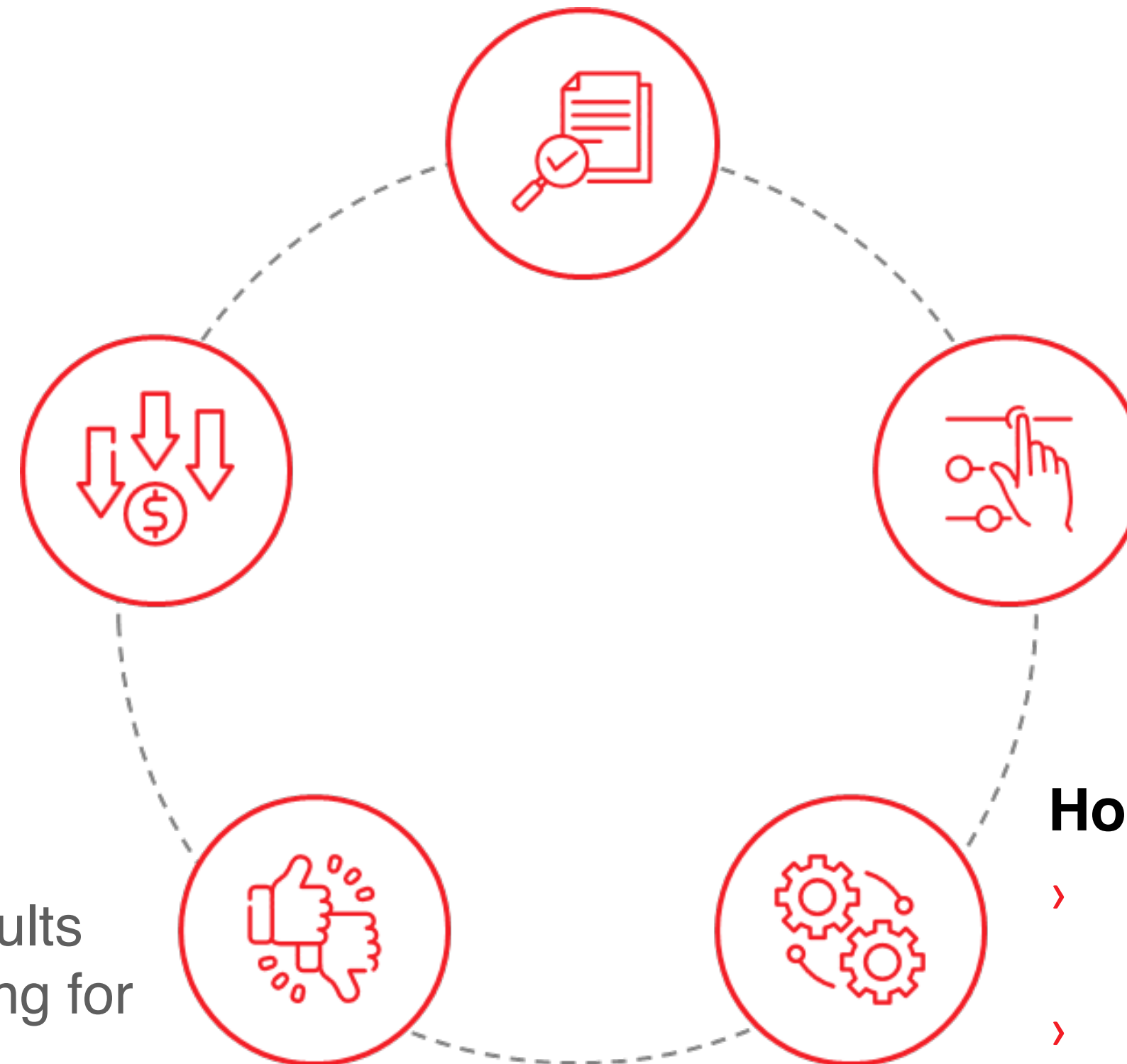
- › Customized to focus on specific controls
- › Flexibility in scaling up or down based on needs

Actionable Feedback

- › Generates specific, quantifiable results
- › Facilitates prioritized decision-making for resource allocation

Holistic View (Simulation + Tree)

- › Integrates both technical and non-technical controls
- › Recalculate attack tree with broken controls marked as “failed”



Q & A

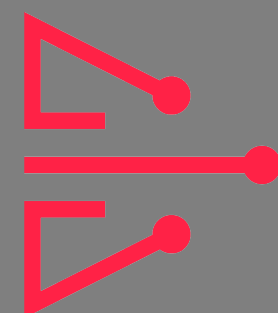


THANK YOU



Christian Schneider (@cschneider4711) — Christian-Schneider.net

Kevin Ott (@kevin0x90) — ExploitLabs.de



**EXPLOIT
LABS**

Free tool used for model creation: AttackTree.online