VULNERABILITY MANAGEMENT

Martin Karel
Global Vulnerability Management and Offensive Security Lead

Jenifer Jiménez
Vulnerability Management Platform Architect

Angelo Punturiero
Vulnerability Management Specialist
1. Who is starting the VM process after scanning the assets?

2. Who is doing some adhoc activities for Critical vulnerabilities?

3. Who has full overview of all VM related activities and their current status?
**CVE Timeline**

- **t0**: Discovered by researcher
  - Vulnerability is discovered and reported to the vendor

- **t1**: Published by vendor
  - Vendor release the fix

- **tE**: Exploit public
  - Vulnerability is exploited

- **t2**: Found by scanner
  - The vulnerability scanner vendor release the signature and all the systems in scope are scanned

**Time to Detect**
- T1 to T2, an average time to have a vulnerability detected on system is about 70 days.

**Time to Exploit**
- T1 to TE, vulnerabilities are being publicly exploited between 0 and 60 days, in average 19 Days

**Only 30% coverage**
- In average only about 30% of Critical and High vulnerabilities have a scanning signature

Statistics are calculated based on data from the past 3 years.
**VM Approach Options**

**Scanning approach**
- Discovered Vulnerabilities
  - Scanner finding Ticket

**Bulletin Approach**
- Vulnerability feeds
  - Bundle
  - Bulletin Ticket

**Pros / Cons**

**Scanning approach Pros**
- Exact vulnerability and risk exposure tracking
- Assurance of the resolution

**Scanning approach Cons**
- Costly and time consuming
- Scanner technology coverage
- Large number of vulnerabilities
- Frequent ownership problems

**Bulletin approach Pros**
- Prompt availability of the assessment
- Can be better aligned with Patch process
- Easy to setup

**Bulletin approach Cons**
- Only theoretical alerts
- No exact tracking of affected systems
Combined process

Combined approach

- Prompt availability of the assessment
- Can be aligned with Patching calendar
- Provides precise tracking of resolution

- Reduce number of Unassigned scanner findings
- Enable complex-shared ownership model
- Better SLA calculation

Vulnerability feeds → CPE subscription → Bundle → Patching Calendar

Discovered Vulnerabilities → Remaining Vulnerabilities → Scanner finding Ticket → Patch Tracking Ticket

Team 1

Fallback owner
**Patch Tracking Ticket**

- **Vulnerability feeds**
- **Nestlé inventories**
- **Scanners**

**Feed Based CVEs**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Nestlé Rating</th>
<th>Vuln #</th>
<th>Max CVSS3</th>
<th>Exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office</td>
<td>HIGH</td>
<td>5</td>
<td>7.8</td>
<td>NO</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>HIGH</td>
<td>41</td>
<td>8.8</td>
<td>NO</td>
</tr>
<tr>
<td>Windows Server 2011</td>
<td>HIGH</td>
<td>49</td>
<td>8.8</td>
<td>NO</td>
</tr>
</tbody>
</table>

**Vulnerability Scanning**

<table>
<thead>
<tr>
<th>Confirmed Vulnerability Count</th>
<th>Confirmed Patched/Vulnerability Count</th>
<th>Saved %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1041</td>
<td>491</td>
<td>47.64%</td>
</tr>
</tbody>
</table>

**Detected Vulnerabilities**

<table>
<thead>
<tr>
<th>Status</th>
<th>Title</th>
<th>Hostname</th>
<th>IP</th>
<th>CVSS</th>
<th>Severity</th>
<th>Risk Rating</th>
<th>First Found</th>
<th>Last Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Microsoft Office and Microsoft Office Services and Web Apps Security Update (June 2020)</td>
<td></td>
<td>13</td>
<td>CPE</td>
<td>Critical</td>
<td>9.9</td>
<td>06-29-2020</td>
<td>06-30-2020</td>
</tr>
<tr>
<td></td>
<td>AD20076T Microsoft Windows Adobe Flash Player Security Update for June 2020 (AD20076T)</td>
<td></td>
<td>18</td>
<td>CPE</td>
<td>Critical</td>
<td>9.9</td>
<td>06-30-2020</td>
<td>06-30-2020</td>
</tr>
<tr>
<td></td>
<td>AD20076T Microsoft Windows Adobe Flash Player Security Update for June 2020 (AD20076T)</td>
<td></td>
<td>18</td>
<td>CPE</td>
<td>Critical</td>
<td>9.9</td>
<td>06-30-2020</td>
<td>06-30-2020</td>
</tr>
<tr>
<td></td>
<td>AD20076T Microsoft Internet Explorer Security Update for June 2020</td>
<td></td>
<td>13</td>
<td>CPE</td>
<td>Critical</td>
<td>9.9</td>
<td>07-12-2020</td>
<td>06-30-2020</td>
</tr>
<tr>
<td></td>
<td>AD20076T Microsoft Windows Adobe Flash Player Security Update for June 2020 (AD20076T)</td>
<td></td>
<td>18</td>
<td>CPE</td>
<td>Critical</td>
<td>9.9</td>
<td>06-30-2020</td>
<td>06-30-2020</td>
</tr>
</tbody>
</table>

**Scanner Findings**
Vulnerability Management Tasks

- Monitoring Threats and Vulnerabilities
- Discovering Attack surface
- Discovering vulnerabilities on Nestle assets
- Offensive Security
- Orchestration and reporting
Collecting information on threats and vulnerabilities from various internal and external sources and further enriching it for risk calculations, resulting in unified Nestlé vulnerability rating.

1. Identification and assessment of potential vulnerabilities in deployed technologies.
2. Dynamic prioritization based on vulnerability intelligence and current threat exploitability.
3. Optionally, this capability can be aligned with custom patching calendars and SLAs and it can automatically synchronize with existing ITSM processes and tools.
4. When combined with Vulnerability Scanning, the vulnerabilities can be practically tested, and the resolution automatically tracked.
<table>
<thead>
<tr>
<th>Monitoring Threats and Vulnerabilities</th>
<th>Discovering Attack surface</th>
<th>Discovering vulnerabilities on Nestle assets</th>
<th>Offensive Security</th>
<th>Orchestration and reporting</th>
</tr>
</thead>
</table>

![Image](https://url-to-image.com)
# CVE Investigation & Enrichments

## Monitoring Threats and Vulnerabilities

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Local</th>
<th>Remote</th>
<th>Wormable</th>
<th>Disclosed</th>
<th>Exploited</th>
<th>Popular</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileges Required</td>
<td>N</td>
<td>L</td>
<td>H</td>
<td>N</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>User Interaction</td>
<td>N</td>
<td>R</td>
<td>N</td>
<td>R</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Integrity</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Automatable (v4.0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Exploit Code Maturity</td>
<td></td>
<td></td>
<td></td>
<td>P</td>
<td>F</td>
<td>H</td>
</tr>
<tr>
<td>Exploit Maturity (v4.0)</td>
<td></td>
<td></td>
<td></td>
<td>P</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

## CVSS Details

- **CSOC Warns**: + + + +
- **Source Feed**: + + +
- **References**: + + +
- **Countermeasures**: + +
- **CISA Known**: +

## Enrichments

- **Discovering Attack surface**
- **Discovering vulnerabilities on Nestle assets**
- **Offensive Security**
- **Orchestration and reporting**

## Countermeasures

- **IDS**
- **IPS**
- **WAF**
- **EDR**

## Source Feed

- **CVE Investigation & Enrichments**

## Discovering Vulnerabilities on Nestle Assets

- **Discovering Asset Surface**
- **Offensive Security**
- **Orchestration and Reporting**

## Countermeasure Hits Trend

- **Daily Hits By Action**
- **Countermeasure Hits Trend**

## Information Technology
CVE Investigation & Enrichments

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Local</th>
<th>Remote</th>
<th>Wormable</th>
<th>Disclosed</th>
<th>Exploited</th>
<th>Popular</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>
| Privileges Required | N | L | H | N
| User Interaction | N | R | N | N
| Integrity | L | H | L | H |
| Automatable (v4.0) | L | H | YES |
| Exploit Code Maturity | P | F | H | P |
| Exploit Maturity (v4.0) | P | A |

CSOC Warns | + | + | +
Source Feed | + | + | +
References | + | + | +
Countermeasures | + | + | +
CISA Known | + | |

Countermeasures

IDS
IPS
WAF
EDR
SIEM

Settings

Critical + Popular → Burning
Wormable + Exploited → Critical Candidates
High + Popular → Important
## CVE Investigation & Enrichments

### Monitoring Threats and Vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>Discovering Attack surface</th>
<th>Discovering vulnerabilities on Nestle assets</th>
<th>Offensive Security</th>
<th>Orchestration and reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Local</td>
<td>Remote</td>
<td>Wormable</td>
<td>Disclosed</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>N</td>
<td>L</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>User Interaction</td>
<td>N</td>
<td>L</td>
<td>H</td>
<td>N</td>
</tr>
<tr>
<td>Integrity</td>
<td>N</td>
<td>R</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Automatable (v4.0)</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
</tr>
</tbody>
</table>

### CVSS Details

- **Attack Vector:**
  - Local: L
  - Remote: P
- **Privileges Required:**
  - N
- **User Interaction:**
  - N
- **Integrity:**
  - N
- **Automatable (v4.0):**
  - YES
- **Exploit Code Maturity:**
  - P
- **Exploit Maturity (v4.0):**
  - P

### Enrichments

- **CSOC Warns:** + + + +
- **Source Feed:** + + + +
- **References:** + + +
- **Countermeasures:** + + +
- **CISA Known:** +

### Countermeasures

- **Offensive Security:**
  - IDS
  - IPS
  - WAF
  - EDR

- **CIAM:**
  - NVD
  - flexera
  - Github
  - PasteBin

- **Cyber SOC Threat Intelligence:**
  - Microsoft
  - SAP
  - RedHat
  - Oracle
  - Adobe

- **Application Database:**
  - Exploit Database
CVE Consolidation Process

Monitoring Threats and Vulnerabilities

- Discovering Attack surface
- Discovering vulnerabilities on Nestle assets
- Offensive Security
- Orchestration and reporting

**Monitoring Threats and Vulnerabilities**

- CVSS Analysis
- Data Enrichments and Countermeasures
- Company Context Definition
- Rating Consolidation and notification
- Burning Vulnerabilities follow-up

**CVE Consolidation Process**

- Vector
- Exploitation
- Attempts
- Popularity
- Affected Products
- Critical Candidates
- Patch Tracking Ticket
- Critical
- Ad-hoc alert framework
- Burning
- Important
Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

CVE-2024-27905 - Apache Aurora Unspecified Endpoint
CVSS Score: 9.8 (Critical)

CVE-2023-35078: Ivanti Endpoint Manager Mobile (EPMM)
CVSS Score: 9.8 (Critical)

Nestle’ Rating

Burning

Critical

High

Medium

Low
<table>
<thead>
<tr>
<th>Monitoring Threats and Vulnerabilities</th>
<th>Discovering Attack surface</th>
<th>Discovering vulnerabilities on Nestle assets</th>
<th>Offensive Security</th>
<th>Orchestration and reporting</th>
</tr>
</thead>
</table>

**NO SOFTWARE VULNERABILITIES IF YOU DON'T PROVIDE SOFTWARE**
Collecting information on all Nestlé assets combining active and passive discovery scanning solutions with already existing inventories.
**Monitoring Threats and Vulnerabilities**

**Discovering Attack surface**

**Discovering vulnerabilities on Nestle assets**

**Offensive Security**

**Orchestration and reporting**

---

**How standards proliferate:**

(See: A/C chargers, character encodings, instant messaging, etc.)

**Situation:**
There are 14 competing standards.

**Soon:**

14?! Ridiculous! We need to develop one universal standard that covers everyone's use cases.

Yeah!

**Situation:**
There are 15 competing standards.

---

Source: [HTTPS://XKCD.COM](https://xkcd.com)
### Discovering Threats and Vulnerabilities

#### Discovering Attack Surface

#### Discovering vulnerabilities on Nestle assets

<table>
<thead>
<tr>
<th>Status</th>
<th>Hostname</th>
<th>Private IP Addresses</th>
<th>Public IP Addresses</th>
<th>Operating System</th>
<th>Source Icons</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>server101</td>
<td>10.10.10.23</td>
<td>166.166.166.101</td>
<td>Windows Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Server102</td>
<td>10.10.10.24</td>
<td>Read Hat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>workstation101</td>
<td>10.20.10.52</td>
<td>Windows 10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inactive</td>
<td>server103</td>
<td>10.10.10.27</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>258369</td>
<td>10.10.10.70</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Offensive Security

### Orchestration and reporting

### Consolidation identifiers

<table>
<thead>
<tr>
<th>Data integration</th>
<th>UID</th>
<th>Hostname</th>
<th>Serial Number</th>
<th>MAC Addresses</th>
<th>Public DNS Name</th>
<th>Public IP Addresses</th>
<th>Source:</th>
<th>MAC Address:</th>
<th>UID:</th>
<th>Public DNS Name:</th>
<th>Hostname:</th>
<th>Private IP Address:</th>
<th>Serial Number:</th>
<th>Public IP Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source:</td>
<td>13456</td>
<td>server101</td>
<td>0000-0123-7898</td>
<td>12:ab:34:cd:56</td>
<td>server101.neste.com</td>
<td>166.166.166.101</td>
<td>13456</td>
<td>12:ab:34:cd:56</td>
<td>123456</td>
<td>server101.neste.com</td>
<td>server101</td>
<td>10.10.10.23</td>
<td>10.10.10.23</td>
<td>166.166.166.101</td>
</tr>
<tr>
<td>Source:</td>
<td>456789</td>
<td>server101</td>
<td>0000-0123-7898</td>
<td></td>
<td></td>
<td></td>
<td>456789</td>
<td></td>
<td></td>
<td></td>
<td>server101</td>
<td>10.10.10.24</td>
<td>10.20.10.52</td>
<td>166.166.166.101</td>
</tr>
<tr>
<td>Source:</td>
<td>789123</td>
<td>server101</td>
<td>0000-0123-7898</td>
<td>12:ab:34:cd:56</td>
<td>server101.neste.com</td>
<td></td>
<td>789123</td>
<td>12:ab:34:cd:56</td>
<td>789123</td>
<td>server101.neste.com</td>
<td>server101</td>
<td>10.10.10.27</td>
<td>10.10.10.52</td>
<td>166.166.166.101</td>
</tr>
<tr>
<td>Source:</td>
<td>147258</td>
<td>0000-0123-7898</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>147258</td>
<td></td>
<td></td>
<td></td>
<td>0000-0123-7898</td>
<td>10.10.10.70</td>
<td>10.10.10.70</td>
<td>166.166.166.101</td>
</tr>
<tr>
<td>Source:</td>
<td>258369</td>
<td>server101</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>258369</td>
<td></td>
<td></td>
<td></td>
<td>server101</td>
<td>10.10.10.23</td>
<td>10.10.10.23</td>
<td>166.166.166.101</td>
</tr>
</tbody>
</table>
Combining all available solutions to achieve most effective and generally automated vulnerability discovery.

1. Full picture of Vulnerability Exposure
2. Unified view and Nestle Rating across all VM Solutions.
3. Orchestration, ticketing, SLAs and follow-up
4. Dashboards and reporting
Discovering vulnerabilities on Nestle assets
### Security Advisory

#### Windows Servers
- **CVE-0000** (Medium: Windows 2012)
- **CVE-0001** (High: Active MQ)
- **CVE-0003** (Critical: Active MQ)

#### Application 1
- **Assets:** server101, server104
- **Owner:** B Team
- **CPE Subscription:**
  - Active MQ
  - Apache

### Environments

#### Windows Servers
- **Assets:** server101, server102, server103
- **Owner:** A Team
- **CPE Subscription:** Windows 2012
- **SLA:**
  - Critical: L1
  - High: L2
  - Medium: L3
  - Low: L4

#### Application 1
- **Assets:** server101, server104
- **Owner:** B Team
- **CPE Subscription:**
  - Active MQ
  - Apache
- **SLA:**
  - Critical: L1
  - High: L2
  - Medium: L3

### Patch Tracking Tickets

#### Patch Tracking Ticket March 2024 for Windows Servers

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Potential</td>
<td>Windows Servers</td>
<td>A Team</td>
<td>CVE-0000 (Windows 2012)</td>
<td>Medium</td>
<td>L3</td>
</tr>
</tbody>
</table>

#### Patch Tracking Ticket March 2024 for Application 1

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Potential</td>
<td>Application 1</td>
<td>B Team</td>
<td>CVE-0002 (Apache)</td>
<td>High</td>
<td>L2</td>
</tr>
<tr>
<td>Active</td>
<td>Potential</td>
<td>Application 1</td>
<td>B Team</td>
<td>CVE-0003 (Active MQ)</td>
<td>Critical</td>
<td>L1</td>
</tr>
</tbody>
</table>
## Monitoring Threats and Vulnerabilities

### Discovering Attack surface

### Discovering vulnerabilities on Nestle assets

#### Offensive Security

#### Orchestration and reporting

---

**Patch Tracking Tickets**

**Patch Tracking Ticket March 2024 for Windows Servers**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Potential Vulnerability 1</td>
<td>Windows Servers</td>
<td>A Team</td>
<td>CVE-0000 (Windows 2012)</td>
<td>Medium</td>
<td>L3</td>
</tr>
</tbody>
</table>

**Patch Tracking Ticket March 2024 for Application 1**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Potential Vulnerability 2</td>
<td>Application 1</td>
<td>B Team</td>
<td>CVE-0002 (Apache)</td>
<td>High</td>
<td>L2</td>
</tr>
<tr>
<td>Active</td>
<td>Potential Vulnerability 3</td>
<td>Application 1</td>
<td>B Team</td>
<td>CVE-0003 (Active MQ)</td>
<td>Critical</td>
<td>L1</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Vulnerability 1</td>
<td>server101</td>
<td>?</td>
<td>CVE-0000 (Windows 2012)</td>
<td>Medium</td>
<td>?</td>
</tr>
<tr>
<td>Active</td>
<td>Vulnerability 2</td>
<td>server101</td>
<td>?</td>
<td>CVE-0002 (Apache)</td>
<td>High</td>
<td>?</td>
</tr>
<tr>
<td>Active</td>
<td>Vulnerability 3</td>
<td>server101</td>
<td>?</td>
<td>CVE-0003 (Active MQ)</td>
<td>Critical</td>
<td>?</td>
</tr>
<tr>
<td>Active</td>
<td>Vulnerability 4</td>
<td>server101</td>
<td>?</td>
<td>CVE-0004 (Nginx)</td>
<td>High</td>
<td>?</td>
</tr>
</tbody>
</table>
### Discovering vulnerabilities on Nestle assets

#### Patch Tracking Tickets

**Patch Tracking Ticket March 2024 for Windows Servers**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Potential Vulnerability 1</td>
<td>Windows Servers</td>
<td>A Team</td>
<td>CVE-0000 (Windows 2012)</td>
<td>Medium</td>
<td>L3</td>
</tr>
<tr>
<td>Active</td>
<td>Vulnerability 1</td>
<td>server101</td>
<td>?</td>
<td>CVE-0000 (Windows 2012)</td>
<td>Medium</td>
<td>?</td>
</tr>
</tbody>
</table>

**Patch Tracking Ticket March 2024 for Application 1**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Potential Vulnerability 2</td>
<td>Application 1</td>
<td>B Team</td>
<td>CVE-0002 (Apache)</td>
<td>High</td>
<td>L2</td>
</tr>
<tr>
<td>Active</td>
<td>Vulnerability 2</td>
<td>Server101</td>
<td>?</td>
<td>CVE-0002 (Apache)</td>
<td>High</td>
<td>?</td>
</tr>
<tr>
<td>Active</td>
<td>Potential Vulnerability 3</td>
<td>Application 1</td>
<td>B Team</td>
<td>CVE-0003 (Active MQ)</td>
<td>Critical</td>
<td>L1</td>
</tr>
<tr>
<td>Active</td>
<td>Vulnerability 3</td>
<td>Server101</td>
<td>?</td>
<td>CVE-0003 (Active MQ)</td>
<td>Critical</td>
<td>?</td>
</tr>
</tbody>
</table>

**Scanner Finding Ticket March 2024**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Target</th>
<th>Owner</th>
<th>CVE (Affects)</th>
<th>Rating</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Vulnerability 4</td>
<td>Server101</td>
<td>? Fallback</td>
<td>CVE-0004 (Nginx)</td>
<td>High</td>
<td>Default</td>
</tr>
</tbody>
</table>
Combining Various types of offensive security exercises in order to evaluate real security of environments.

- Penetration Testing
- Red Teaming
  - Bug Bounty
  - Vulnerability Disclosure

1. As in the real world the attackers are not stopped in the surface. The offensive security tests provide realistic assessment and deeper impact understanding than standard scanning or reviews.

2. The exercise will show how an attacker would try to access the systems, perform lateral movement and finally try to abuse the gained access to perform a fraud or other malicious activities.

3. During a penetration test, security controls in place are also verified, which allows to focus the efforts on the most important points.

4. Each assessment provides a comprehensive description of the vulnerabilities and a defined remediation plan with mitigation actions.
Discovering Attack surface

Monitoring Threats and Vulnerabilities

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

Transforming and combining of large amount of data into meaningful and actionable tickets or dashboards is a key to success in Vulnerability management.

1. Single graph database based Vulnerability Orchestration Platform containing all data from previously mentioned Vulnerability Management products and related activities.

2. Security asset inventory combining information from various official and non-official sources, scan results and discovered security vulnerabilities.

3. Automatic ticketing with ability to setup and precisely track resolution and SLOs. Automatic emailing or integration with other Nestlé ITSM or DevOps Tools (ServiceNow, Azure DevOps, Jira)

4. Interactive custom-built dashboards with live data drilldowns and precise access controls. Powerful search across all data.

5. API allowing integration with other tools, processes or automated workflows
✓ Centralized vulnerability and asset information
✓ Timely assessment of new vulnerabilities and continuous threat monitoring
✓ Process aligned with patching calendars
✓ Support for complex ownership structure and SLAs
✓ Flexible reporting for Risk and Compliance
✓ Evaluation of compensation and detection measures
✓ Different models for easier coverage extension
Q&A

Thank you for your time and attention today!