FROM CHECKBOX TO CHECKMATE

WINNING THE GAME FOR SECURITY BUDGETS

WITH SOME PURPLE TEAM STUFF AT THE BEGINNING

$

WHOAMI

I have worn a lot of hats:

- **PREVIOUSLY, BLUE TEAM**

  IT support

  Sysadmin

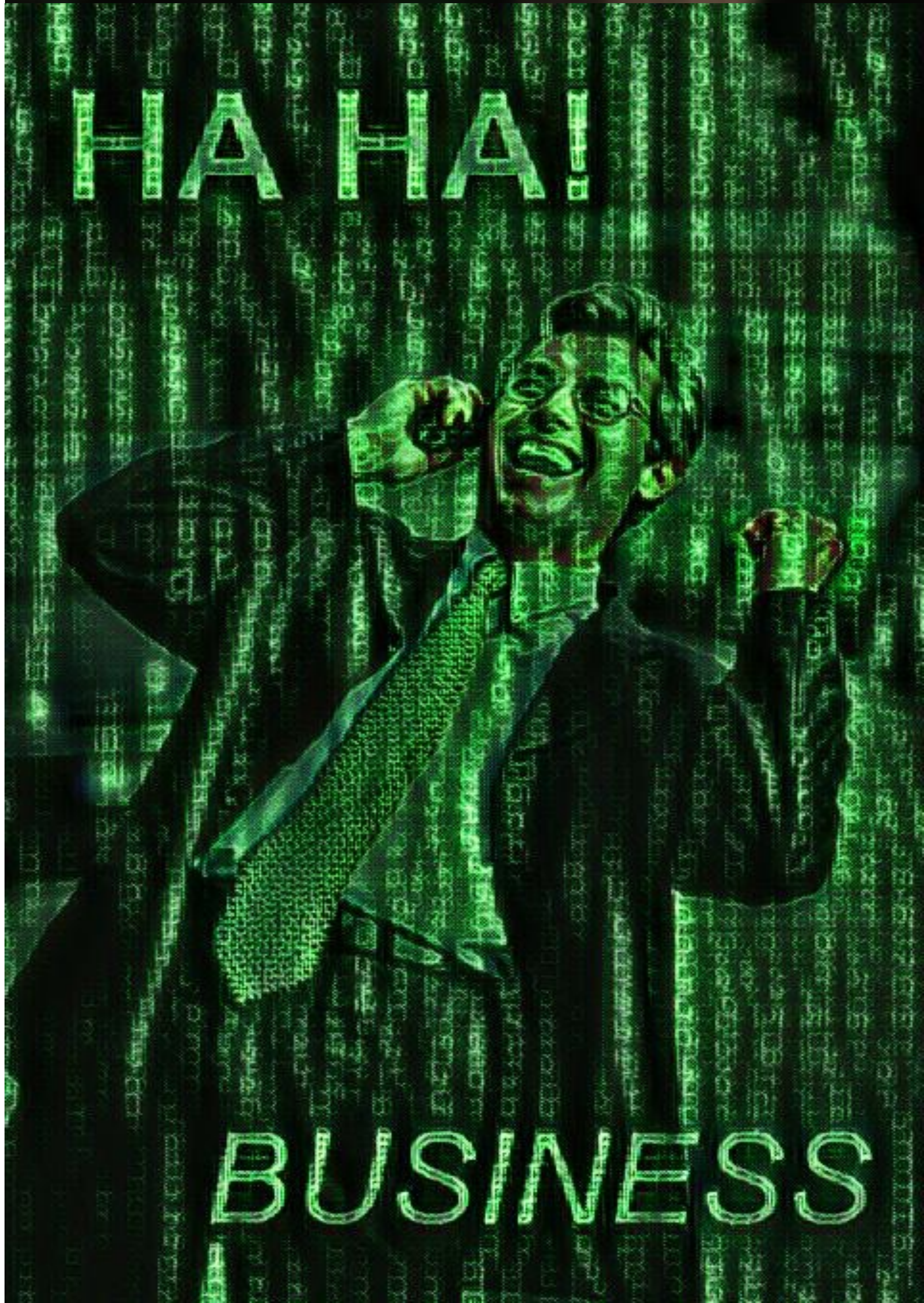
  vCISO

  Compliance

- **ALSO, PREVIOUSLY LED A PENETRATION TESTING PRACTICE**

- **NOW: CONSULTANT AT BISHOP FOX, RED TEAM**

  You can call me Ryan. Let’s talk about a pet peeve of mine *real quick.*



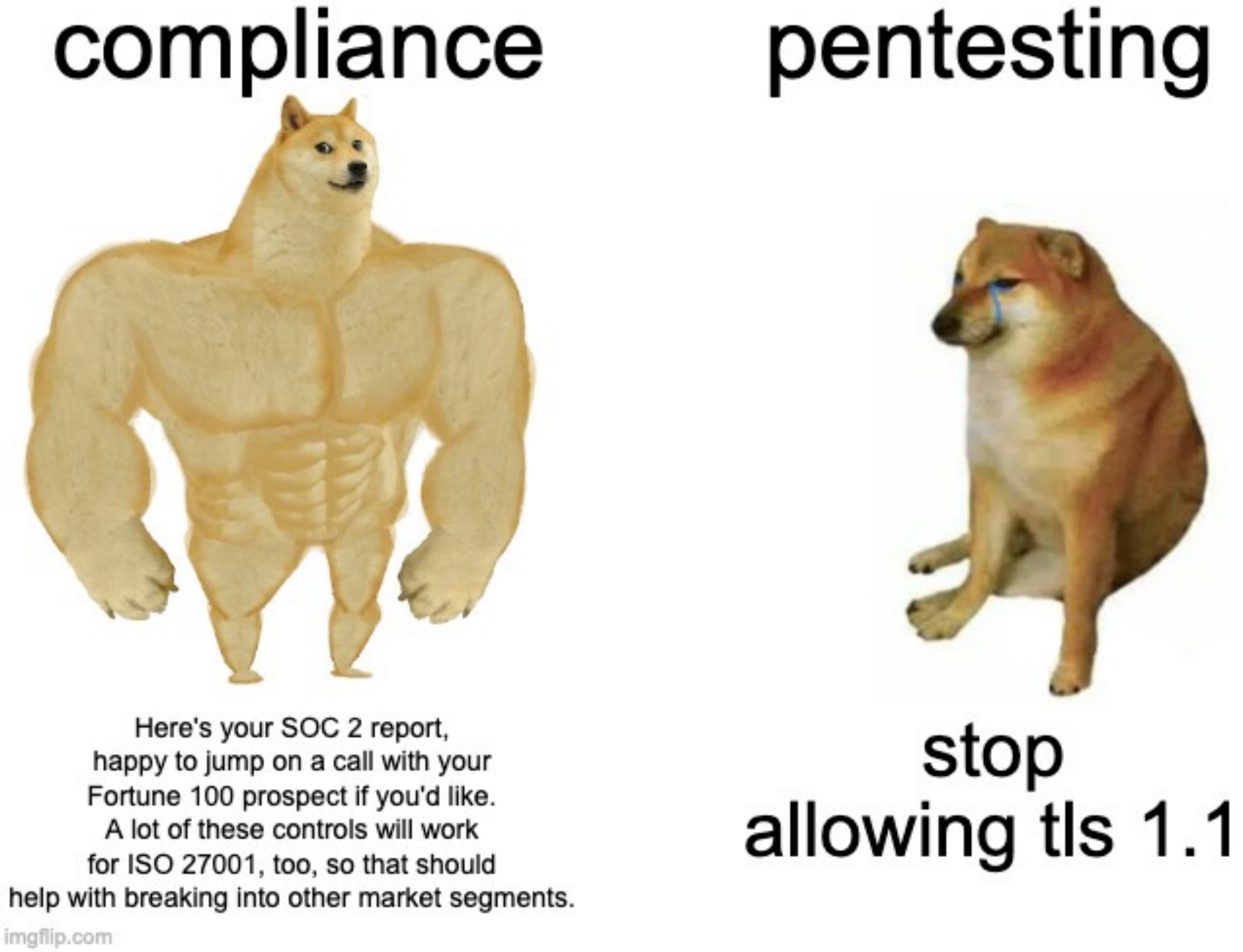
“Hackers like nothing more than to **shit on compliance**.”

- me

LOOK,

I GET IT OKAY?

Compliance gets all the attention


compliance
pentesting
Here's your SOC 2 report,
happy to jump on a call with your
Fortune 100 prospect if you'd like.
A lot of these controls will work
for ISO 27001, too, so that should
help with breaking into other market segments.
stop
allowing tls 1.1
imgflip.com

DOWNSIDES OF

PENTESTING AND RED TEAMING

Pentests are often limited in scope

- Won’t be comprehensive
- Findings can make you look bad
- People get fired
  - Usually the wrong move, but it unfortunately happens
- Reports are checklists of non-contextual findings for someone to fix

Red team exercises: advanced, but…

- Not about coverage
- Systemic issues that are much harder to fix

THE COMMON DENOMINATOR HERE IS A LACK OF CONTEXT

THIS WILL BE A LOT OF INFORMATION

IT SHOULD HAVE BEEN TWO TALKS

- What is a purple team?
- How do purple team exercises work?
- How can purple teaming help me beyond improving security?
  - Wait what

THESE ARE MY IDEAS FOR

A FULL SECOND TALK

- Business Strategy and Political Maneuvering for Painfully Technical People
- I Am Machiavelli and So Can You
- 💰💰💰💰 How to Win Money and Influence Money 💰💰💰💰
- "how to get the CEO to notice me reddit"
- Making Shareholders Smile: A STAR WARS Story

01

WHAT IS A PURPLE TEAM?

WHAT PEOPLE

THINK THEY ARE

- A dedicated team with an entirely different skillset compared to a red team or blue team OR people who are experts at both
  - Kind of, but not really
- A pentesting team that does a pentest while the blue team just sort of watches
  - Kinda weird
- A red team that does a red team while the blue team just sort of watches
  - Also weird
- Let’s make our own definition:

A JOINT, COLLABORATIVE EFFORT BETWEEN ATTACKERS AND DEFENDERS TO TEST DETECTION CAPABILITIES AND IMPROVE SECURITY

WHAT THEY

ACTUALLY ARE

- A joint, collaborative effort between attackers and defenders to test detection capabilities and improve security
  - Not just a pentest where the blue team rides shotgun
  - Not an exercise in “seeing what’s possible”
  - In consulting (like with Bishop Fox), the defenders are our customers, and the attackers are us, the red team
- Test if things are **detected**
- Test if what is detected **alerts someone**
- Test if that alert can be **actioned**

02

HOW DO EXERCISES WORK?

HERE’S HOW THEY

ACTUALLY WORK

» The blue team has a TTP they want to test

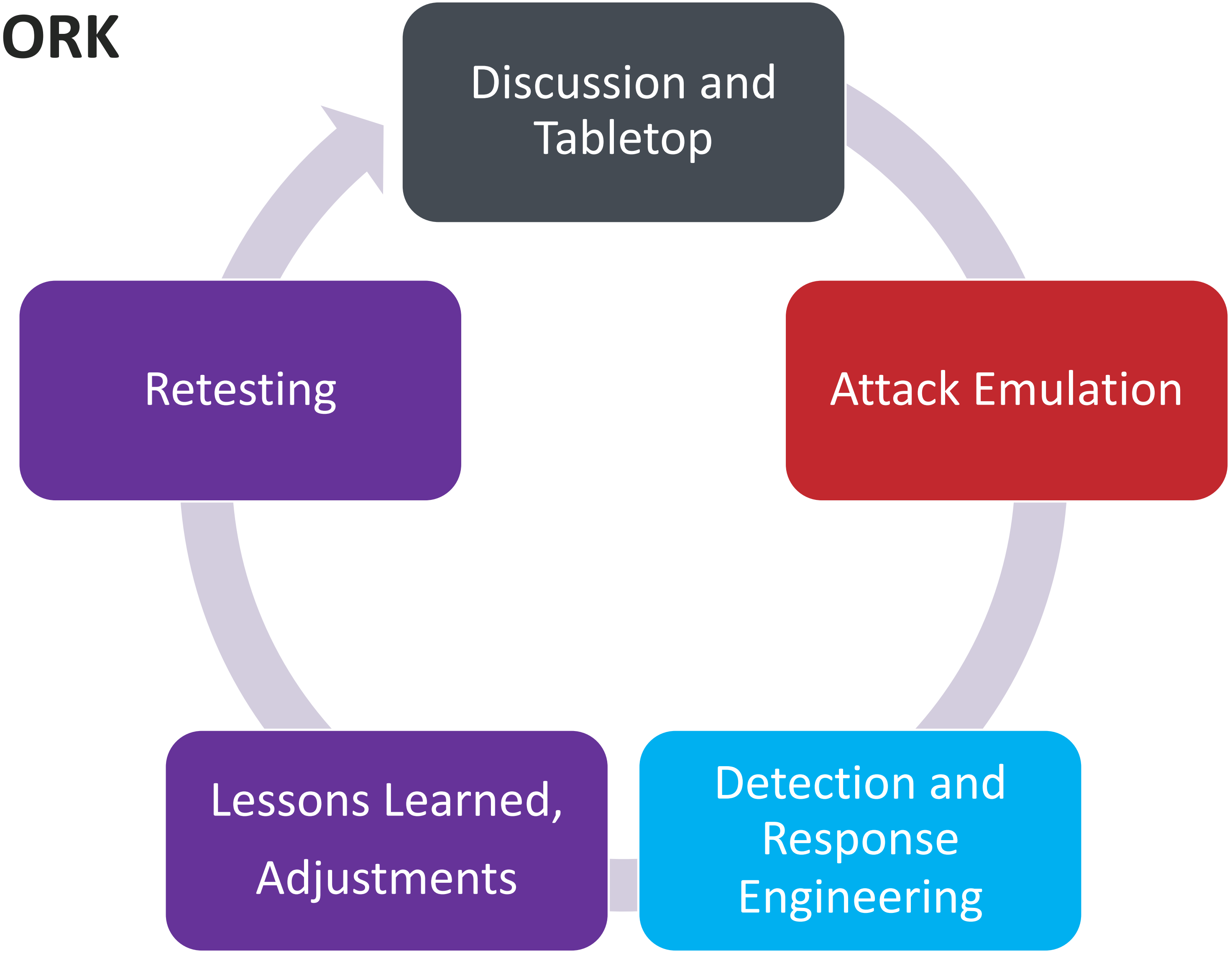
- Penetration test report results
- Scary news headline
- Intel from a threat report
- Anything counts!

» What is a TTP?

- “Tactic, Technique, or Procedure”
- Basically, any action an attacker takes

HERE’S HOW THEY

ACTUALLY WORK


Discussion and Tabletop
Attack Emulation
Detection and Response Engineering
Lessons Learned, Adjustments
Retesting

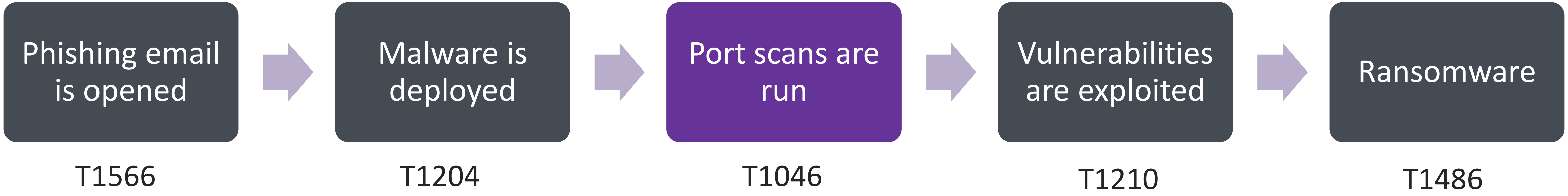
LET’S WORK THROUGH

AN EXAMPLE

- The red team runs a port scan of a network segment from a company Linux server that is "assumed to be compromised"
- The blue team realizes they can't detect port scans, and analyzes network traffic to identify patterns of activity that indicate a port scan is taking place
- The blue team configures their IDS/IPS to shut down hosts from which those patterns are originating
- The red team runs a port scan again and to see if they are blocked by the new defensive controls
- The initial test results, changes, and results of improvement are all recorded and documented

PUTTING IT ALL

IN CONTEXT



Phishing email is opened

T1566

Malware is deployed

T1204

Port scans are run

T1046

Vulnerabilities are exploited

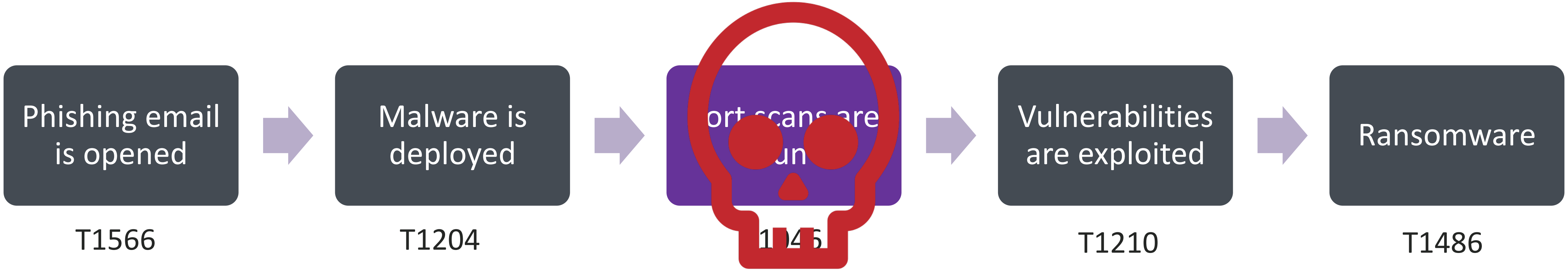
T1210

Ransomware

T1486

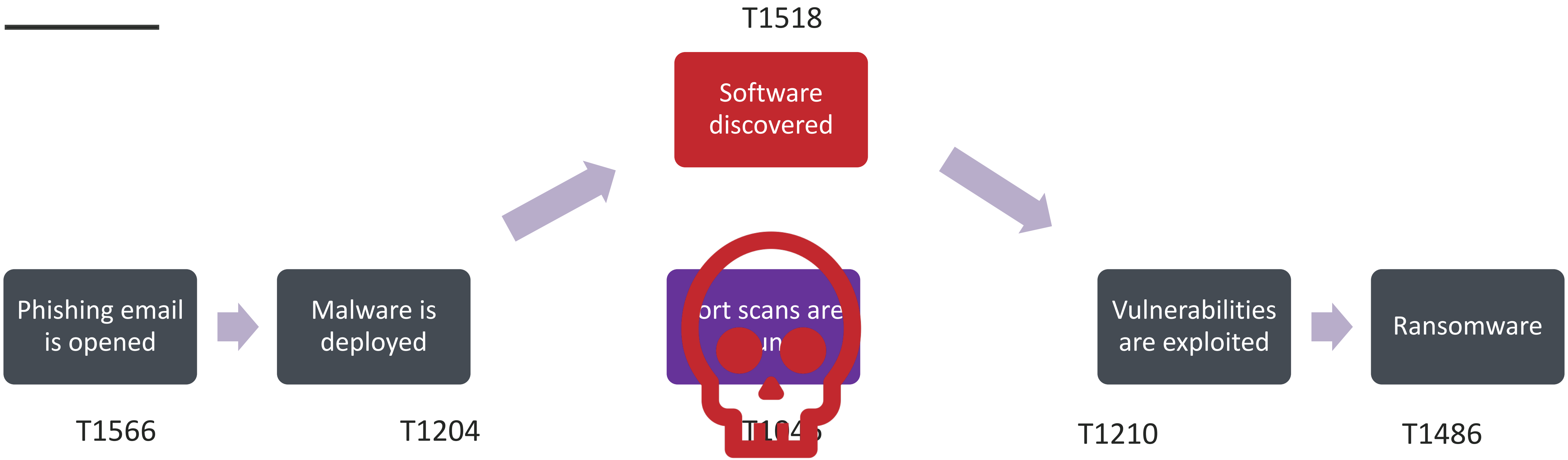
PUTTING IT ALL

IN CONTEXT



PUTTING IT ALL

IN CONTEXT



Phishing email is opened

T1566

Malware is deployed

T1204

T1518

Software discovered

Port scans are run

T1046

Vulnerabilities are exploited

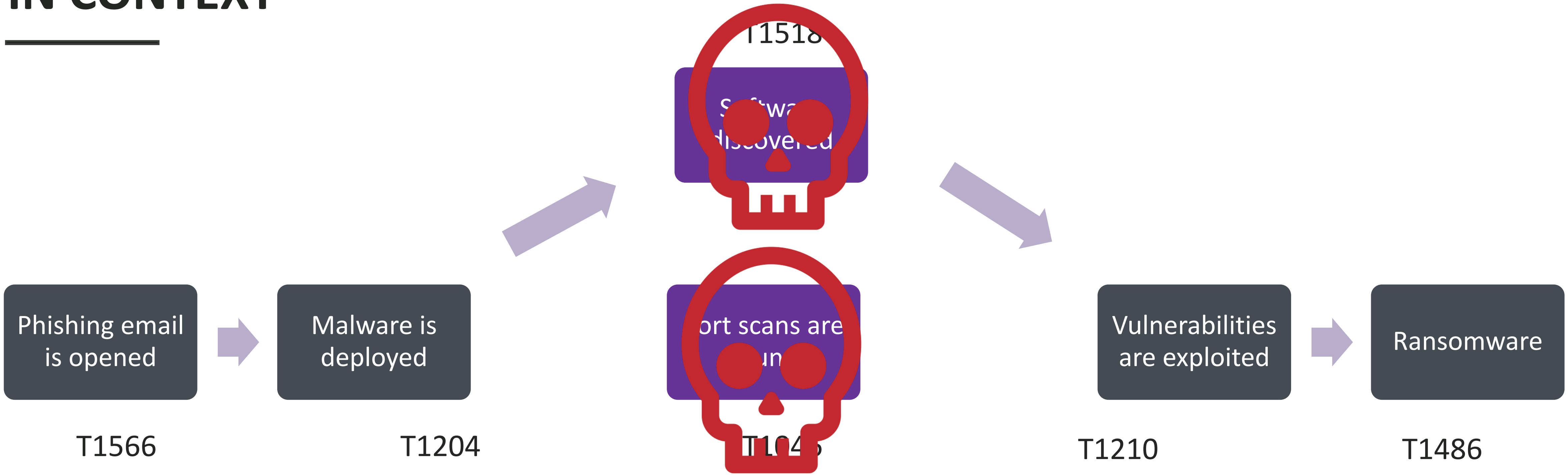
T1210

Ransomware

T1486

PUTTING IT ALL

IN CONTEXT



Phishing email is opened

T1566

Malware is deployed

T1204

T1518

Software discovered

Port scans are run

T1046

Vulnerabilities are exploited

T1210

Ransomware

T1486

WHAT IS IN

THE REPORT

WHAT WAS DONE

- Commands executed, payloads run, etc.

WHAT THE INITIAL RESULT WAS

- Did the blue team detect it? Can they do anything about it?

WHAT NEEDS TO CHANGE

- What improvements were made? Was a detection written? Alerts turned on?

WHAT THE RETEST RESULT WAS

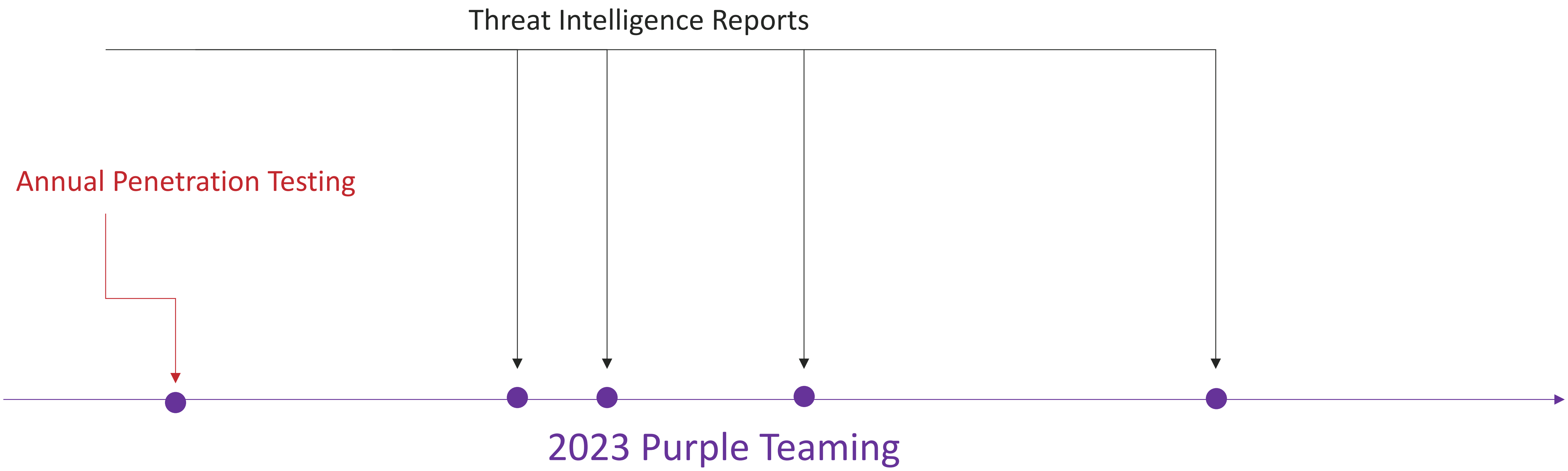
- Did the changes matter?

NEXT ACTIONS

- Can we improve the changes? Can we implement the same or similar improvements in more areas?

PURPLE TEAM

ALL DAY EVERY DAY



03

GOING BEYOND SECURITY

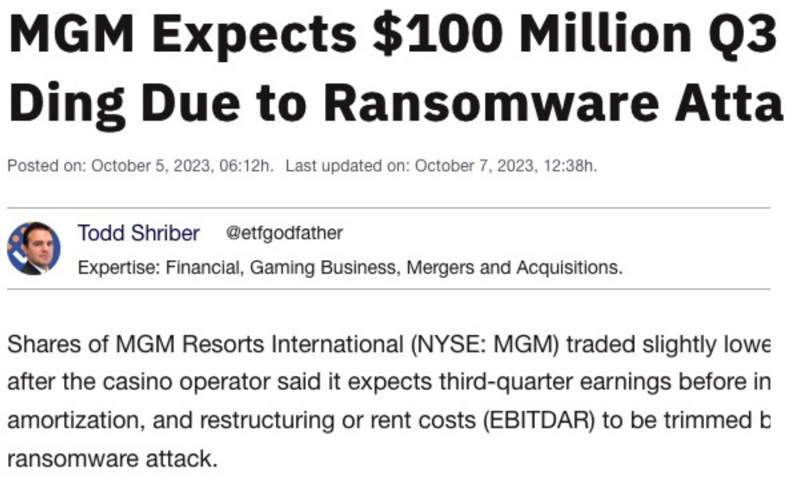
a.k.a getting that *bag*

NAMES AREN’T IMPORTANT BUT

IMAGINE THAT YOU ARE A REALLY BIG CASINO/HOTEL

SCRATCH THAT

IMAGINE THAT YOUR BOSS OWNS A LOT OF CASINOS AND HOTELS

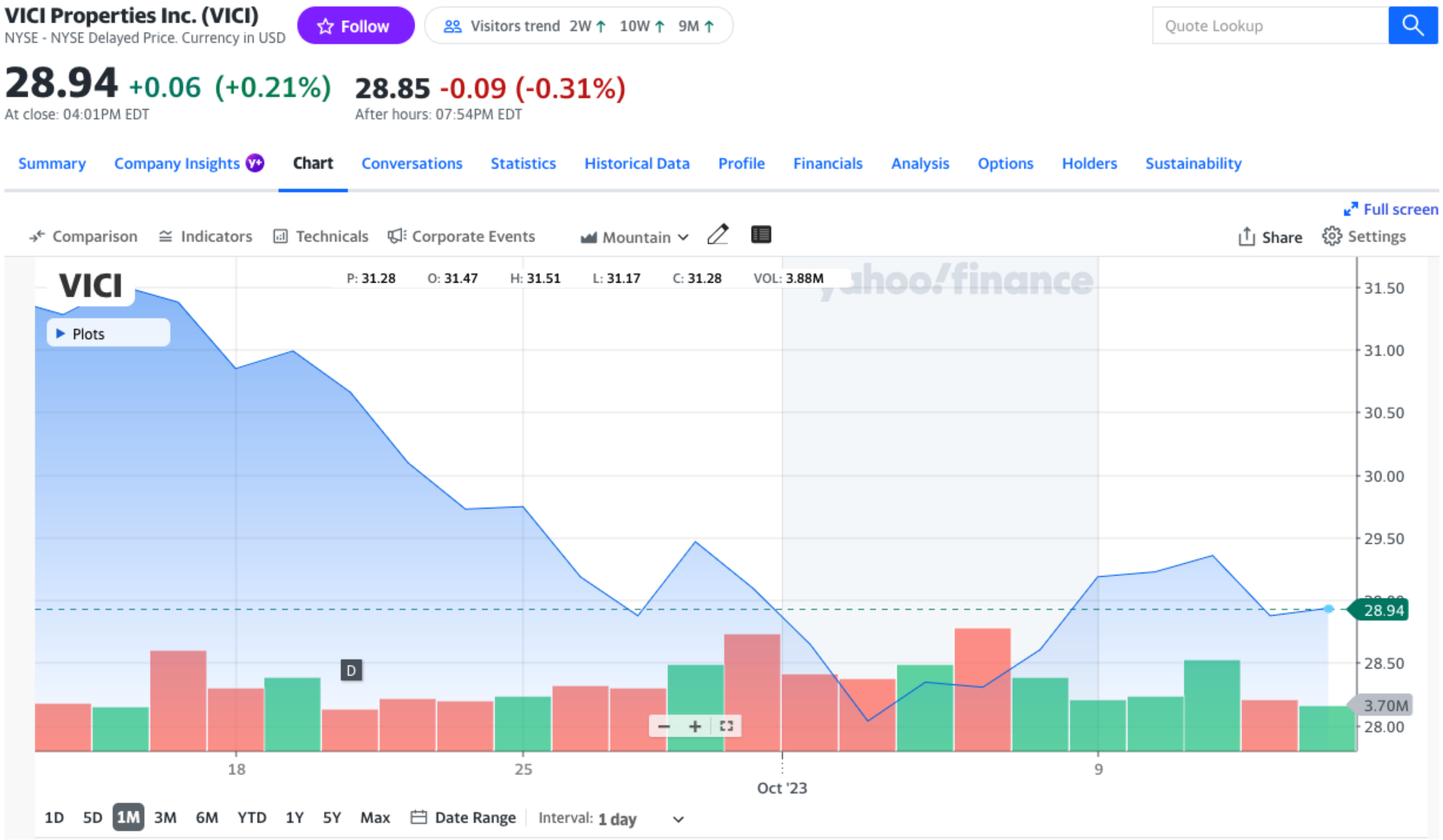


MGM Expects $100 Million Q3 Earnings Ding Due to Ransomware Attack

Posted on: October 5, 2023, 06:12h. Last updated on: October 7, 2023, 12:38h.

Todd Shriber @etfgodfather
Expertise: Financial, Gaming Business, Mergers and Acquisitions.

Shares of MGM Resorts International (NYSE: MGM) traded slightly lowe after the casino operator said it expects third-quarter earnings before in amortization, and restructuring or rent costs (EBITDAR) to be trimmed b ransomware attack.



VICI Properties Inc. (VICI)
NYSE - NYSE Delayed Price. Currency in USD

28.94 +0.06 (+0.21%)
At close: 04:01PM EDT

28.85 -0.09 (-0.31%)
After hours: 07:54PM EDT

P: 31.28 O: 31.47 H: 31.51 L: 31.17 C: 31.28 VOL: 3.88M

THE BOSS IS

VERY CONCERNED

☑ You already tested a bunch of ransomware TTPs

- Ransomware group tactics are not complicated and are well documented (see Conti playbook)

☑ You restricted password reset capability to specific individuals

- They must be escalated beyond the first tier of support

☑ You require verification steps to be completed that are difficult to bypass

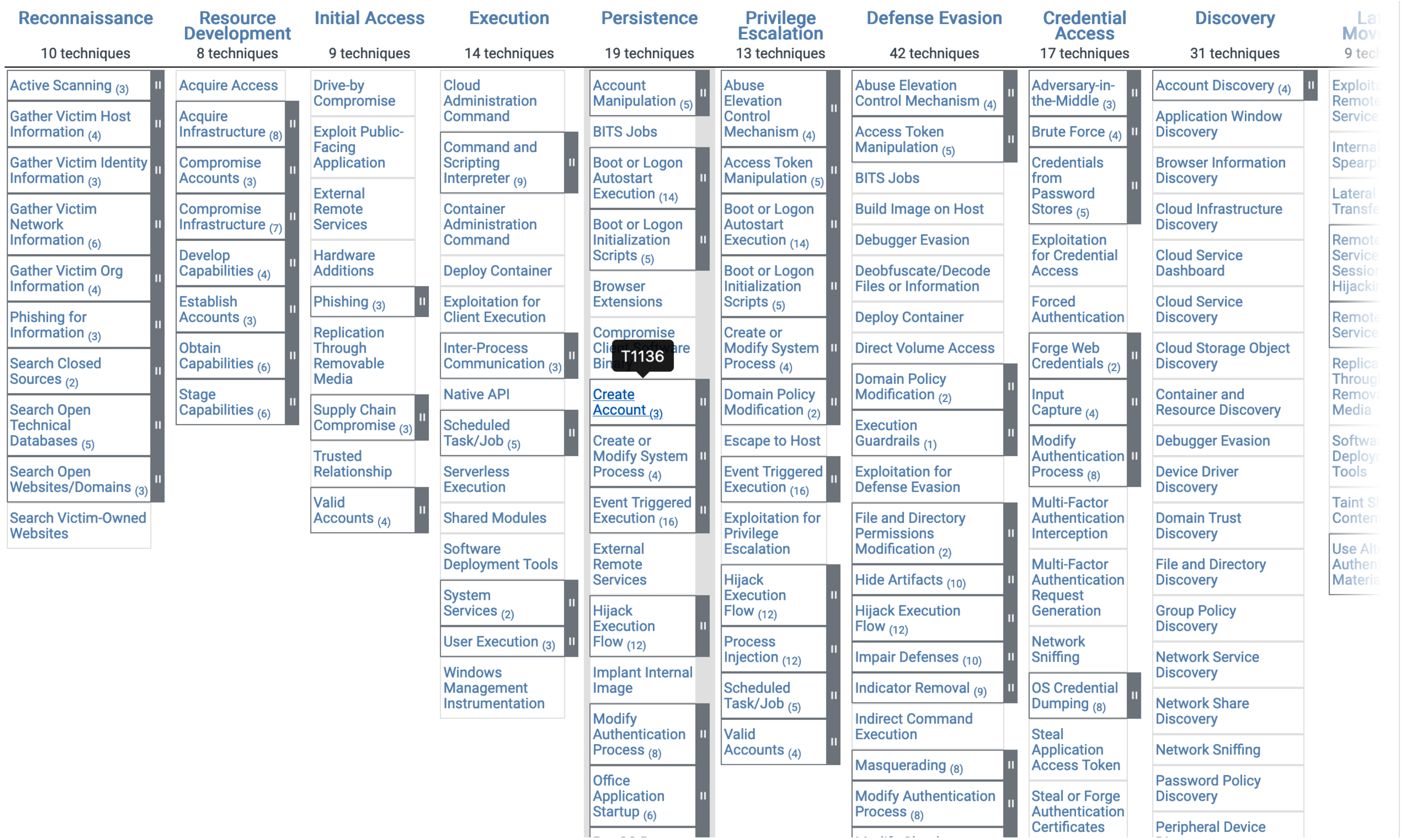
- Call the individual at their contact number, require an MFA token entry

NICE

HERE ARE SOME

EXAMPLE METRICS

- Percentage of MITRE ATT&CK TTPs detected/blocked



Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Cli are Bin
- T1136
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (8)
- Office Application Startup (6)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (10)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (8)
- Modify Authentication Process (8)

Credential Access
17 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates

Discovery
31 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device

La Mov
9 tec

- Exploit Remote Service
- Interna Spearp
- Lateral Transfe
- Remote Service Session Hijackin
- Remote Service
- Replica Throug Remova Media
- Softwa Deploy Tools
- Taint S Conten
- Use Alt Authen Materia

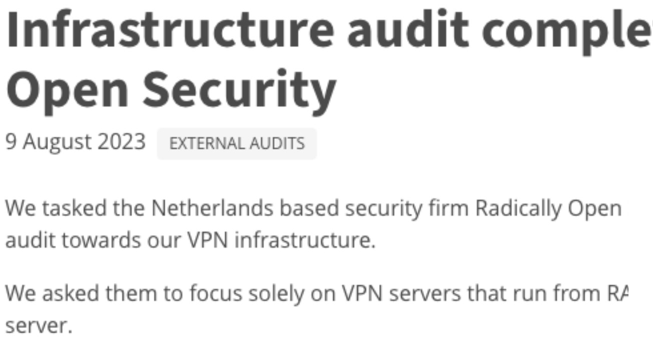
HERE ARE SOME

EXAMPLE METRICS

- Percentage of MITRE ATT&CK TTPs detected/blocked
- Average intruder detection rates over time
- Efficacy of detecting data exfiltration
- Number of data encryption methods used by ransomware groups tested and stopped

THE PART WHERE I GET

DAY DREAMY AND IDEALISTIC

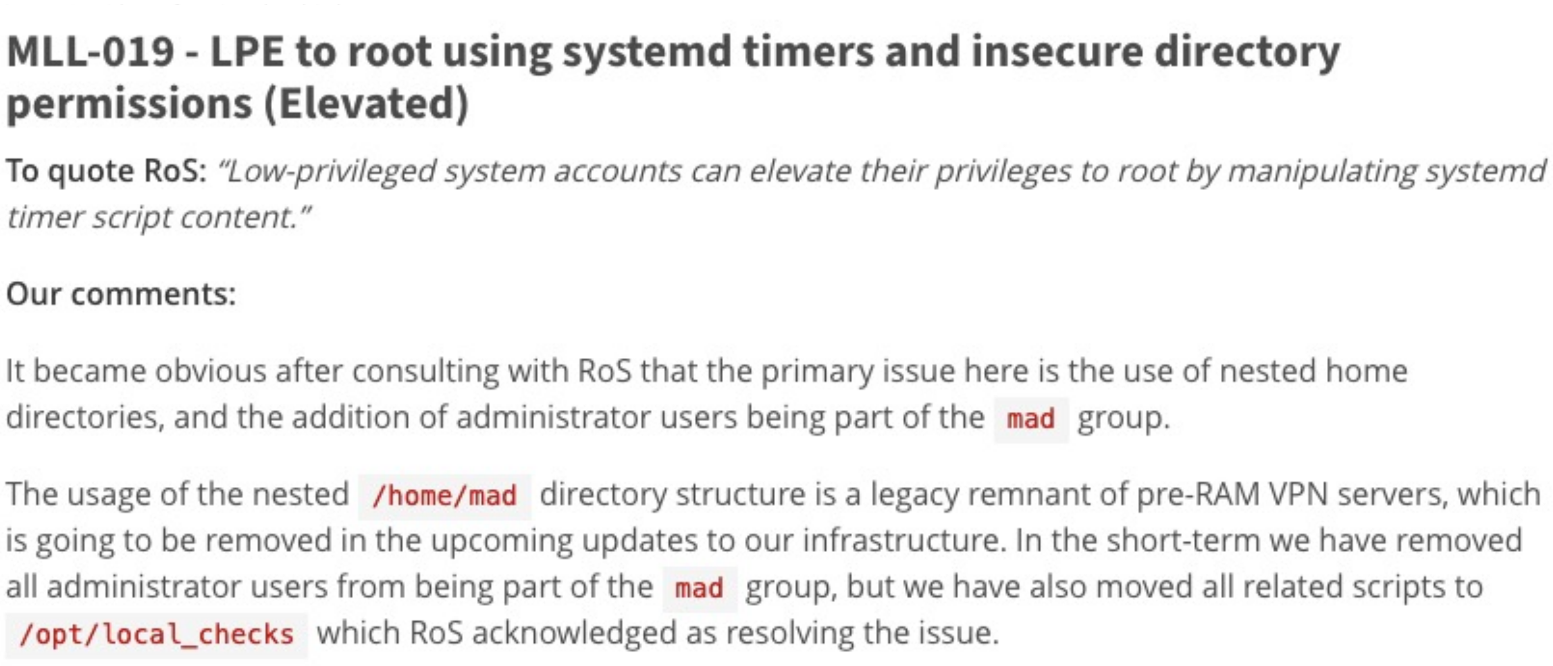


Infrastructure audit completed by Radically Open Security

9 August 2023 EXTERNAL AUDITS

We tasked the Netherlands based security firm Radically Open
audit towards our VPN infrastructure.

We asked them to focus solely on VPN servers that run from RA
server.



MLL-019 - LPE to root using systemd timers and insecure directory permissions (Elevated)

To quote RoS: *"Low-privileged system accounts can elevate their privileges to root by manipulating systemd timer script content."*

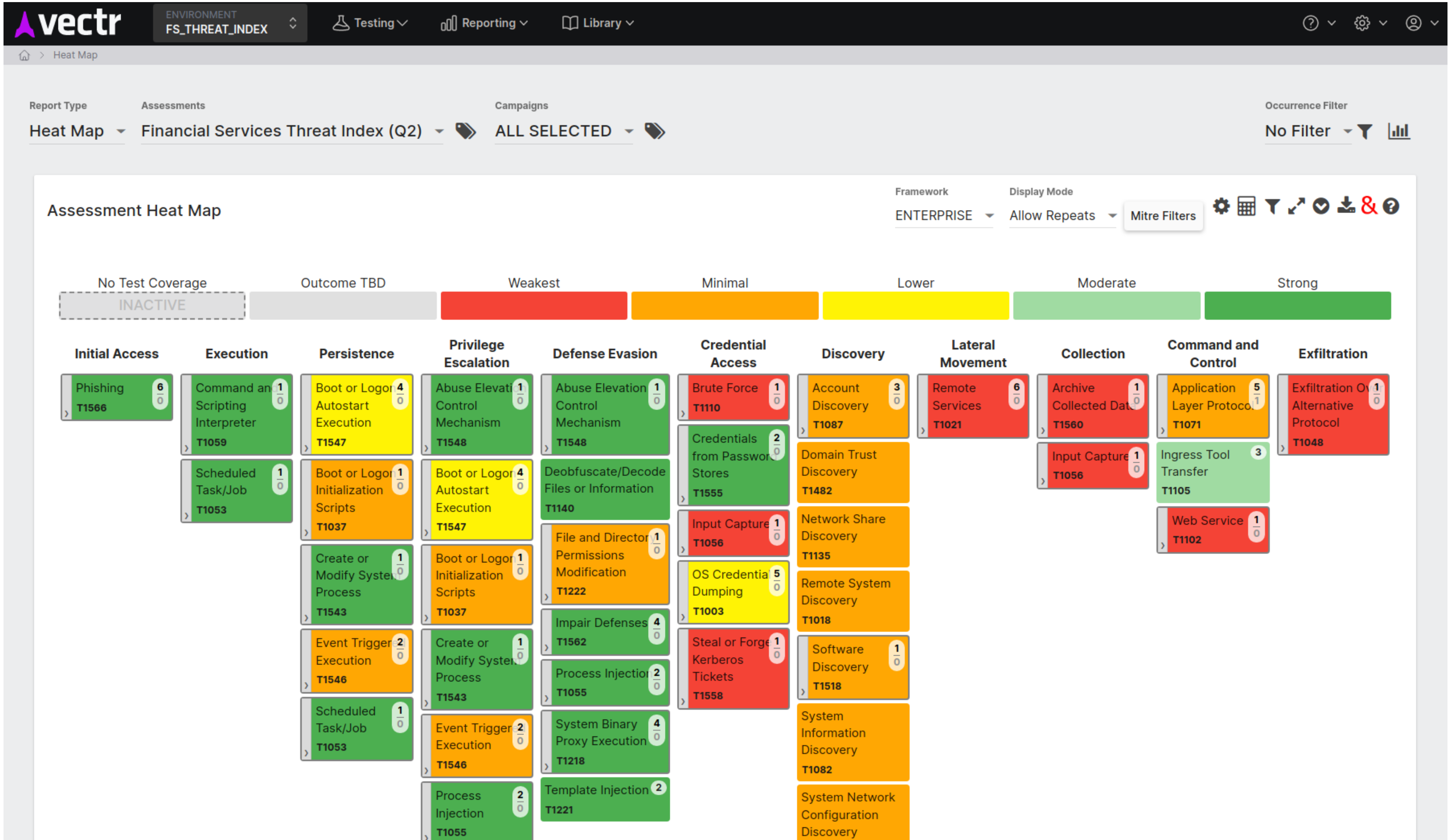
Our comments:

It became obvious after consulting with RoS that the primary issue here is the use of nested home directories, and the addition of administrator users being part of the `mad` group.

The usage of the nested `/home/mad` directory structure is a legacy remnant of pre-RAM VPN servers, which is going to be removed in the upcoming updates to our infrastructure. In the short-term we have removed all administrator users from being part of the `mad` group, but we have also moved all related scripts to `/opt/local_checks` which RoS acknowledged as resolving the issue.

HERE'S SOME

FREE STUFF



ENVIRONMENT FS_THREAT_INDEX

Report Type: Heat Map

Assessments: Financial Services Threat Index (Q2)

Campaigns: ALL SELECTED

Occurrence Filter: No Filter

Assessment Heat Map

Framework: ENTERPRISE

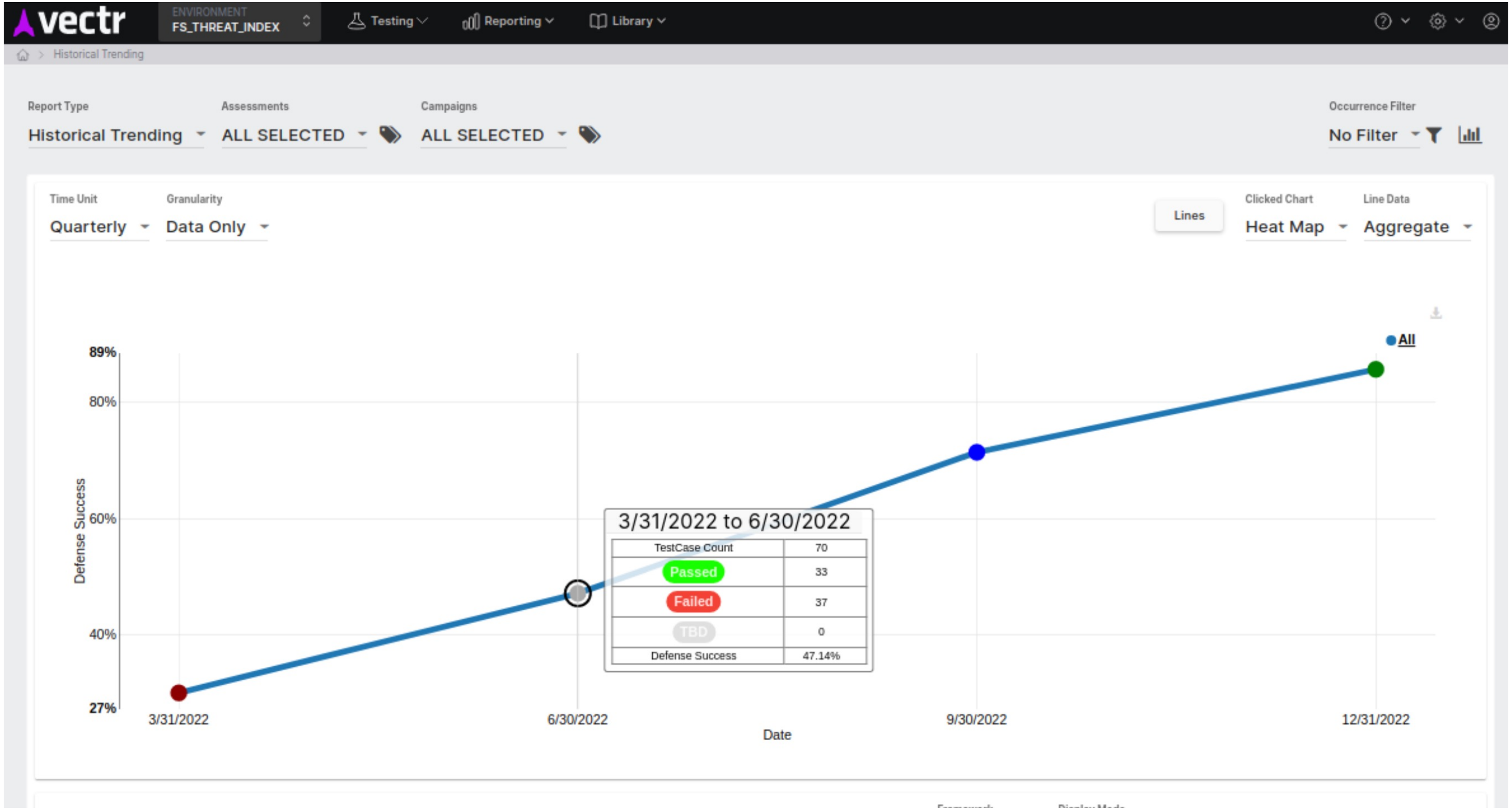
Display Mode: Allow Repeats

No Test Coverage	Outcome TBD	Weakest	Minimal	Lower	Moderate	Strong
INACTIVE						

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Phishing T1566 6 0	Command and Scripting Interpreter T1059 1 0	Boot or Logon Autostart Execution T1547 4 0	Abuse Elevation Control Mechanism T1548 1 0	Abuse Elevation Control Mechanism T1548 1 0	Brute Force T1110 1 0	Account Discovery T1087 3 0	Remote Services T1021 6 0	Archive Collected Data T1560 1 0	Application Layer Protocol T1071 5 1	Exfiltration Over Alternative Protocol T1048 1 0
	Scheduled Task/Job T1053 1 0	Boot or Logon Initialization Scripts T1037 1 0	Boot or Logon Autostart Execution T1547 4 0	Deobfuscate/Decode Files or Information T1140	Credentials from Password Stores T1555 2 0	Domain Trust Discovery T1482		Input Capture T1056 1 0	Ingress Tool Transfer T1105 3	
		Create or Modify System Process T1543 1 0	Boot or Logon Initialization Scripts T1037 1 0	File and Directory Permissions Modification T1222 1 0	Input Capture T1056 1 0	Network Share Discovery T1135			Web Service T1102 1 0	
		Event Triggered Execution T1546 2 0	Create or Modify System Process T1543 1 0	Impair Defenses T1562 4 0	OS Credential Dumping T1003 5 0	Remote System Discovery T1018				
		Scheduled Task/Job T1053 1 0	Event Triggered Execution T1546 2 0	Process Injection T1055 2 0	Steal or Forge Kerberos Tickets T1558 1 0	Software Discovery T1518 1 0				
			Process Injection T1055 2 0	System Binary Proxy Execution T1218 4 0		System Information Discovery T1082				
				Template Injection T1221 2		System Network Configuration Discovery				

HERE'S SOME

FREE STUFF



ENVIRONMENT FS_THREAT_INDEX

Report Type: Historical Trending

Assessments: ALL SELECTED

Campaigns: ALL SELECTED

Occurrence Filter: No Filter

Time Unit: Quarterly

Granularity: Data Only

Clicked Chart: Heat Map

Line Data: Aggregate

3/31/2022 to 6/30/2022

TestCase Count	70
Passed	33
Failed	37
TBD	0
Defense Success	47.14%

HERE’S SOME

FREE STUFF

https://attack.mitre.org/matrices/enterprise/

https://atomicredteam.io/

https://docs.vectr.io/