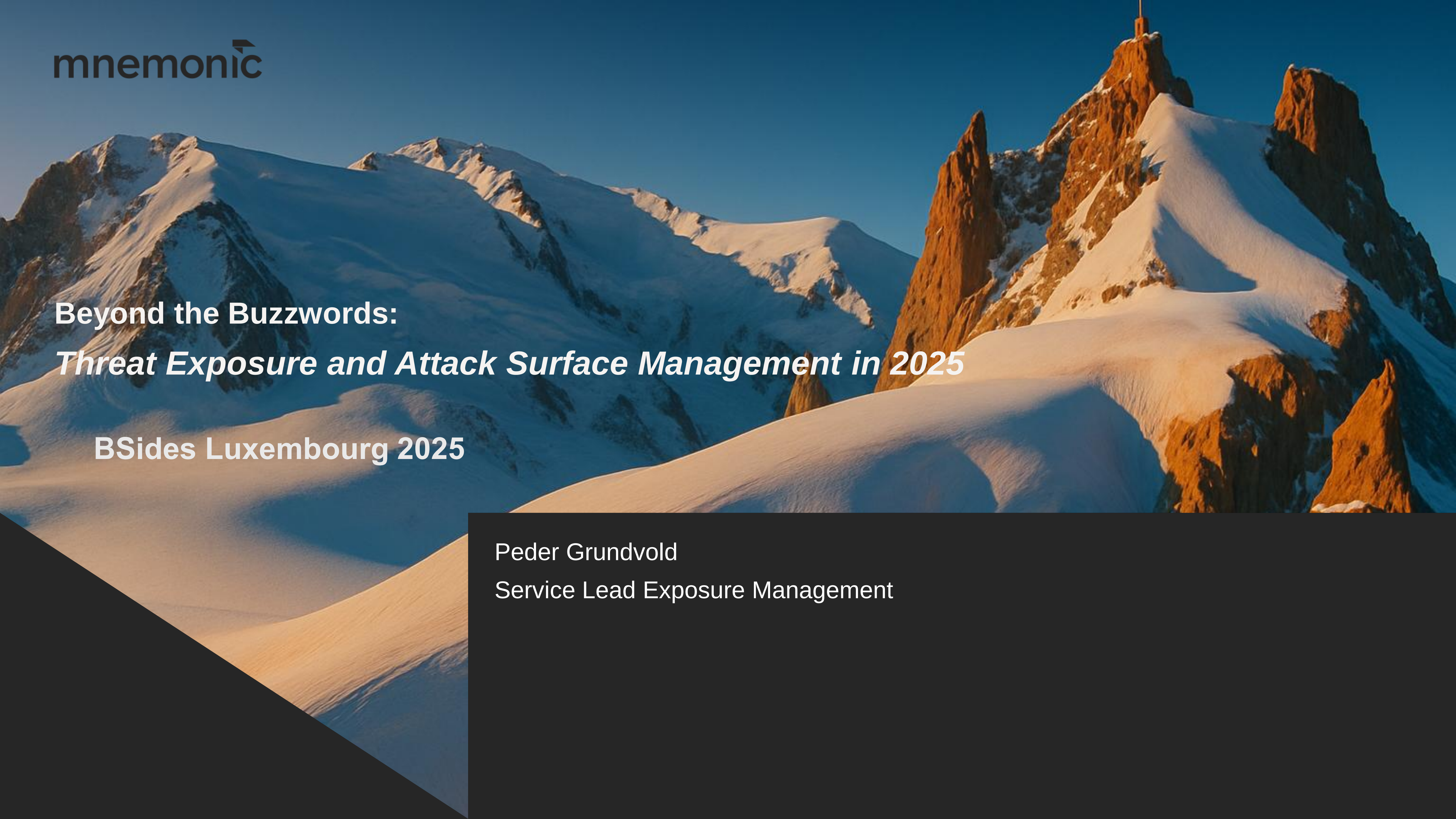
mnemonic



Beyond the Buzzwords:

Threat Exposure and Attack Surface Management in 2025

BSides Luxembourg 2025

Peder Grundvold

Service Lead Exposure Management

whoami

- From Oslo, Norway ❄ 🐻
- M.Sc. (Information Security) from NTNU and UCSB
- Working with offensive security, pentesting and "VMaaS"
- Last two years leading the area of exposure mgmt. in my current company
- Fun fact: all "mountain pictures" here are from Chamonix, France – where I have also lived ⛷

mnemonic

Peder Grundvold
Service Lead Exposure Management | TRS
+47 907 34 010
peder@mnemonic.no

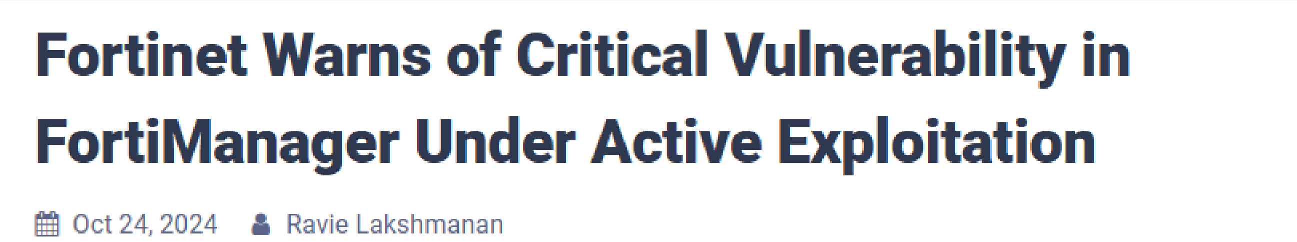
mnemonic AS | Henrik Ibsens Gate 100, 0255 Oslo

Agenda

- Threat landscape in 2025
- Evolution in the last 20 years
- Current phase: CTEM
- “Validation”
- CTEM in practice
- Key takeaways

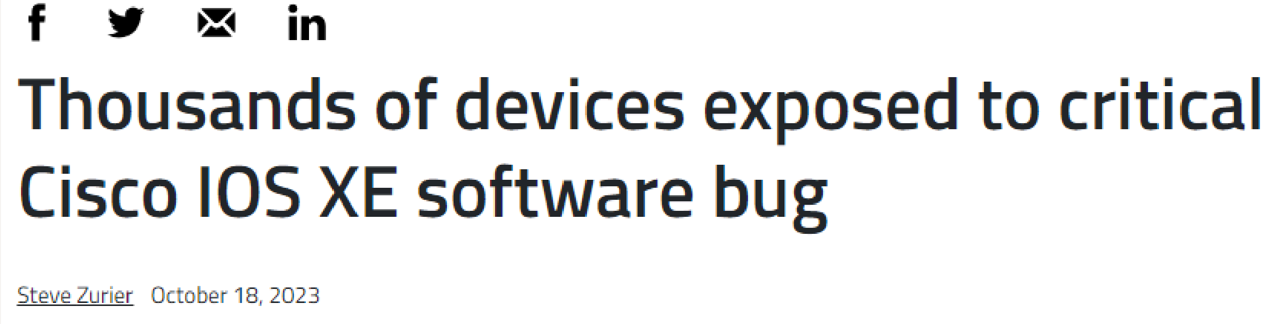
mnemonic

Threat Landscape



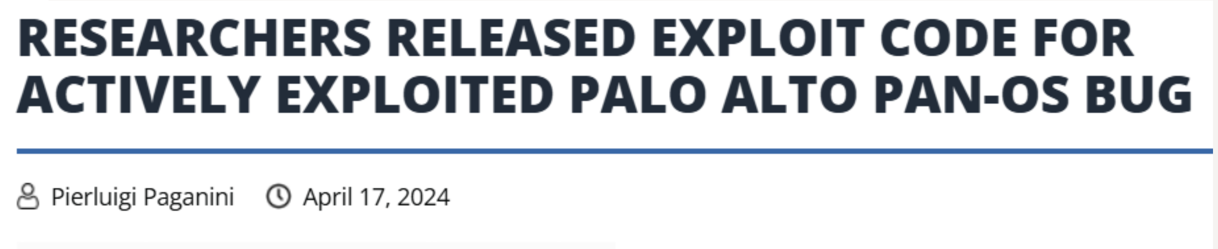
Fortinet Warns of Critical Vulnerability in FortiManager Under Active Exploitation

Oct 24, 2024 Ravie Lakshmanan



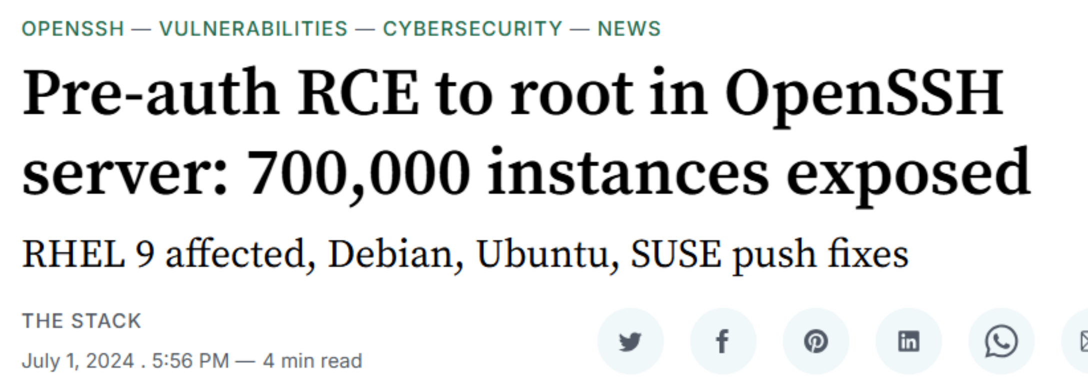
Thousands of devices exposed to critical Cisco IOS XE software bug

Steve Zurier October 18, 2023



RESEARCHERS RELEASED EXPLOIT CODE FOR ACTIVELY EXPLOITED PALO ALTO PAN-OS BUG

Pierluigi Paganini April 17, 2024



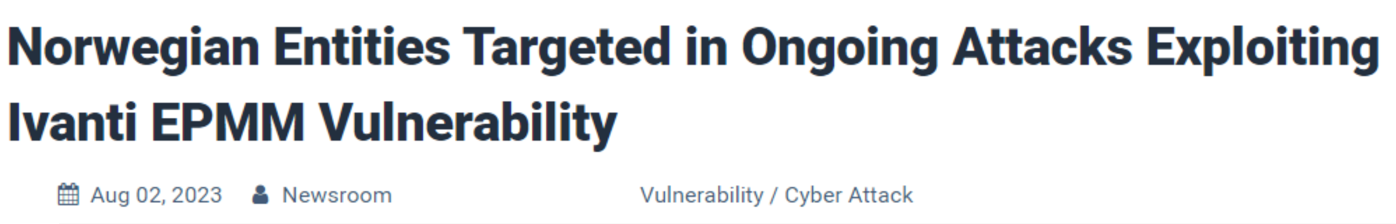
OPENSSH — VULNERABILITIES — CYBERSECURITY — NEWS

Pre-auth RCE to root in OpenSSH server: 700,000 instances exposed

RHEL 9 affected, Debian, Ubuntu, SUSE push fixes

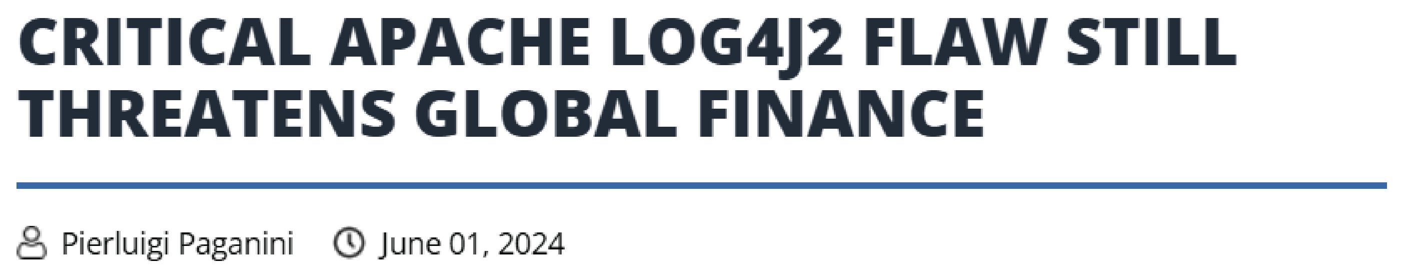
THE STACK

July 1, 2024 . 5:56 PM — 4 min read



Norwegian Entities Targeted in Ongoing Attacks Exploiting Ivanti EPMM Vulnerability

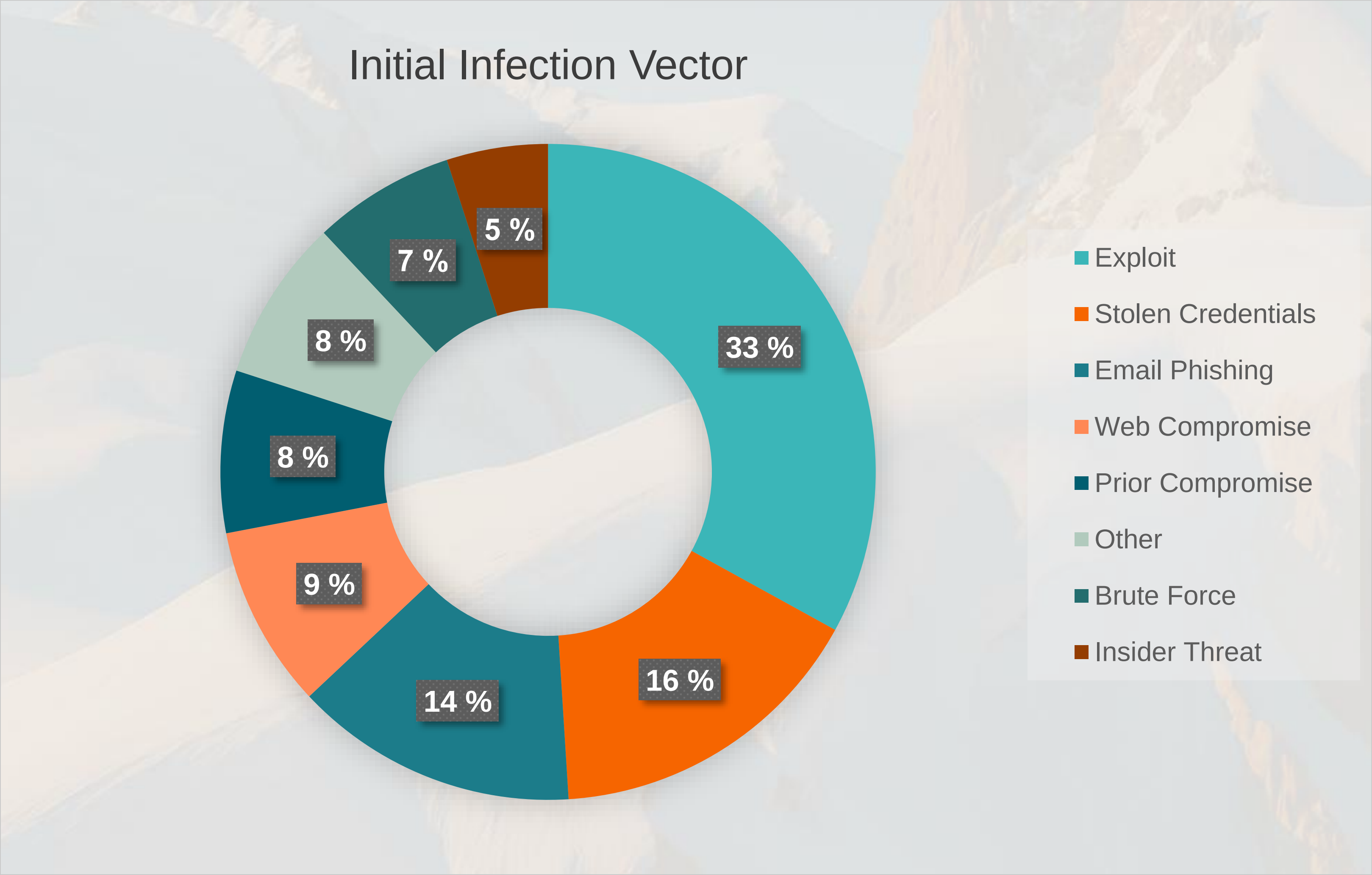
Aug 02, 2023 Newsroom Vulnerability / Cyber Attack



CRITICAL APACHE LOG4J2 FLAW STILL THREATENS GLOBAL FINANCE

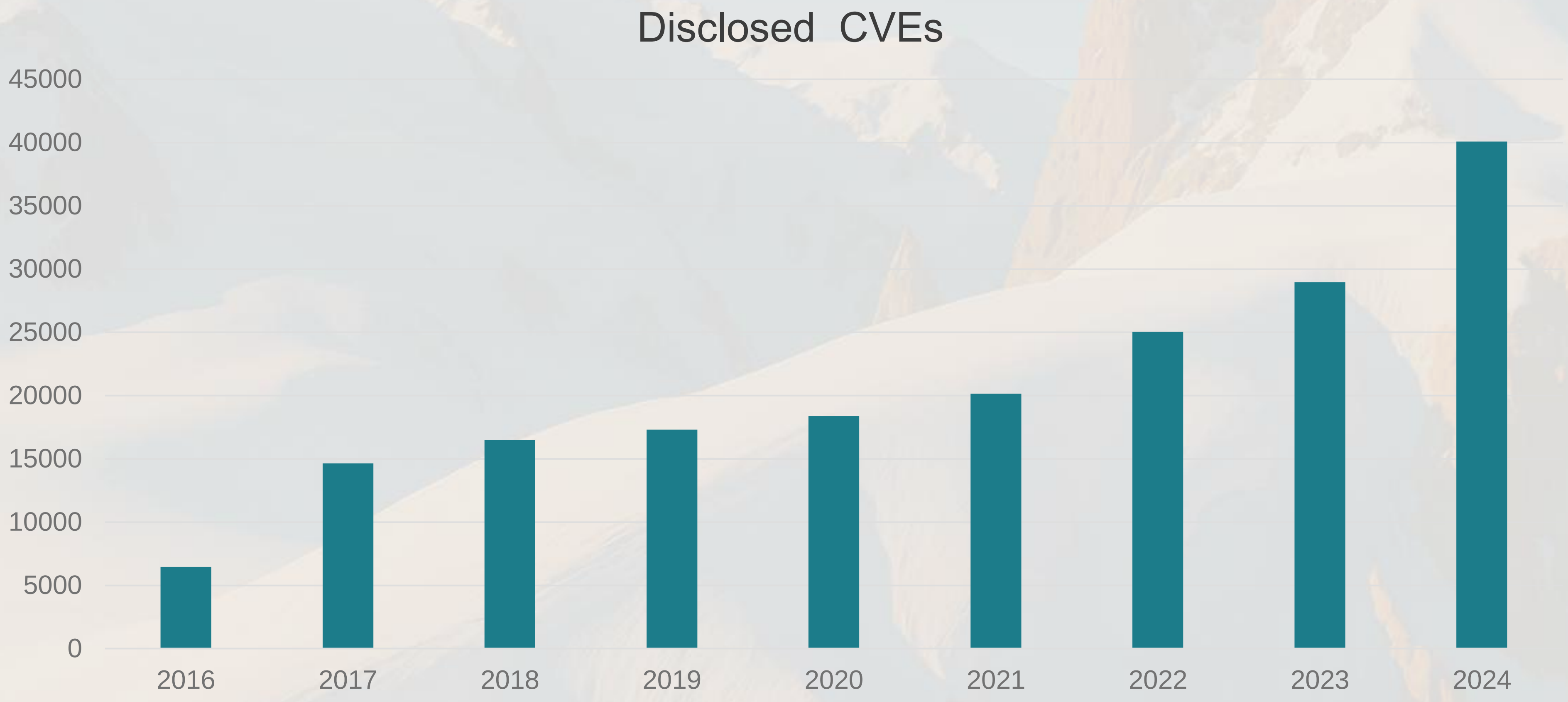
Pierluigi Paganini June 01, 2024

Threat Landscape



Source: CrowdStrike: https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf

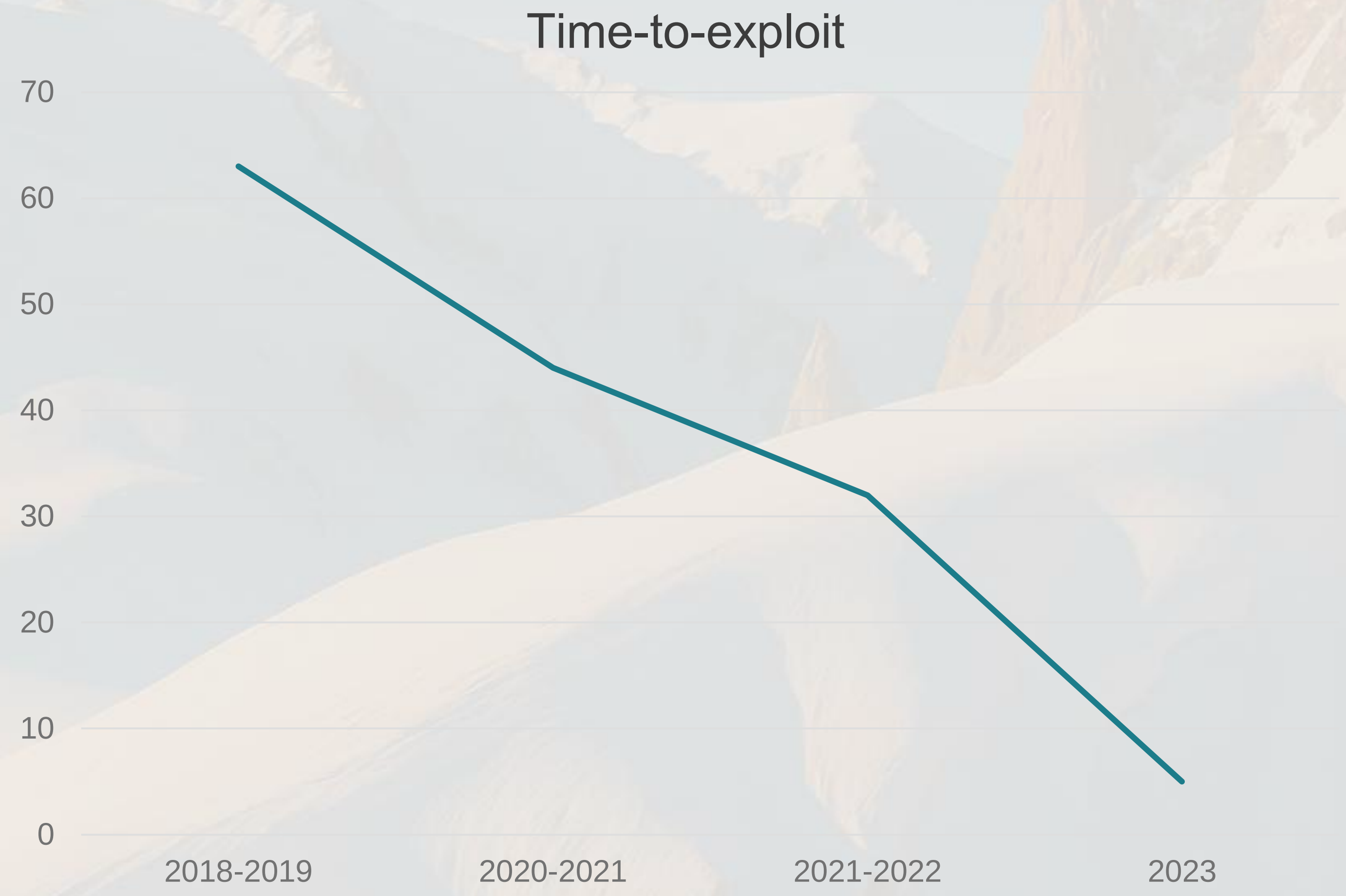
Threat Landscape



Source: Common Vulnerabilities and Exposures: https://www.cve.org/about/Metrics

mnemonic

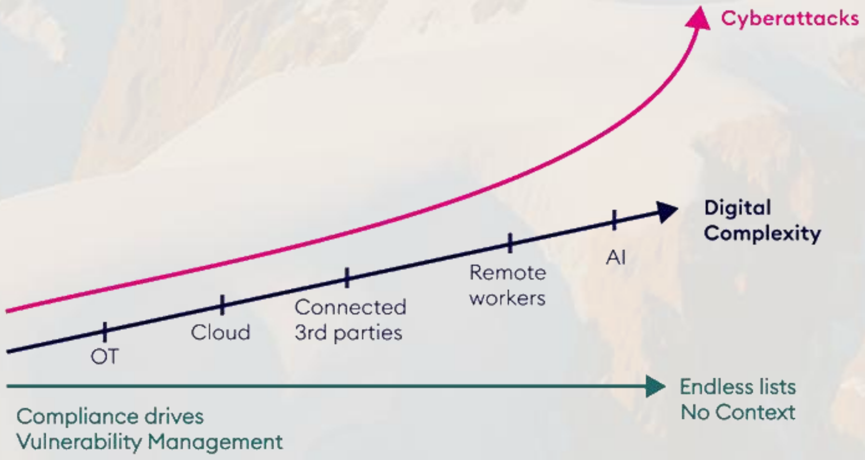
Threat Landscape



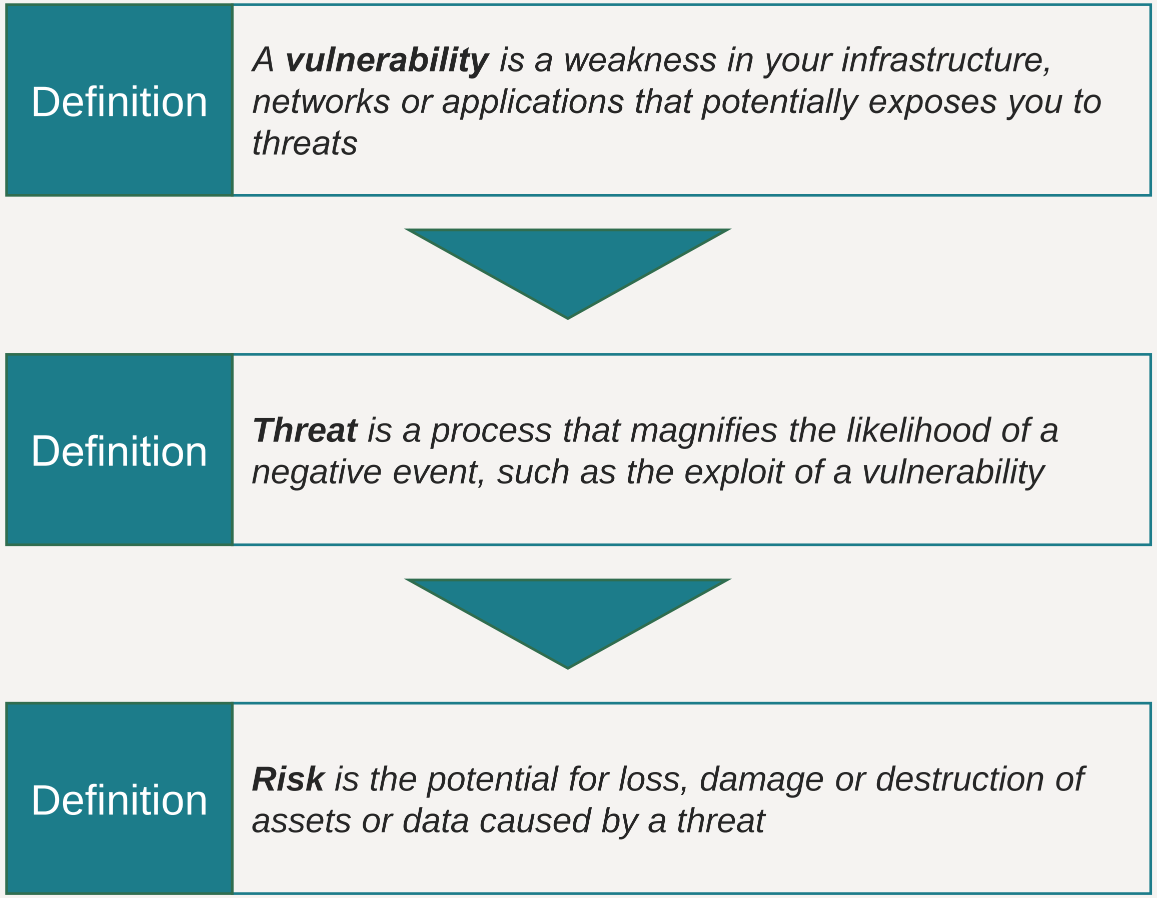
Source: Google Mandiant: https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022, https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023

“The Perfect Storm”

- **Expansion of Digital Footprint**
  - Modern attack surfaces include cloud services, IoT devices, and third-party integrations, in addition to traditional IT assets
- **Increased Complexity**
  - Rapid adoption of new technologies increases misconfigurations and unknown exposures
- **More Sophisticated Attackers**
  - The capabilities of threat actors are rapidly increasing, using AI and automations to facilitate continuous detection and rapid mass exploitations



Recap definitions…



Definition

*A **vulnerability** is a weakness in your infrastructure, networks or applications that potentially exposes you to threats*

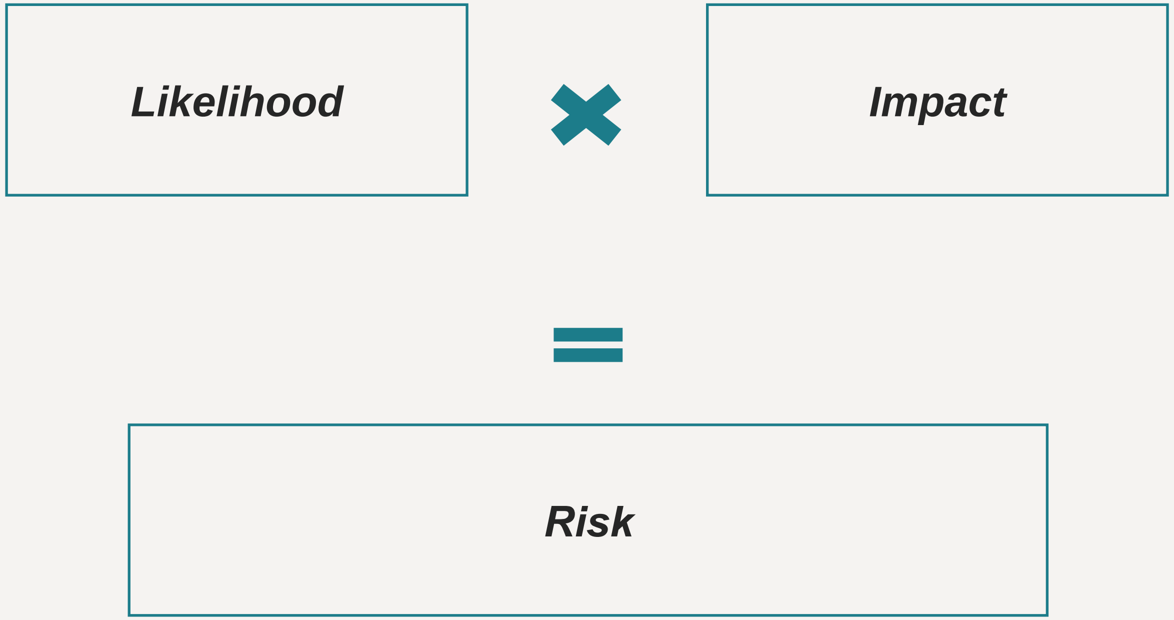
Definition

***Threat** is a process that magnifies the likelihood of a negative event, such as the exploit of a vulnerability*

Definition

***Risk** is the potential for loss, damage or destruction of assets or data caused by a threat*

Recap definitions…



Likelihood × *Impact*

=

Risk

Mission goal

*… for “**proactive security**”:*

*“Enhance **Cybersecurity resilience** by **reducing** the **likelihood** of successful attacks and **minimizing** the potential **impact** of any given threats”*

Mission goal

… for “__proactive security__”:

Cybersecurity resilience: reducing likelihood, minimizing impact

Mission goal

*… for “**proactive security**”:*

Cybersecurity resilience**: **reducing likelihood, minimizing impact

Note: **Removing** all **risk** is **not possible**…

- *Cannot patch all **vulnerabilities***
- *Cannot eliminate all **threats***

Externally: reduce attack surface, close open doors

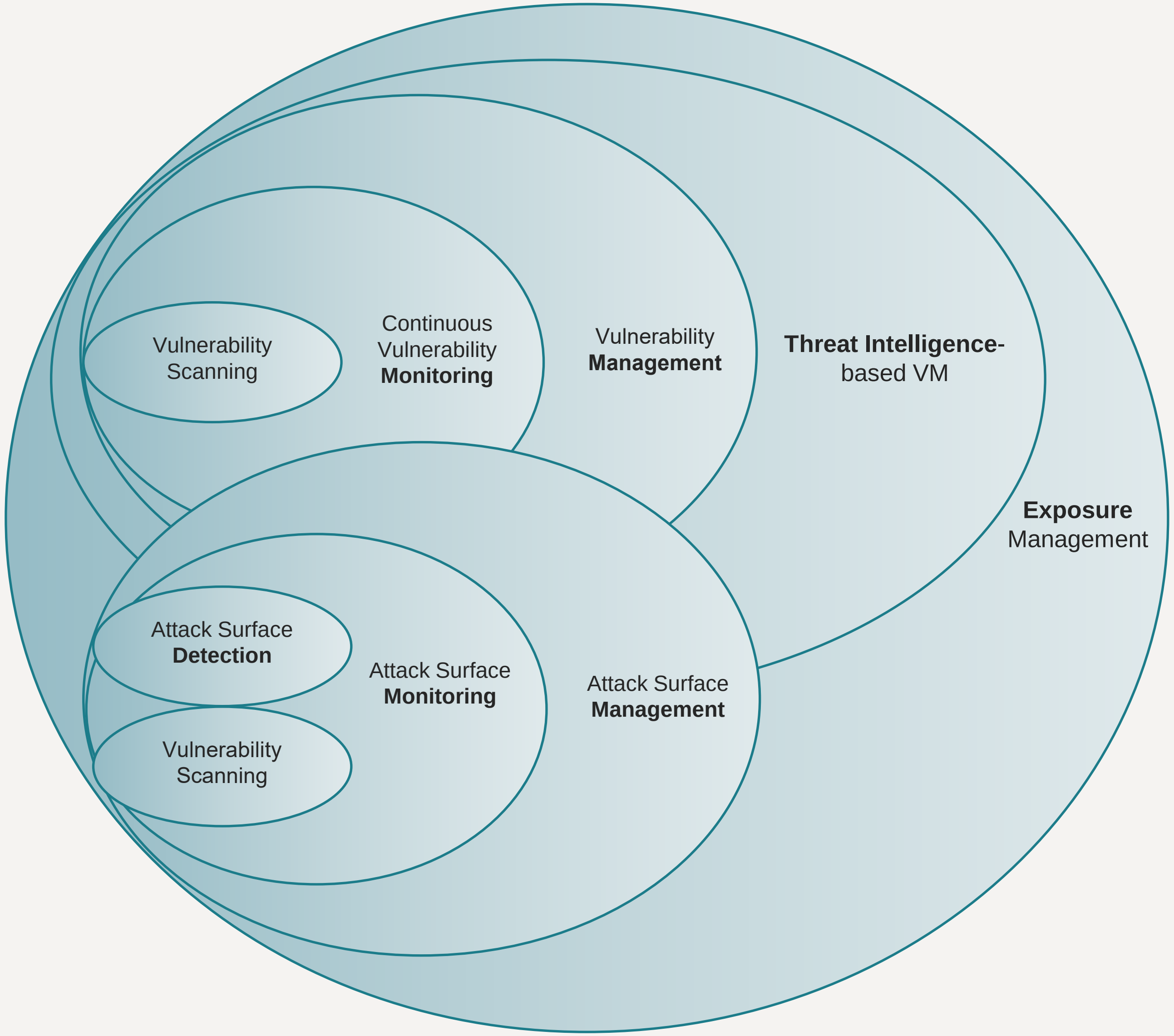
- *Run faster than the other guy*

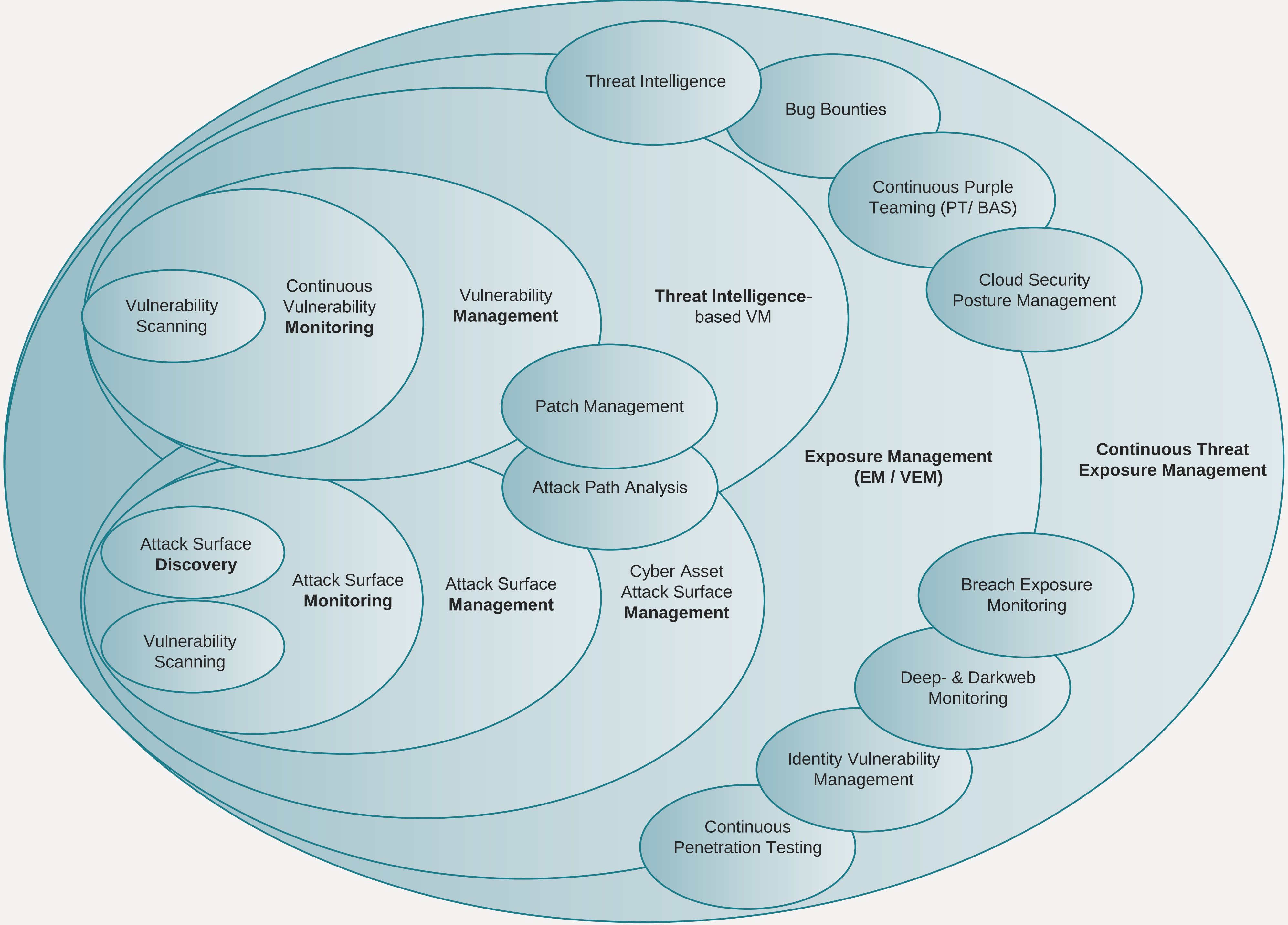
Internally: increase the required attack complexity

- *I.e. give your blue team enough time to detect and respond*

Evolution

- ***Vulnerability Scanning***
  - Assess your single on-prem perimeter firewall
- ***(Continuous) Vulnerability Monitoring***
  - Automatically assess your infrastructure at continuous intervals. Simple reporting
- ***Vulnerability Management***
  - Follow-up discovered vulnerabilities in a structured way, see trends, create reports, mitigate and resolve issues
- ***Attack Surface Management***
  - Expands with automatic asset detection. Attacker's perspective and smarter vulnerability prioritization.
- ***Threat Intelligence-based VM***
  - Increasingly sophisticated attackers necessitate more insight, actively using threat intelligence feeds
- ***Exposure Management***
  - Tougher prioritizing, shift from vulnerabilities to *validated exposures*
- ***Continuous Threat Exposure Management***
  - …


Vulnerability Scanning
Continuous Vulnerability **Monitoring**
Vulnerability **Management**
Threat Intelligence- based VM
Exposure Management
Attack Surface **Detection**
Vulnerability Scanning
Attack Surface **Monitoring**
Attack Surface **Management**


Threat Intelligence
Bug Bounties
Continuous Purple Teaming (PT/ BAS)
Cloud Security Posture Management
Vulnerability Scanning
Continuous Vulnerability **Monitoring**
Vulnerability **Management**
Threat Intelligence- based VM
Patch Management
Attack Path Analysis
Exposure Management (EM / VEM)
Continuous Threat Exposure Management
Attack Surface **Discovery**
Attack Surface **Monitoring**
Attack Surface **Management**
Cyber Asset Attack Surface **Management**
Vulnerability Scanning
Breach Exposure Monitoring
Deep- & Darkweb Monitoring
Identity Vulnerability Management
Continuous Penetration Testing

mnemonic

Continuous Threat Exposure Management

Definition	*«An integrated, iterative approach, made of five-steps cycles prioritizing and validating responses and optimizations to continually refine security posture improvements.»*

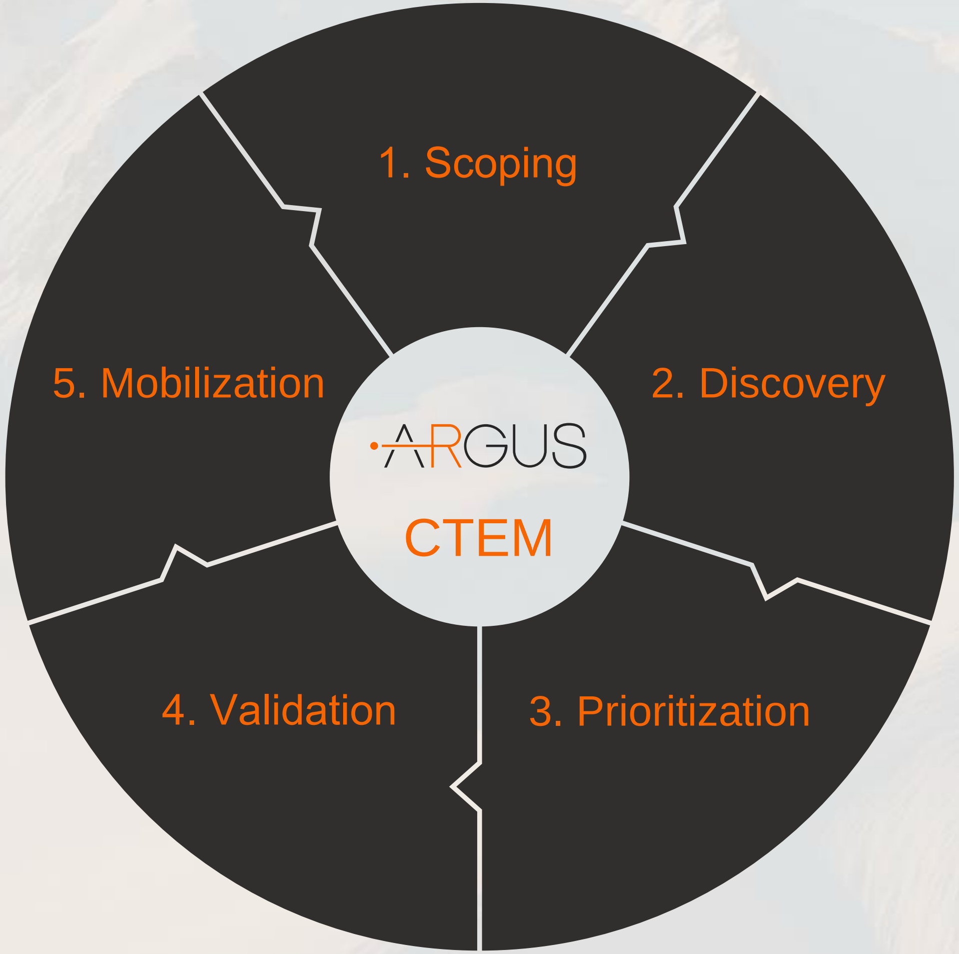
Gartner names CTEM as the second most important strategic technology trend for 2024 (right after AI …).

Source: Gartner

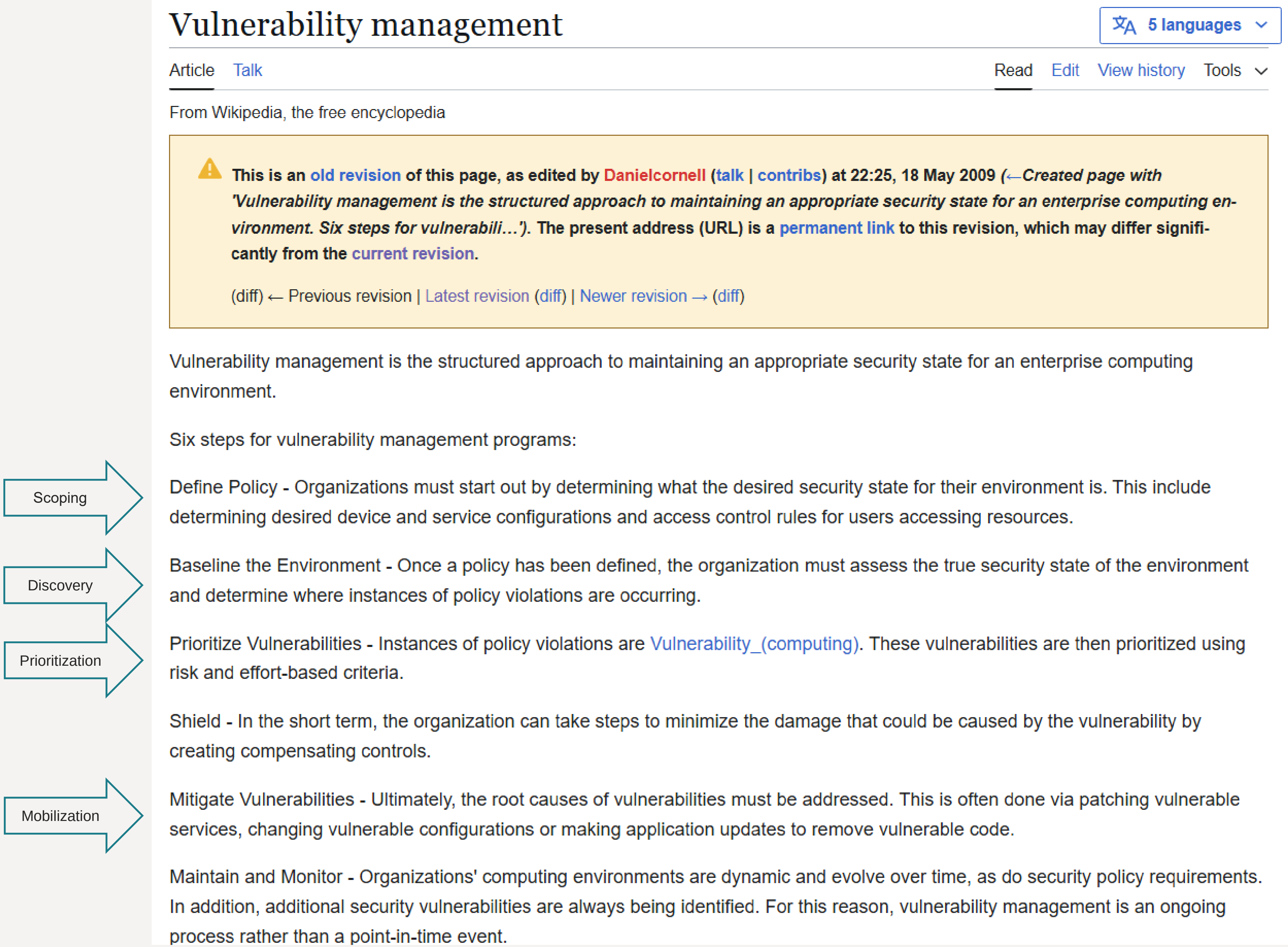
CTEM: Next-Gen VulnMgmt

- Focusing on **threats** and **exposures**
- Scope to **business goals**, not technical objectives
- Continuous **validation**
  - Proactive: assess security controls
  - Reactive: test detection and response

The CTEM Cycle



1. **Scoping**
   - Define specific business objects, key recourses, and their potential threat vectors
   - Start smaller, expand later
2. **Discover**
   - Inventory and categorize assets and exposures using several different solutions for discovery and assessment
3. **Prioritization**
   - Focus on exposures related to critical business objects, factoring in compensating controls and tolerance for residual risk
   - The goal is not to fix everything - assess based likelihood and impact
4. **Validation**
   - Simulate attack scenarios to validate findings, test the effectiveness of both mitigating controls and detection and response
   - Produce evidence for convincing business stakeholders
5. **Mobilization**
   - Mobilize resources to fix, mitigate, or accept discovered risks
   - Don’t fight symptoms – battle root causes



Vulnerability management

文A 5 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

⚠ **This is an old revision of this page, as edited by Danielcornell (talk | contribs) at 22:25, 18 May 2009 (*←Created page with 'Vulnerability management is the structured approach to maintaining an appropriate security state for an enterprise computing environment. Six steps for vulnerabili...'*). The present address (URL) is a permanent link to this revision, which may differ significantly from the current revision.**

(diff) ← Previous revision | Latest revision (diff) | Newer revision → (diff)

Vulnerability management is the structured approach to maintaining an appropriate security state for an enterprise computing environment.

Six steps for vulnerability management programs:

Scoping

Define Policy - Organizations must start out by determining what the desired security state for their environment is. This include determining desired device and service configurations and access control rules for users accessing resources.

Discovery

Baseline the Environment - Once a policy has been defined, the organization must assess the true security state of the environment and determine where instances of policy violations are occurring.

Prioritization

Prioritize Vulnerabilities - Instances of policy violations are Vulnerability_(computing). These vulnerabilities are then prioritized using risk and effort-based criteria.

Shield - In the short term, the organization can take steps to minimize the damage that could be caused by the vulnerability by creating compensating controls.

Mobilization

Mitigate Vulnerabilities - Ultimately, the root causes of vulnerabilities must be addressed. This is often done via patching vulnerable services, changing vulnerable configurations or making application updates to remove vulnerable code.

Maintain and Monitor - Organizations' computing environments are dynamic and evolve over time, as do security policy requirements. In addition, additional security vulnerabilities are always being identified. For this reason, vulnerability management is an ongoing process rather than a point-in-time event.

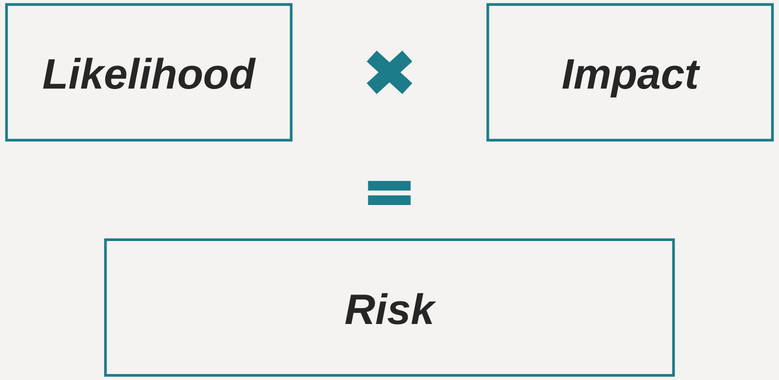
“Validation”

- Simulate attack scenarios to validate findings, test the effectiveness of both **mitigating controls** and **detection and response**

- **Proactive validation**: test mitigating controls
  - Can a given threat actually happened in our systems?
- **Reactive validation**: test detection and response
  - Can we sufficiently defend against this threat?

Proactive validation

- **Penetration testing** validates identified threats
- Three results:
  - Not possible to exploit (low **likelihood**)
  - Possible, but no results/little effect (low **impact**)
  - Possible, and exploitation gives results (high **likelihood** + high **impact** = high ***risk***)



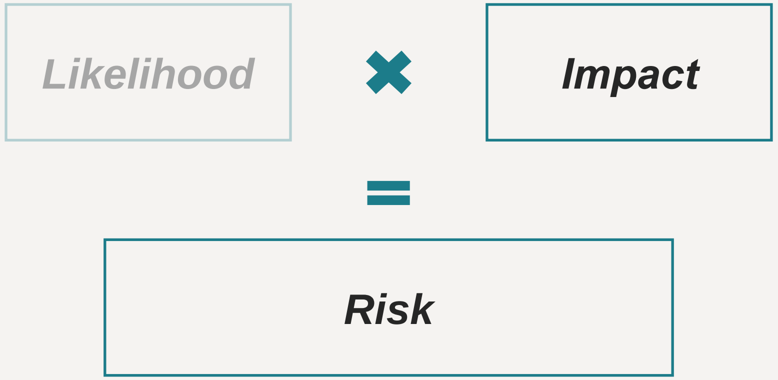
Likelihood ✖ ***Impact***

=

Risk

Reactive validation

- **Purple teaming** (or “BAS”) validates identified threats
- Three results for a given threat:
  - Detected and responded to
  - Detected but no response (medium **impact**)
  - No detections at all (high **impact**)

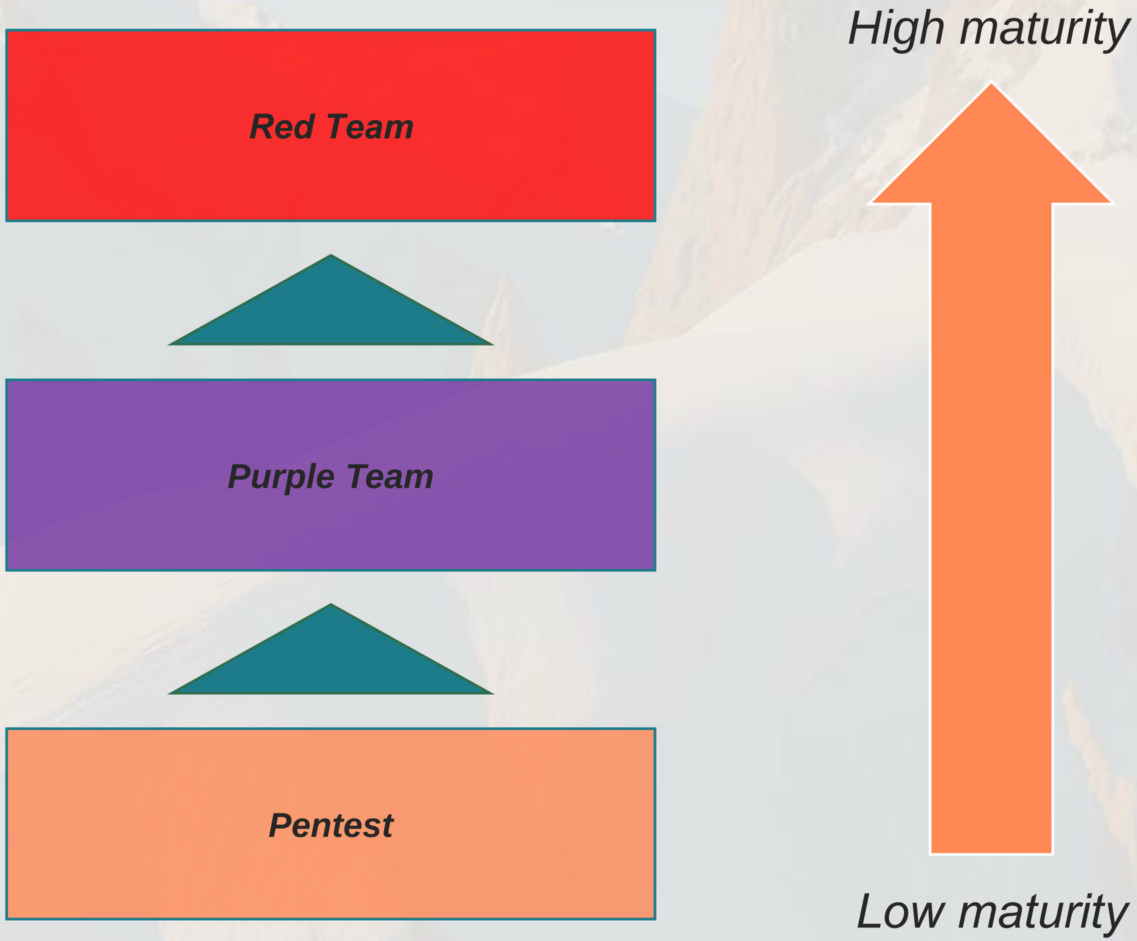


Likelihood ✖ *Impact*

=

Risk

Proactive validation + reactive validation



CTEM: Next-Gen VulnMgmt

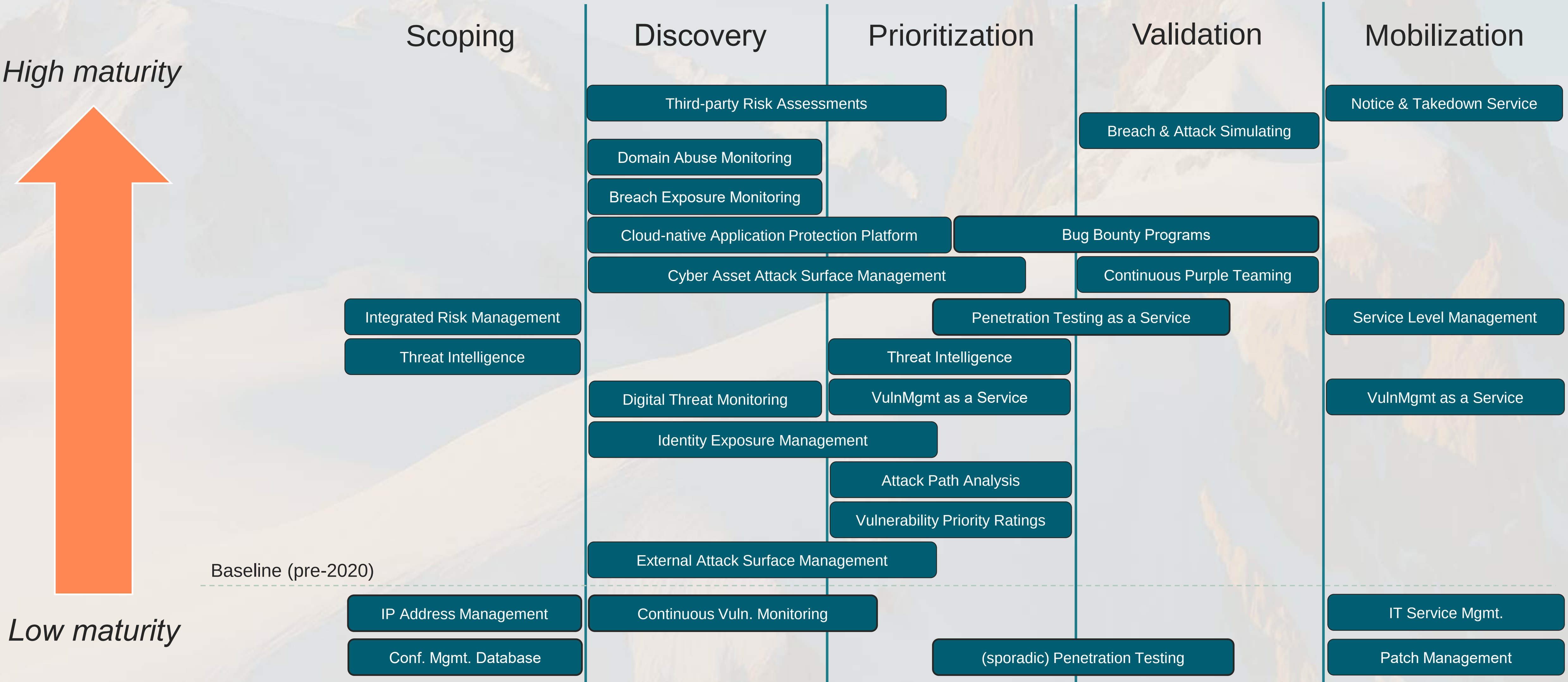
- *“A framework for working with the several different technologies, processes and solutions that this area now encompasses”*

“78% of Organizations Use More than 50 Different Cybersecurity Products to Address Security Issues”

- Not a new «*silver bullet*»
- Standard methodology for vulnerability management is still relevant
  - But this might make it easier to structure everything…

Source: Oracle and KPMG Cloud Threat Report

CTEM in Practice



Scoping | Discovery | Prioritization | Validation | Mobilization

High maturity

Third-party Risk Assessments

Notice & Takedown Service

Breach & Attack Simulating

Domain Abuse Monitoring

Breach Exposure Monitoring

Cloud-native Application Protection Platform

Bug Bounty Programs

Cyber Asset Attack Surface Management

Continuous Purple Teaming

Integrated Risk Management

Penetration Testing as a Service

Service Level Management

Threat Intelligence

Threat Intelligence

Digital Threat Monitoring

VulnMgmt as a Service

VulnMgmt as a Service

Identity Exposure Management

Attack Path Analysis

Vulnerability Priority Ratings

Baseline (pre-2020)

External Attack Surface Management

IP Address Management

Continuous Vuln. Monitoring

IT Service Mgmt.

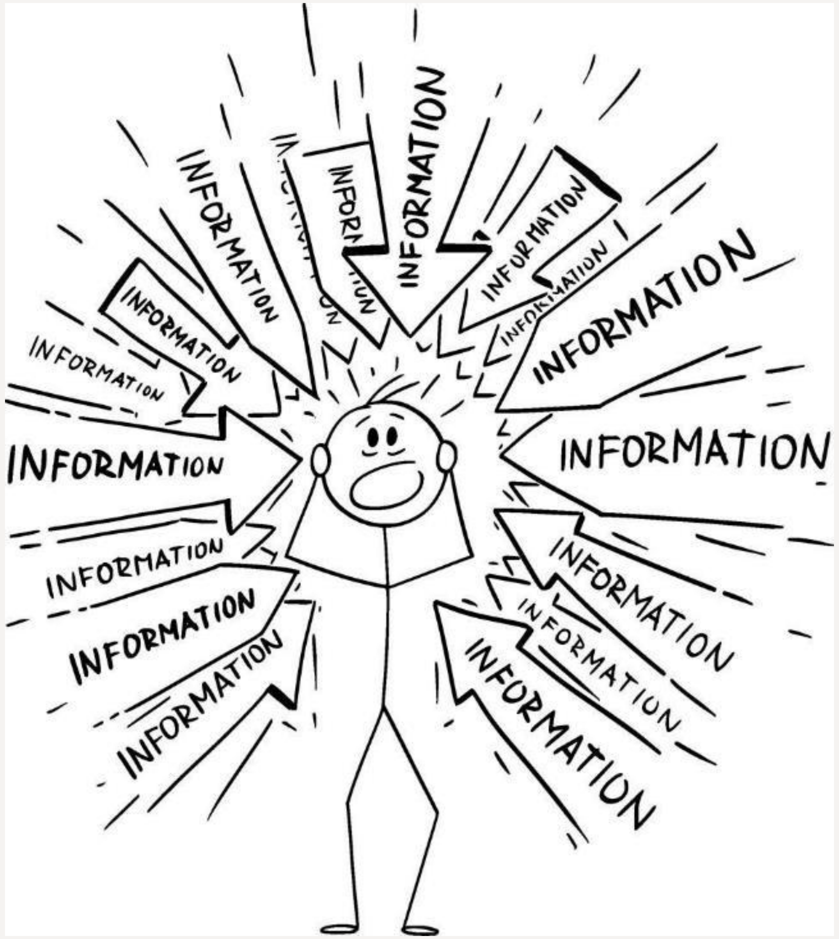
Low maturity

Conf. Mgmt. Database

(sporadic) Penetration Testing

Patch Management

mnemonic

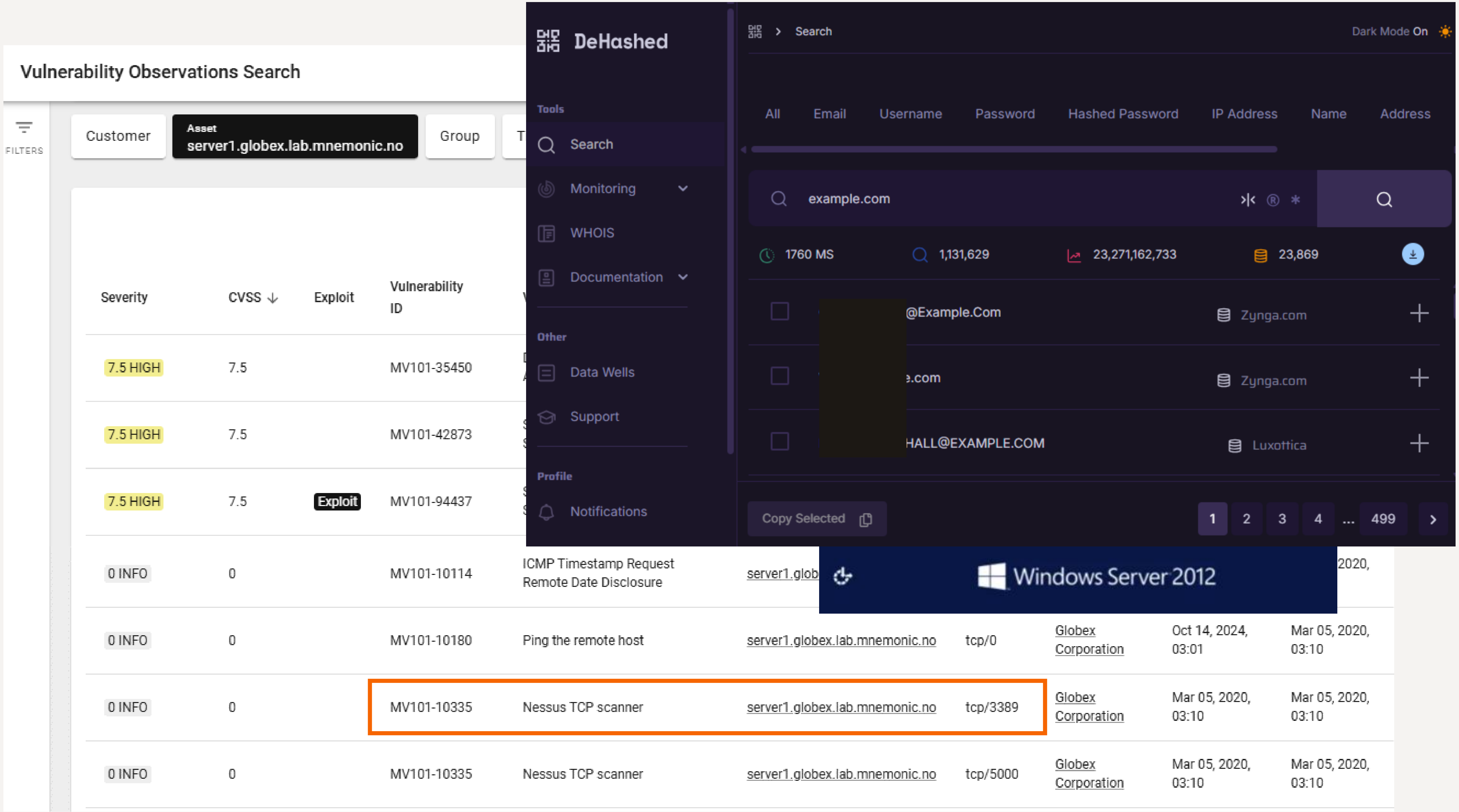

INFORMATION

Key takeaways

- **Pick-and-choose**
  - Do not try to implement all at once, focus on aspects that makes most sense for your organization
  - In most cases, for quick ROI: start with EASM

Key takeaways

- **Pick-and-choose**
  - Do not try to implement all at once, focus on aspects that makes most sense for your organization
  - In most cases, for quick ROI: start with EASM
- **Shift focus: *exposures, not vulnerabilities***
  - Focus on removing exposures, not solely vulnerabilities and patching



Vulnerability Observations Search

FILTERS

Customer | Asset server1.globex.lab.mnemonic.no | Group | T

Severity	CVSS ↓	Exploit	Vulnerability ID						
7.5 HIGH	7.5		MV101-35450						
7.5 HIGH	7.5		MV101-42873						
7.5 HIGH	7.5	Exploit	MV101-94437						
0 INFO	0		MV101-10114	ICMP Timestamp Request Remote Date Disclosure	server1.glob				2020,
0 INFO	0		MV101-10180	Ping the remote host	server1.globex.lab.mnemonic.no	tcp/0	Globex Corporation	Oct 14, 2024, 03:01	Mar 05, 2020, 03:10
0 INFO	0		MV101-10335	Nessus TCP scanner	server1.globex.lab.mnemonic.no	tcp/3389	Globex Corporation	Mar 05, 2020, 03:10	Mar 05, 2020, 03:10
0 INFO	0		MV101-10335	Nessus TCP scanner	server1.globex.lab.mnemonic.no	tcp/5000	Globex Corporation	Mar 05, 2020, 03:10	Mar 05, 2020, 03:10

DeHashed

Search

Dark Mode On

example.com

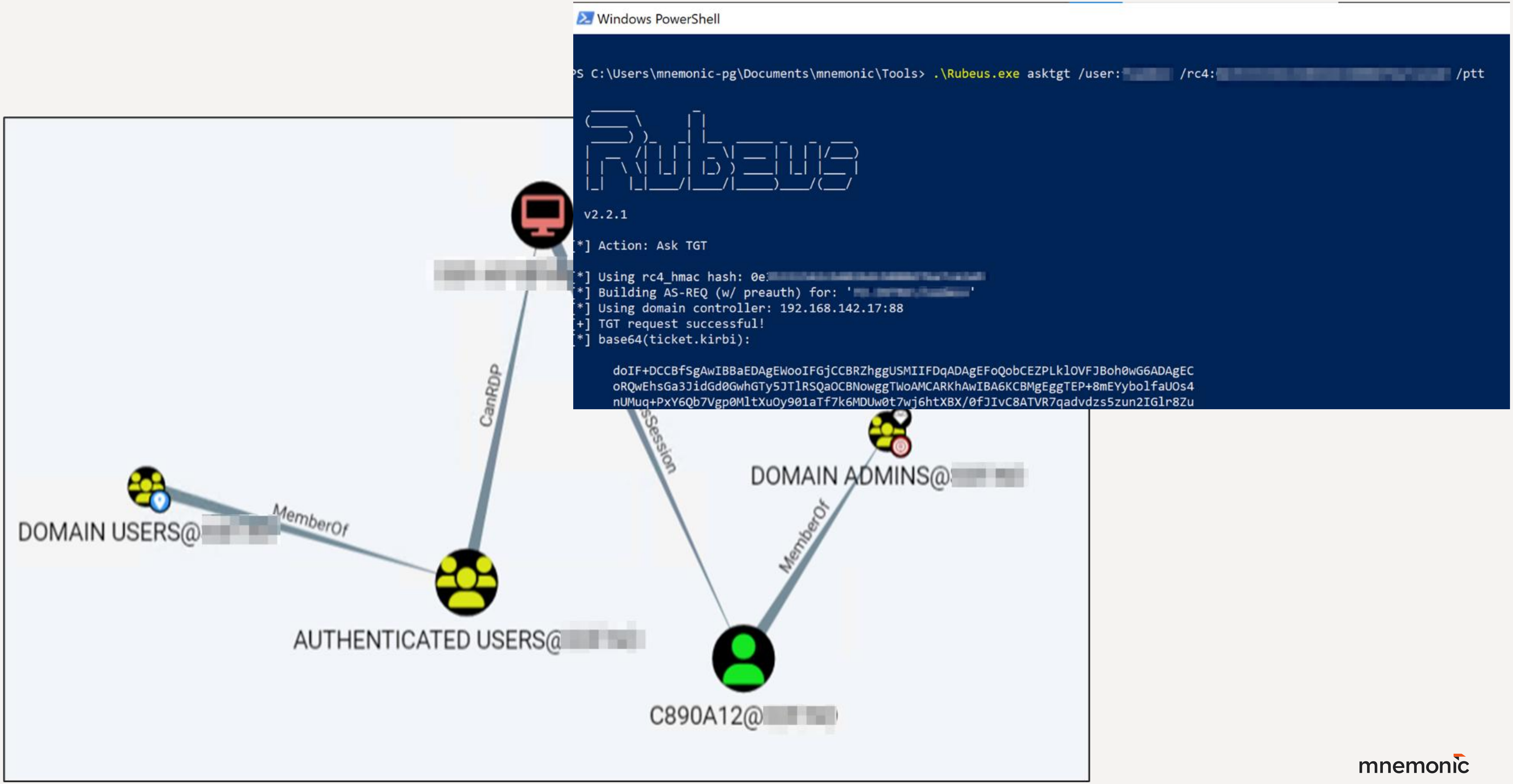
1760 MS | 1,131,629 | 23,271,162,733 | 23,869

□	[redacted]@Example.Com	Zynga.com
□	[redacted].com	Zynga.com
□	[redacted]HALL@EXAMPLE.COM	Luxottica

Windows Server 2012

Key takeaways

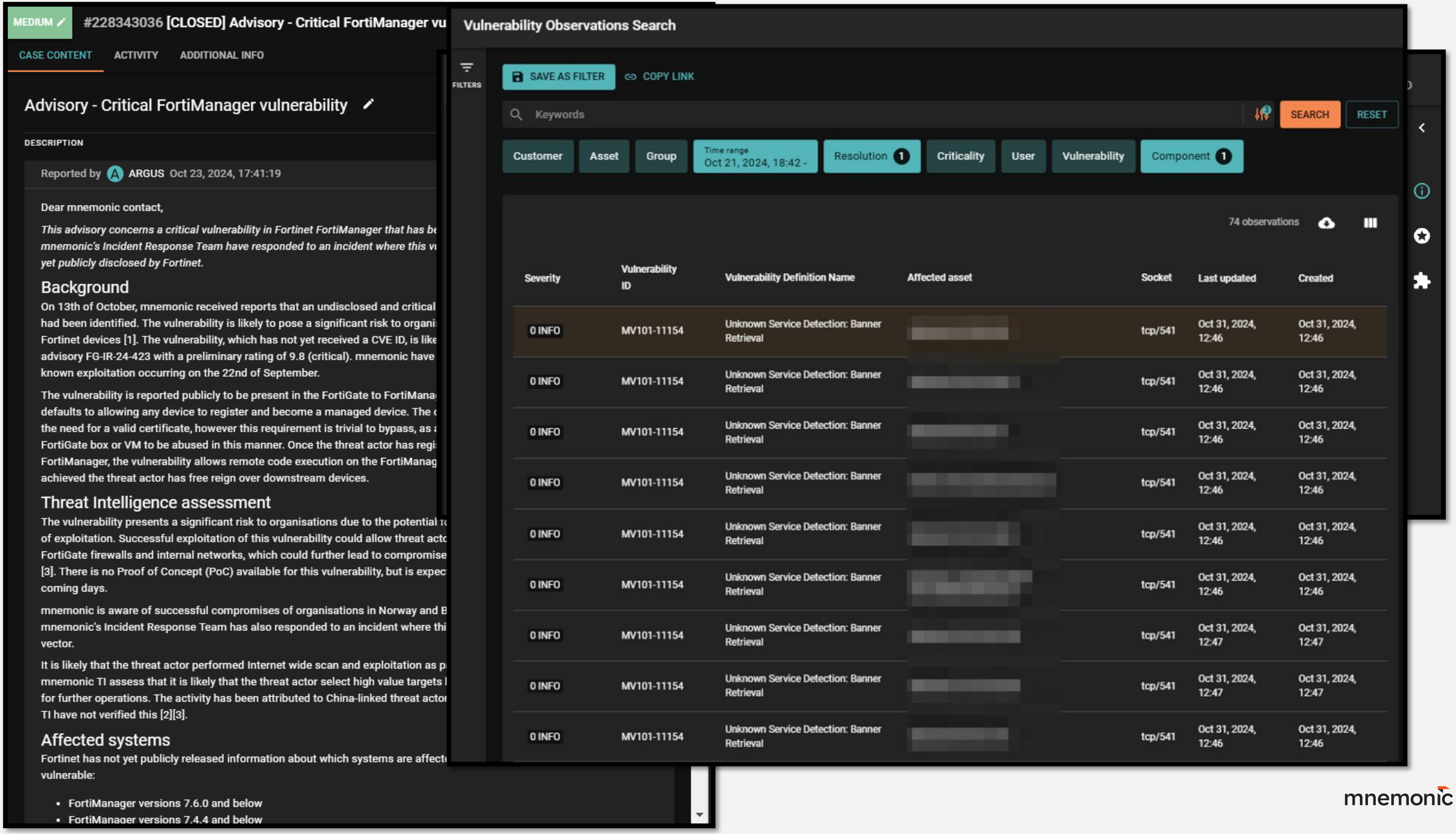
- **Pick-and-choose**
  - Do not try to implement all at once, focus on aspects that makes most sense for your organization
  - In most cases, for quick ROI: start with EASM
- **Shift focus: *exposures, not vulnerabilities***
  - Focus on removing exposures, not solely vulnerabilities and patching
- **Do not forget Identities**
  - An attacker's best friend is on-prem AD when the organization is "moving to the cloud"



```
PS C:\Users\mnemonic-pg\Documents\mnemonic\Tools> .\Rubeus.exe asktgt /user:[redacted] /rc4:[redacted] /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.1

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 0e[redacted]
[*] Building AS-REQ (w/ preauth) for: '[redacted]'
[*] Using domain controller: 192.168.142.17:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIF+DCCBfSgAwIBBaEDAgEWooIFGjCCBRZhggUSMIIFDqADAgEFoQobCEZPLklOVFJBoh0wG6ADAgEC
      oRQwEhsGa3JidGd0GwhGTy5JTlRSQaOCBNowggTWoAMCARKhAwIBA6KCBMgEggTEP+8mEYybolfaUOs4
      nUMuq+PxY6Qb7Vgp0MltXuOy901aTf7k6MDUw0t7wj6htXBX/0fJIvC8ATVR7qadvdzs5zun2IGlr8Zu
```

Key takeaways

- **Pick-and-choose**
  - Do not try to implement all at once, focus on aspects that makes most sense for your organization
  - In most cases, for quick ROI: start with EASM
- **Shift focus: *exposures, not vulnerabilities***
  - Focus on removing exposures, not solely vulnerabilities and patching
- **Do not forget Identities**
  - An attacker's best friend is on-prem AD when the organization is "moving to the cloud"
- **Threat Intelligence**
  - Leverage TI information in all cycles of the process, from scoping to mobilization



#228343036 [CLOSED] Advisory - Critical FortiManager vu

Advisory - Critical FortiManager vulnerability

DESCRIPTION

Reported by A ARGUS Oct 23, 2024, 17:41:19

Dear mnemonic contact,

This advisory concerns a critical vulnerability in Fortinet FortiManager that has be
mnemonic's Incident Response Team have responded to an incident where this v
yet publicly disclosed by Fortinet.

Background

On 13th of October, mnemonic received reports that an undisclosed and critical
had been identified. The vulnerability is likely to pose a significant risk to organi
Fortinet devices [1]. The vulnerability, which has not yet received a CVE ID, is like
advisory FG-IR-24-423 with a preliminary rating of 9.8 (critical). mnemonic have
known exploitation occurring on the 22nd of September.

The vulnerability is reported publicly to be present in the FortiGate to FortiMana
defaults to allowing any device to register and become a managed device. The
the need for a valid certificate, however this requirement is trivial to bypass, as
FortiGate box or VM to be abused in this manner. Once the threat actor has regi
FortiManager, the vulnerability allows remote code execution on the FortiManag
achieved the threat actor has free reign over downstream devices.

Threat Intelligence assessment

The vulnerability presents a significant risk to organisations due to the potential
of exploitation. Successful exploitation of this vulnerability could allow threat acto
FortiGate firewalls and internal networks, which could further lead to compromise
[3]. There is no Proof of Concept (PoC) available for this vulnerability, but is expec
coming days.

mnemonic is aware of successful compromises of organisations in Norway and B
mnemonic's Incident Response Team has also responded to an incident where thi
vector.

It is likely that the threat actor performed Internet wide scan and exploitation as p
mnemonic TI assess that it is likely that the threat actor select high value targets
for further operations. The activity has been attributed to China-linked threat acto
TI have not verified this [2][3].

Affected systems

Fortinet has not yet publicly released information about which systems are affect
vulnerable:

- FortiManager versions 7.6.0 and below
- FortiManager versions 7.4.4 and below

Vulnerability Observations Search

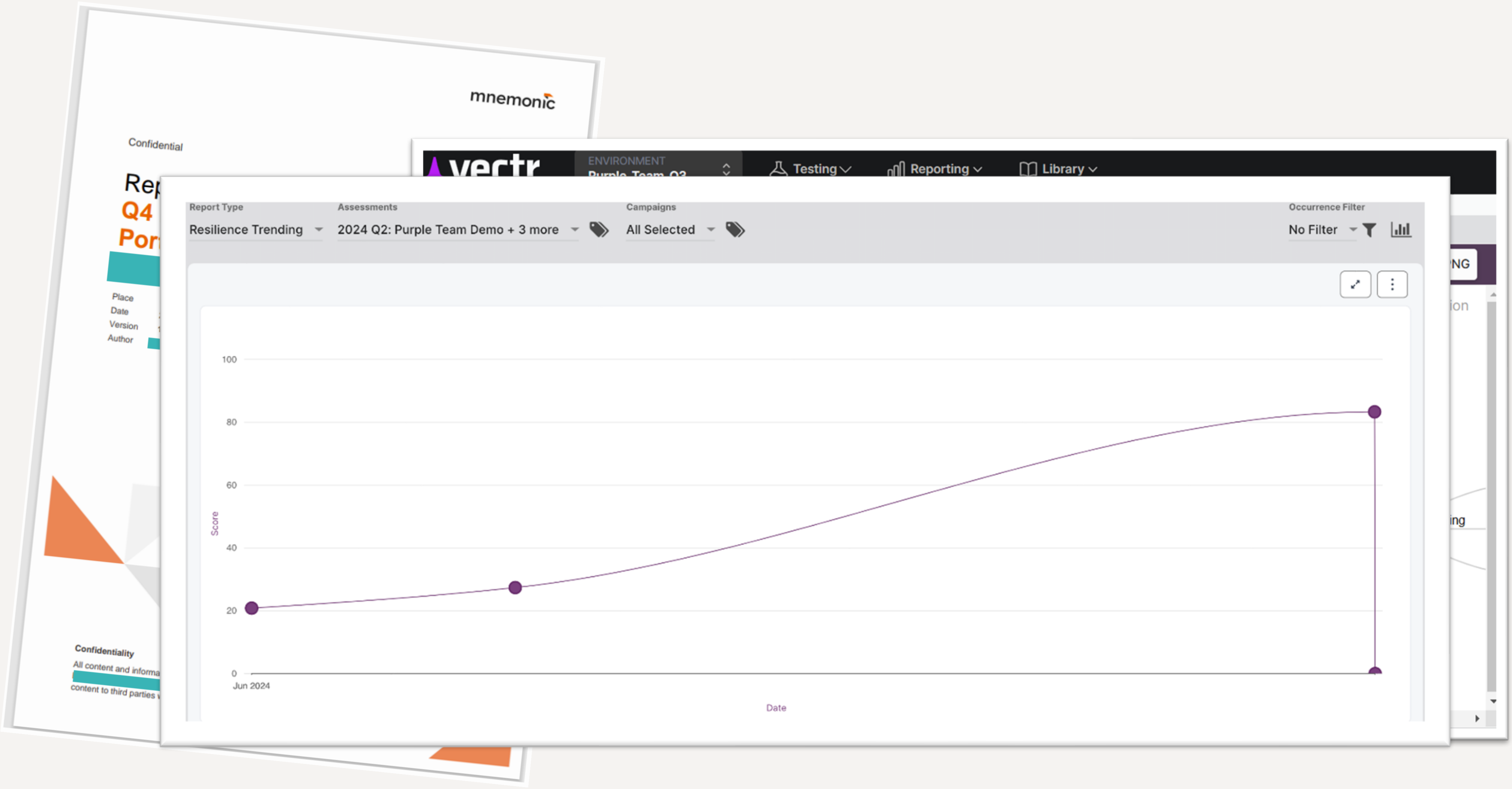
Customer | Asset | Group | Time range Oct 21, 2024, 18:42 - | Resolution 1 | Criticality | User | Vulnerability | Component 1

74 observations

Severity	Vulnerability ID	Vulnerability Definition Name	Affected asset	Socket	Last updated	Created
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:46	Oct 31, 2024, 12:46
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:46	Oct 31, 2024, 12:46
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:46	Oct 31, 2024, 12:46
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:46	Oct 31, 2024, 12:46
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:46	Oct 31, 2024, 12:46
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:46	Oct 31, 2024, 12:46
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:47	Oct 31, 2024, 12:47
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:47	Oct 31, 2024, 12:47
0 INFO	MV101-11154	Unknown Service Detection: Banner Retrieval	[redacted]	tcp/541	Oct 31, 2024, 12:46	Oct 31, 2024, 12:46

Key takeaways

- **Pick-and-choose**
  - Do not try to implement all at once, focus on aspects that makes most sense for your organization
  - In most cases, for quick ROI: start with EASM
- **Shift focus: *exposures, not vulnerabilities***
  - Focus on removing exposures, not solely vulnerabilities and patching
- **Do not forget Identities**
  - An attacker's best friend is on-prem AD when the organization is "moving to the cloud"
- **Threat Intelligence**
  - Leverage TI information in all cycles of the process, from scoping to mobilization
- **Continuous validations**
  - Implement continuous proactive (penetration testing) and reactive (purple teaming / BAS) validating steps



mnemonic

Confidential

Rep

Q4

Por

Place

Date

Version

Author

Confidentiality

All content and informa

content to third parties

vectr

ENVIRONMENT

Purple Team Q3

Testing

Reporting

Library

Report Type: Resilience Trending

Assessments: 2024 Q2: Purple Team Demo + 3 more

Campaigns: All Selected

Occurrence Filter: No Filter

Key takeaways

- **Pick-and-choose**
  - Do not try to implement all at once, focus on aspects that makes most sense for your organization
  - In most cases, for quick ROI: start with EASM
- **Shift focus: *exposures, not vulnerabilities***
  - Focus on removing exposures, not solely vulnerabilities and patching
- **Do not forget Identities**
  - An attacker's best friend is on-prem AD when the organization is "moving to the cloud"
- **Threat Intelligence**
  - Leverage TI information in all cycles of the process, from scoping to mobilization
- **Continuous validations**
  - Implement continuous proactive (penetration testing) and reactive (purple teaming / BAS) validating steps

mnemonic

Thank you!

mnemonic

Peder Grundvold
Service Lead Exposure Management | TRS
+47 907 34 010
peder@mnemonic.no

mnemonic AS | Henrik Ibsens Gate 100, 0255 Oslo

mnemonic.io/solutions/vulnerability-and-exposure-management