VULNERABILITY MANAGEMENT

Martin Karel

Global Vulnerability Management and Offensive Security Lead

Jenifer Jiménez

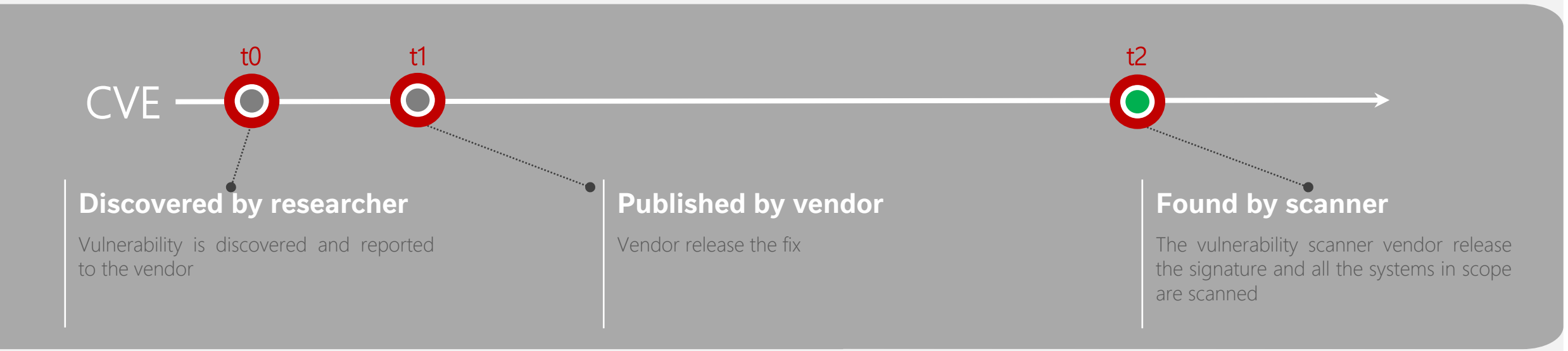
Vulnerability Management Platform Architect

Angelo Punturiero

Vulnerability Management Senior Specialist

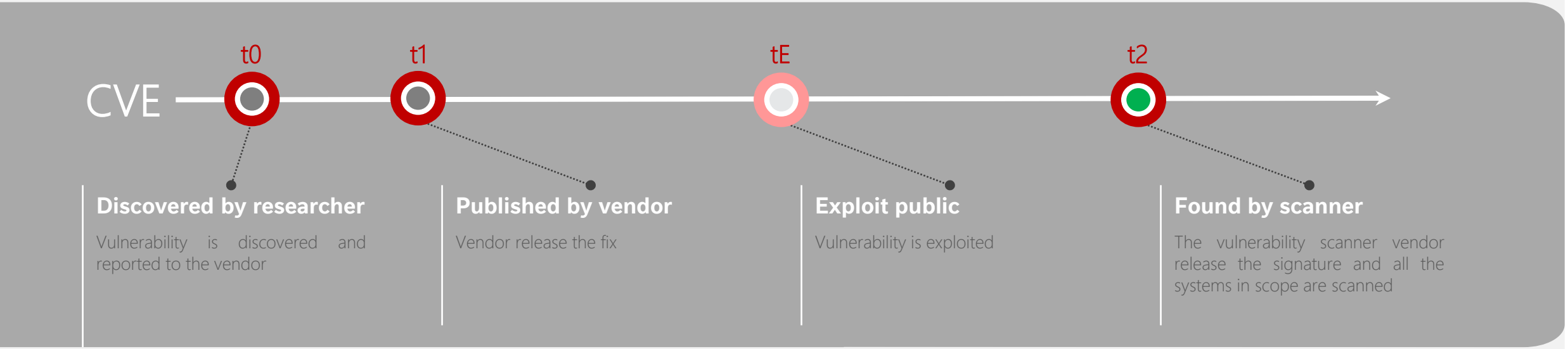
CYBER SECURITY OPERATIONS CENTER

CVE Timeline



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



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

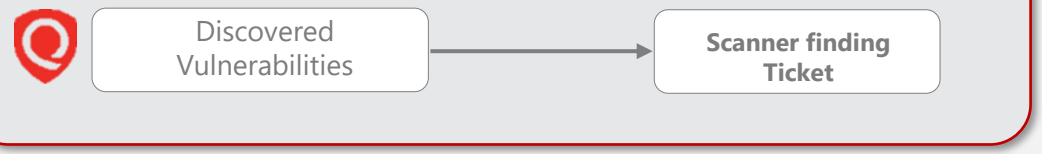
Only 30% coverage

In average only about 30% of Critical and High vulnerabilities have a scanning signature

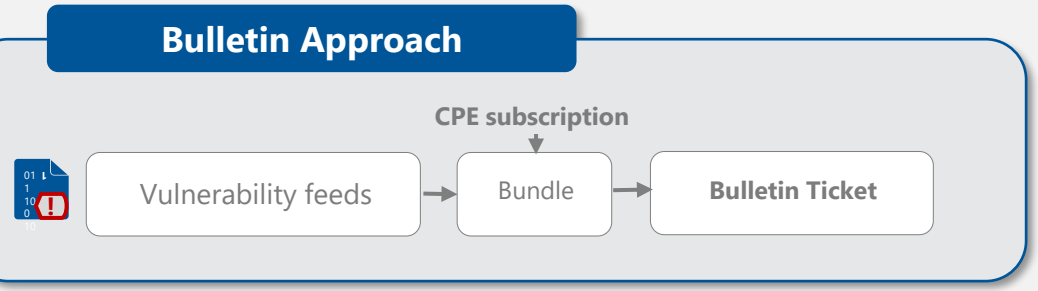
Statistics are calculated based on data from the past 3 years.

VM Approach Options

Scanning approach



Bulletin Approach



Pros / Cons

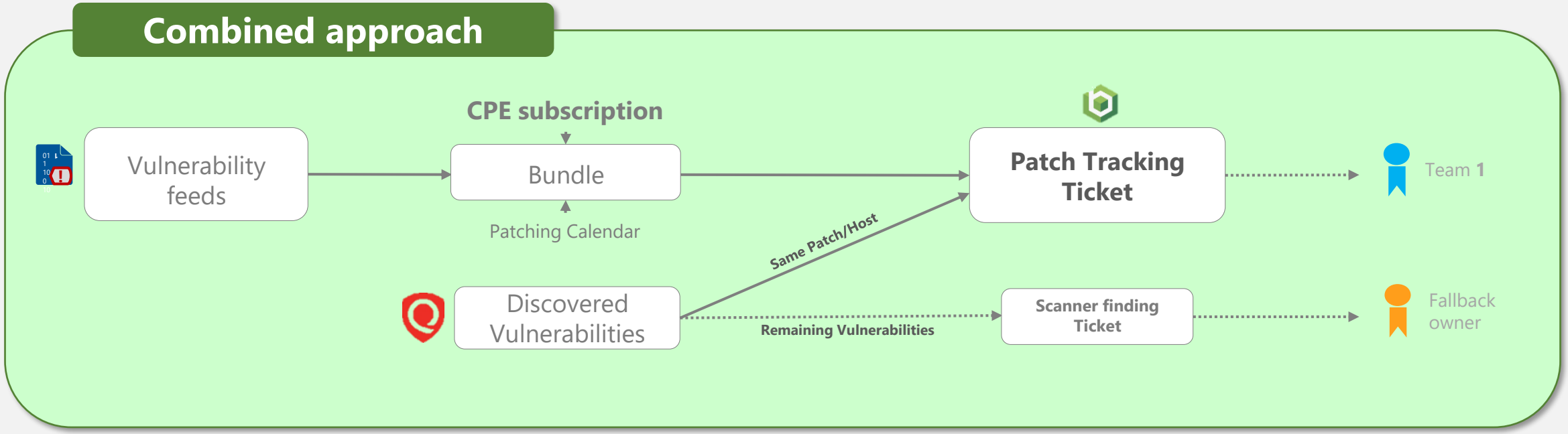
Scanning approach

- \+ Exact vulnerability and risk exposure tracking
- \+ Assurance of the resolution
- \- Delay between patch release and scan finding
- \- Costly and time consuming
- \- Scanner technology coverage
- \- Large number of vulnerabilities
- \- Frequent ownership problems

Bulletin Approach

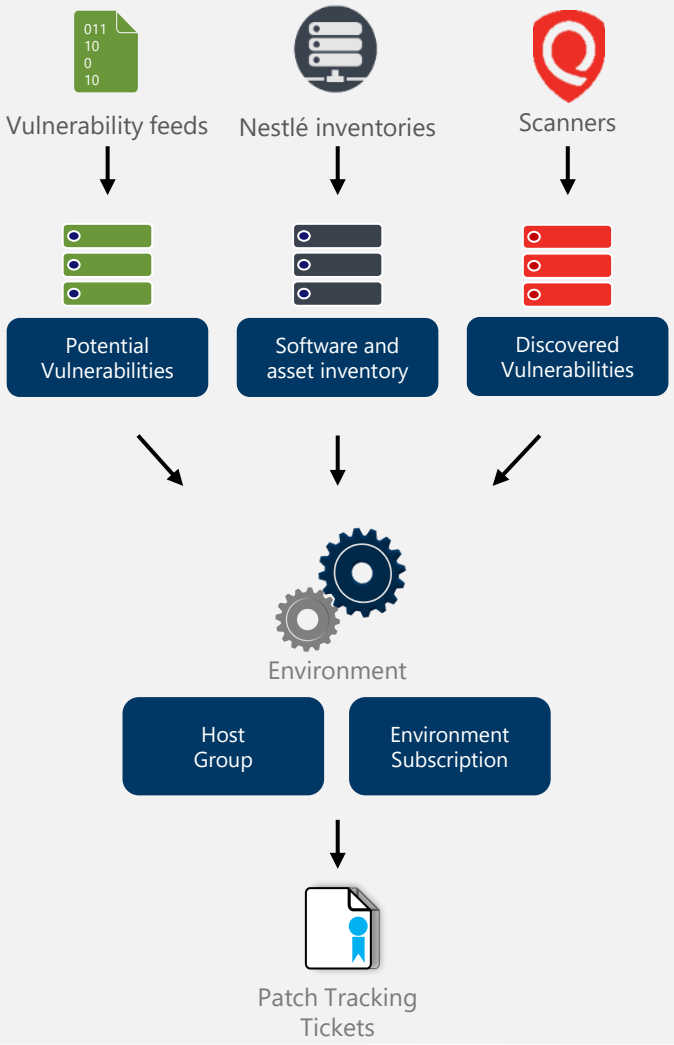
- \+ Prompt availability of the assessment
- \+ Can be better aligned with Patch process
- \+ Easy to setup
- \- Only theoretical alerts
- \- No exact tracking of affected systems

Combined process



- 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

Patch Tracking Ticket



Feed Based CVEs

Platform	Nestle Rating	Vuln #	Max CVSS3	Exploited
Office	HIGH	5	7.8	NO
Windows Server 2008	HIGH	41	8.8	NO
Windows Server 2012	HIGH	49	8.8	NO

Host Groups

Search

Name

Nespresso PCI Windows Servers

Vulnerability Scanning

Confirmed Vulnerability Count	Confirmed Patched Vulnerability Count	Solved %
1041	496	47.64649376

Detected Vulnerabilities

Search

Status	Title	Hostname	IP	CVSS	Severity	Risk Rating	First Found	Last Found
ACTIVE	Microsoft Office and Microsoft Office Services and Web Apps Security Update June 2020			9.3	HIGH	HIGH	06-10-2020	06-25-2020
ACTIVE	Microsoft Windows Adobe Flash Player Security Update for June 2020 (ADV200010)			10	HIGH	HIGH	06-10-2020	06-25-2020
FIXED	Microsoft Windows Adobe Flash Player Security Update for June 2020 (ADV200010)			10	HIGH	HIGH	06-21-2020	06-28-2020
ACTIVE	Microsoft Internet Explorer Security Update for June 2020			7.6	HIGH	HIGH	06-10-2020	07-12-2020
ACTIVE	Microsoft Windows Adobe Flash Player Security Update for June 2020 (ADV200010)			10	HIGH	HIGH	06-10-2020	06-25-2020
FIXED	Microsoft Office and Microsoft Office Services and Web Apps Security Update June 2020			9.3	HIGH	HIGH	06-10-2020	06-24-2020
ACTIVE	Microsoft Office and Microsoft Office Services and Web Apps Security Update June 2020			9.3	HIGH	HIGH	06-10-2020	06-25-2020
ACTIVE	Microsoft Office and Microsoft Office Services and Web Apps Security Update June 2020			9.3	HIGH	HIGH	06-10-2020	06-25-2020
ACTIVE	Microsoft Office and Microsoft Office Services and Web Apps Security Update June 2020			9.3	HIGH	HIGH	06-10-2020	06-25-2020
FIXED	Microsoft Windows Adobe Flash Player Security Update for June 2020 (ADV200010)			10	HIGH	HIGH	06-14-2020	06-28-2020

Showing 1 to 10 of 1,041 records

|← ← 1 2 3 → →|

Scanner Findings

Information Technology

Vulnerability Management Tasks

Monitoring Threats and Vulnerabilities

Discovering Attack surface

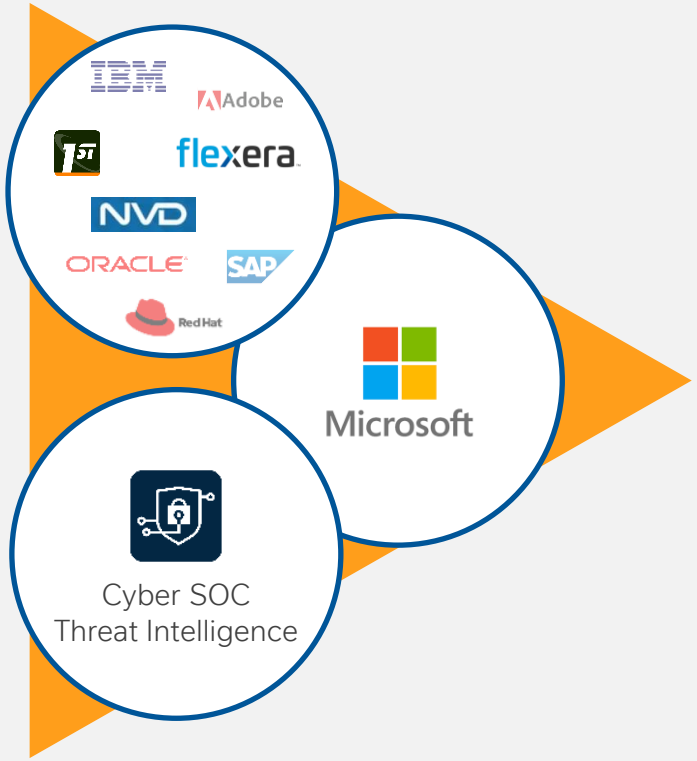
Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

Monitoring Threats and Vulnerabilities

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



Centralized Vulnerability Database

Vendor Advisories Bulletins

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.

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

CVE Investigation & Enrichments

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

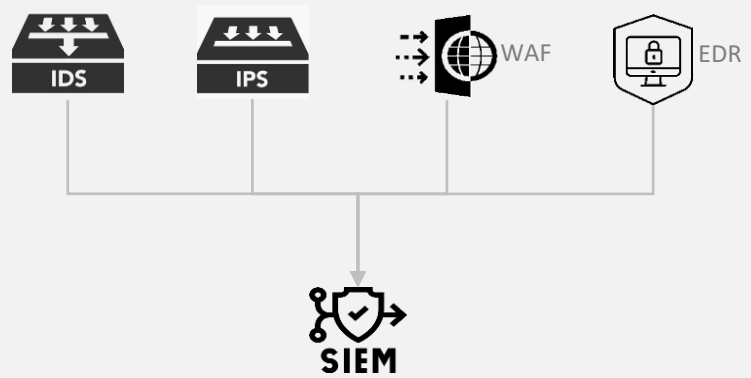
CVSS Details

	Local	Remote	**Wormable**	**Disclosed**	**Exploited**	**Popular**
Attack Vector	L|P	N|A	N			
Privileges Required	N|L|H	N|L|H	N			
User Interaction	N|R	N|R	N			
Integrity	L|H	L|H	L|H			
Automatable (v4.0)			YES			
Exploit Code Maturity				P	F|H	
Exploit Maturity (v4.0)				P	A	

Enrichments

CSOC Warns	+	+	+
Soure Feed	+	+	+
References	+	+	+
Countermeasures		+	+
CISA Known			+

Countermeasures



Information Technology

CVE Investigation & Enrichments

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

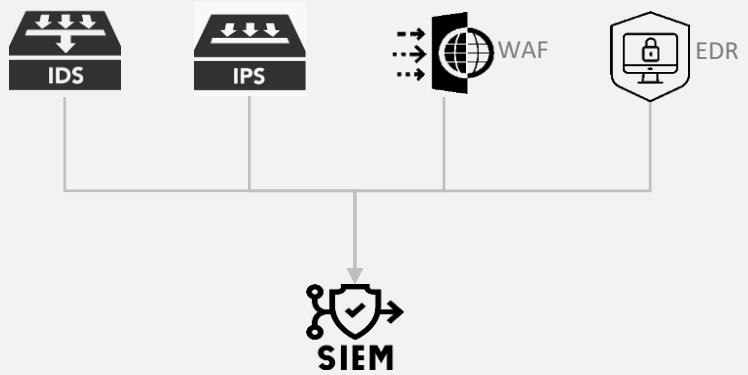
Offensive Security

Orchestration and reporting

CVSS Details

	Local	Remote	**Wormable**	**Disclosed**	**Exploited**	**Popular**
Attack Vector	L|P	N|A	N			
Privileges Required	N|L|H	N|L|H	N			
User Interaction	N|R	N|R	N			
Integrity	L|H	L|H	L|H			
Automatable (v4.0)			YES			
Exploit Code Maturity				P	F|H	
Exploit Maturity (v4.0)				P	A	

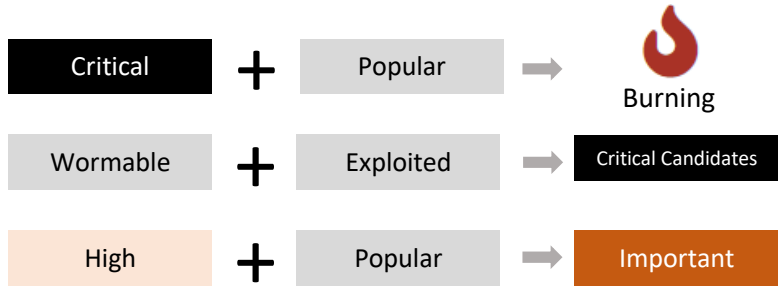
Countermeasures



Enrichments

CSOC Warns	+	+	+
Soure Feed	+	+	+
References	+	+	+
Countermeasures		+	+
CISA Known			+

Settings



Information Technology

CVE Investigation & Enrichments

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

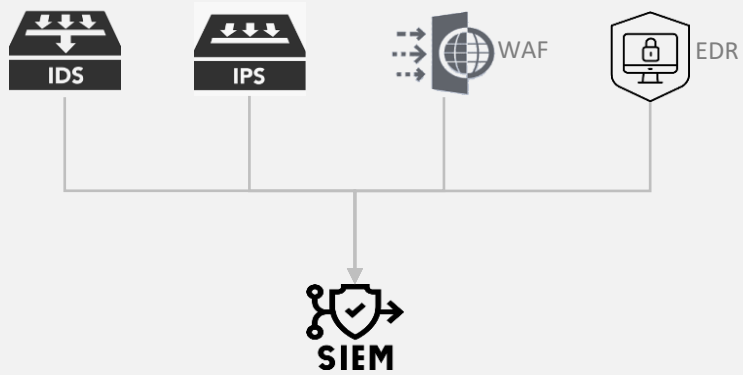
CVSS Details

	Local	Remote	Wormable	Disclosed	Exploited	Popular
Attack Vector	L|P	N|A	N			
Privileges Required	N|L|H	N|L|H	N			
User Interaction	N|R	N|R	N			
Integrity	L|H	L|H	L|H			
Automatable (v4.0)			YES			
Exploit Code Maturity				P	F|H	
Exploit Maturity (v4.0)				P	A	

Enrichments

CSOC Warns	+	+	+
Soure Feed	+	+	+
References	+	+	+
Countermeasures		+	+
CISA Known			+

Countermeasures



NVD
flexera
GitHub
PASTEBIN
Microsoft
SAP
Red Hat
ORACLE
Adobe
Cyber SOC Threat Intelligence
EXPLOIT DATABASE

CVE Consolidation Process

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

Vector

Exploitation

Attempts

Popularity

Affected Products

Critical Candidates

Patch Tracking Ticket

Critical

High

Ad-hoc alert framework

Burning

Important

Information Technology

All-at-once

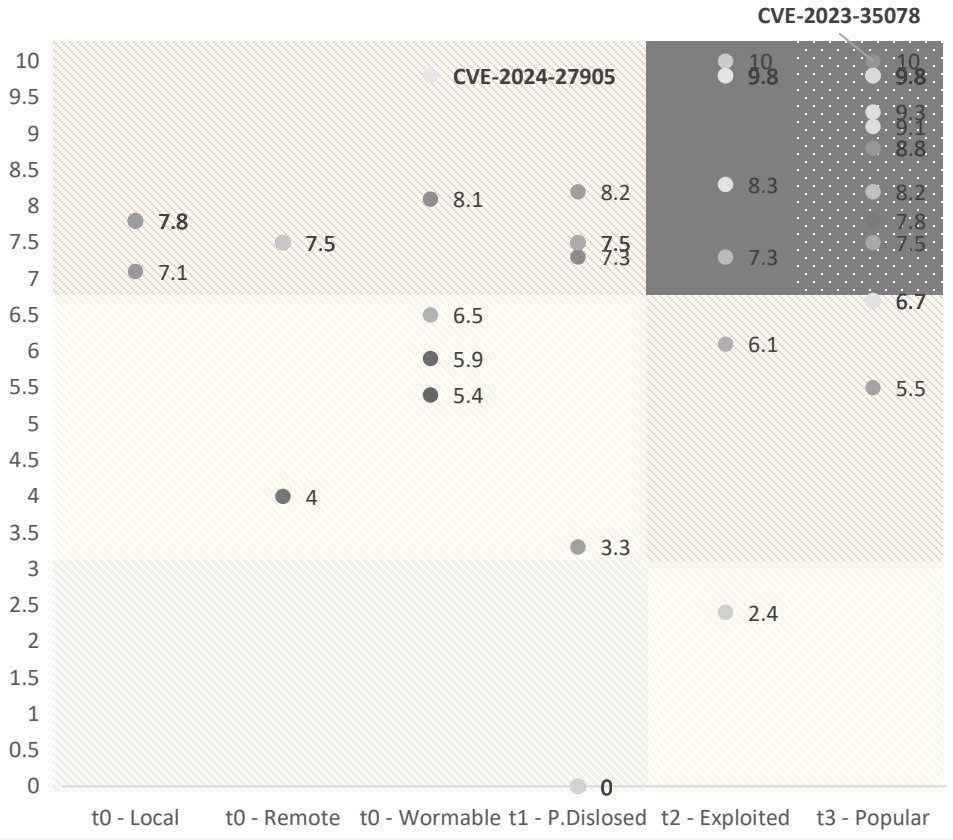
Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

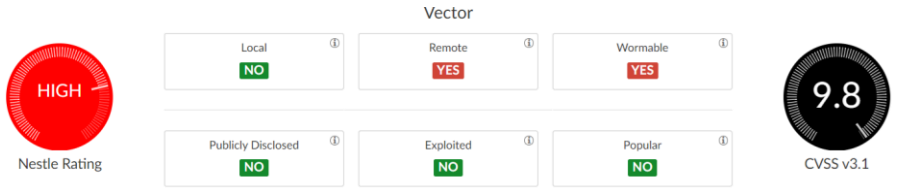
Orchestration and reporting



CVE-2024-27905 - Apache Aurora Unspecified Endpoint

CVSS Score: 9.8 (**Critical**)

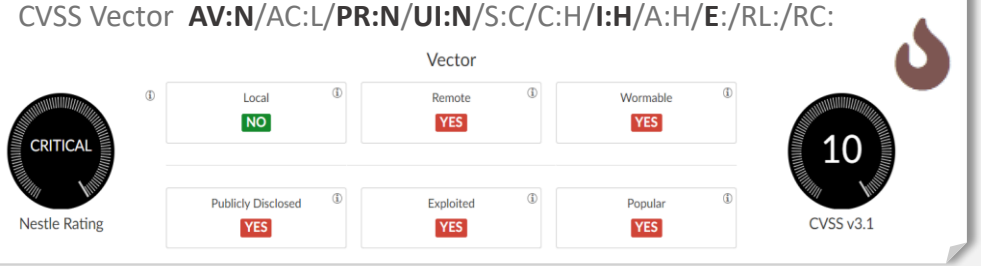
CVSS Vector: **AV**:N/AC:L/**PR**:N/**UI**:N/S:U/C:H/**I**:H/A:H/E:/RL:/RC:



CVE-2023-35078:Ivanti Endpoint Manager Mobile (EPMM)

CVSS Score : 10 (**Critical**)

CVSS Vector **AV:N**/AC:L/**PR:N**/**UI:N**/S:C/C:H/**I:H**/A:H/**E**:/RL:/RC:



Nestle' Rating Burning Critical High Medium Low

Information Technology

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

Collecting information on all Nestlé assets combining active and passive discovery scanning solutions with already existing inventories.

Active scanning

Internal and external networks

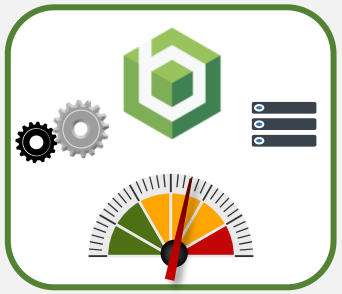
External Attack Surface

Cloud Workload Protection

IoT and Facilities

OT Environments

Passive discovery



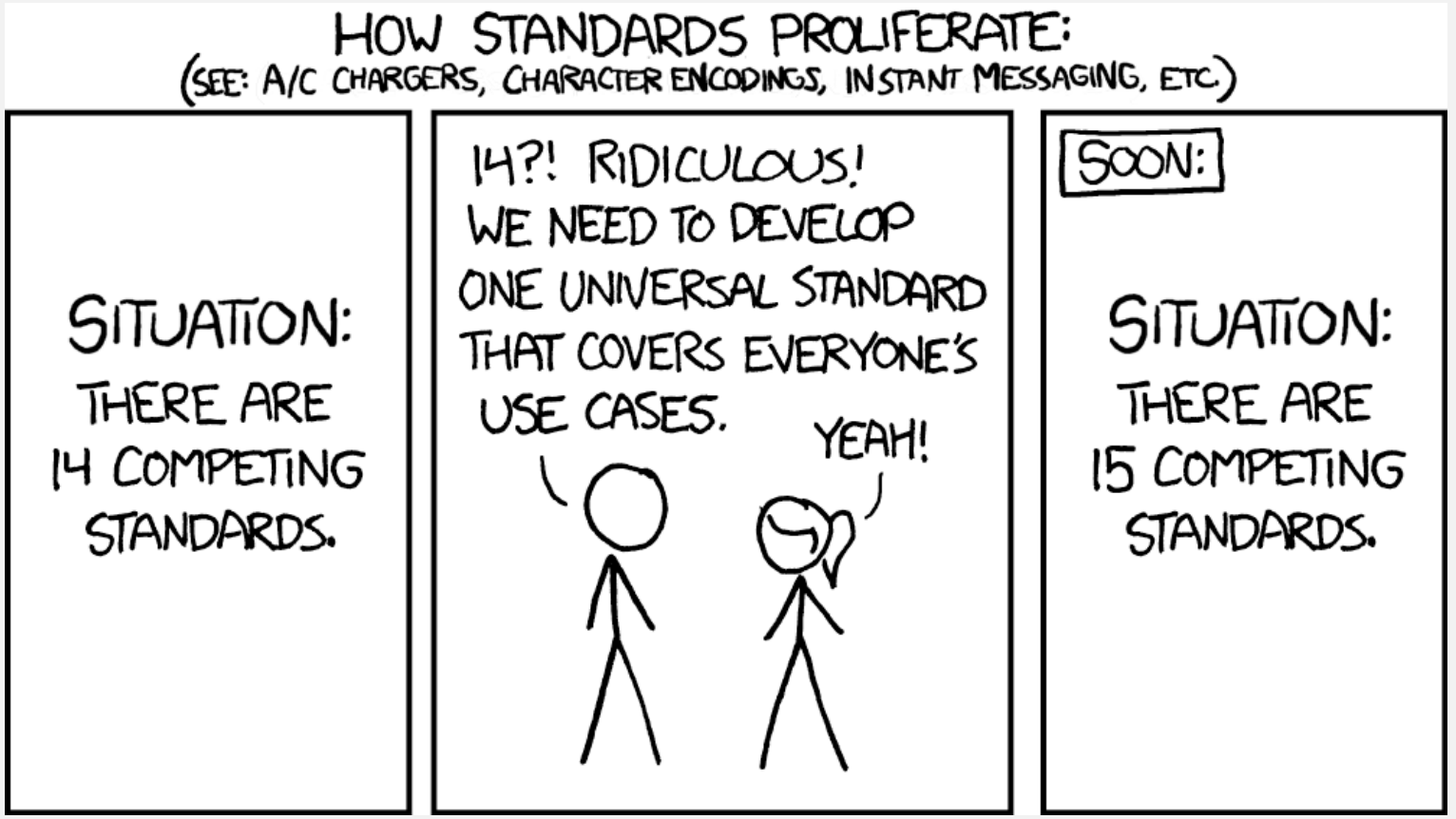
Unified Asset Security Inventory

Software Inventory

ServiceNow, MS SCCM, WCM, LDAP, ArcSight, DigiPI, SCI Inventories, SNTC, Splunk, MEN&MICE, MS Intune, PRISMA, Azure, AWS, GCP, Defender

Host / Network / SW Inventories

Information Technology



Source: HTTPS://XKCD.COM

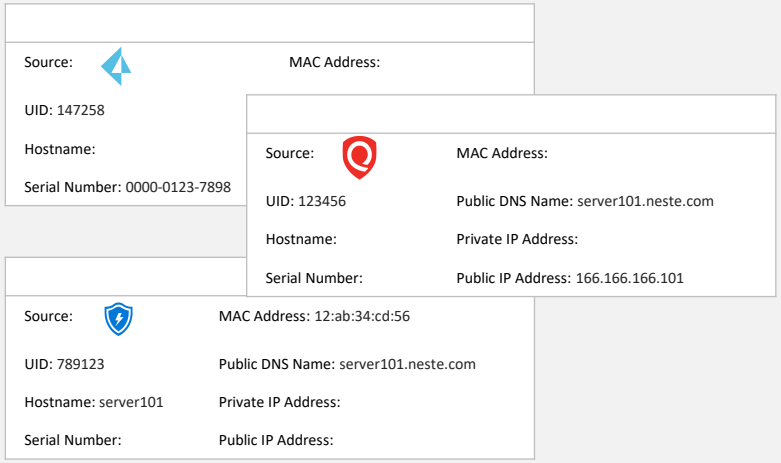
Monitoring Threats and Vulnerabilities

Discovering Attack surface

Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting



Status	Hostname	Private IP Addresses	Public IP Addresses	Operating System	Source Icons	Type
Active	server101	10.10.10.23	166.166.166.101	Windows Server		
Active	Server102	10.10.10.24		Read Hat		
Active	workstation101	10.20.10.52		Windows 10		
Inactive	server103	10.10.10.27				
Active	258369	10.10.10.70				

Consolidation identifiers

Data integration	UID	Hostname	Serial Number	MAC Addresses	Public DNS Name	Public IP Addresses
	123456				server101.neste.com	166.166.166.101
	456789	server101	0000-0123-7898			
	789123	server101		12:ab:34:cd:56	server101.neste.com	
	147258		0000-0123-7898			
	258369	server101				

Information Technology

Monitoring Threats and Vulnerabilities | Discovering Attack surface | **Discovering vulnerabilities on Nestle assets** | Offensive Security | Orchestration and reporting

Custom Application Code
SEC DevOps

Third party plugins | CMS | App

OS | APP Server | Scripting env.

Hypervisor/Container/HW Server

IOT Device / NW Device

OT Device (Factories)

Offensive Security

Bug Bounty
Vulnerability Disclosure

Application scan

Authenticated scan
VM Agent
Compliance scan

Container Security

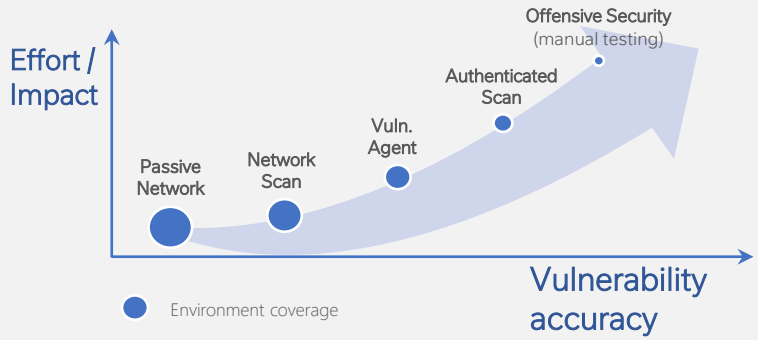
Passive SW Inventory

External Attack surface

Passive Network

Combining all available solutions to achieve most effective and generally **automated vulnerability discovery**.

Combined Vulnerabilities & Findings



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

Information Technology

Monitoring Threats and Vulnerabilities

Discovering Attack surface

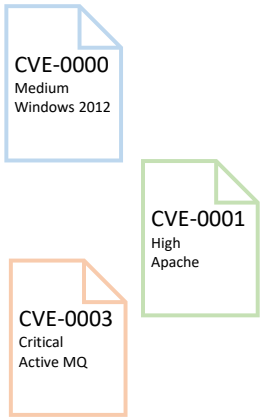
Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

Monitoring Threats and Vulnerabilities | Discovering Attack surface | **Discovering vulnerabilities on Nestle assets** | Offensive Security | Orchestration and reporting

Security Advisory



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
- Low: L3

Patch Tracking Tickets

Patch Tracking Ticket March 2024 for Windows Servers

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Potential Vulnerability 1	Windows Servers	A Team	CVE-0000 (Windows 2012)	Medium	L3

Patch Tracking Ticket March 2024 for Application 1

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Potential Vulnerability 2	Application 1	B Team	CVE-0002 (Apache)	High	L2
● Active	Potential Vulnerability 3	Application 1	B Team	CVE-0003 (Active MQ)	Critical	L1

Monitoring Threats and Vulnerabilities | Discovering Attack surface | **Discovering vulnerabilities on Nestle assets** | Offensive Security | Orchestration and reporting

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Vulnerability 1	server101	?	CVE-0000 (Windows 2012)	Medium	?
● Active	Vulnerability 2	server101	?	CVE-0002 (Apache)	High	?
● Active	Vulnerability 3	server101	?	CVE-0003 (Active MQ)	Critical	?
● Active	Vulnerability 4	server101	?	CVE-0004 (Nginx)	High	?

Patch Tracking Tickets

Patch Tracking Ticket March 2024 for Windows Servers

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Potential Vulnerability 1	Windows Servers	A Team	CVE-0000 (Windows 2012)	Medium	L3

Patch Tracking Ticket March 2024 for Application 1

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Potential Vulnerability 2	Application 1	B Team	CVE-0002 (Apache)	High	L2
● Active	Potential Vulnerability 3	Application 1	B Team	CVE-0003 (Active MQ)	Critical	L1

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

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Potential Vulnerability 1	Windows Servers	A Team	CVE-0000 (Windows 2012)	Medium	L3
● Active	Vulnerability 1	server101	? → A Team	CVE-0000 (Windows 2012)	Medium	? → L3

Patch Tracking Ticket March 2024 for Application 1

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Potential Vulnerability 2	Application 1	B Team	CVE-0002 (Apache)	High	L2
● Active	Vulnerability 2	Server101	? → B Team	CVE-0002 (Apache)	High	? → L2
● Active	Potential Vulnerability 3	Application 1	B Team	CVE-0003 (Active MQ)	Critical	L1
● Active	Vulnerability 3	Server101	? → B Team	CVE-0003 (Active MQ)	Critical	? → L1

Scanner Finding Ticket March 2024

Status	Description	Target	Owner	CVE (Affects)	Rating	SLA
● Active	Vulnerability 4	Server101	? → Fallaback	CVE-0004 (Nginx)	High	? → Default

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

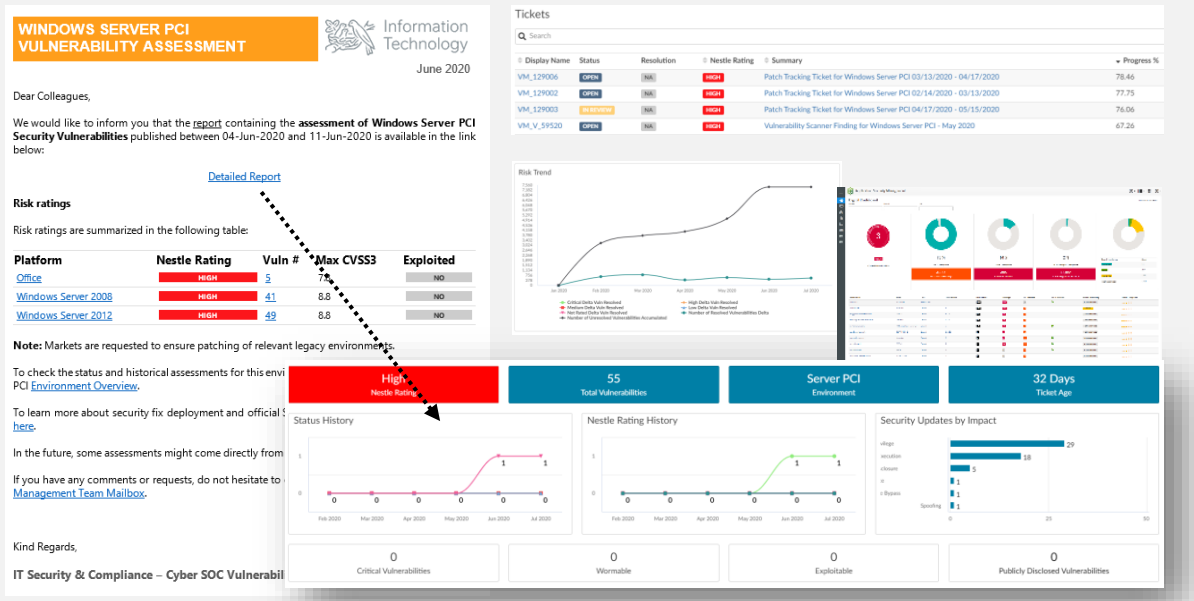
Discovering vulnerabilities on Nestle assets

Offensive Security

Orchestration and reporting

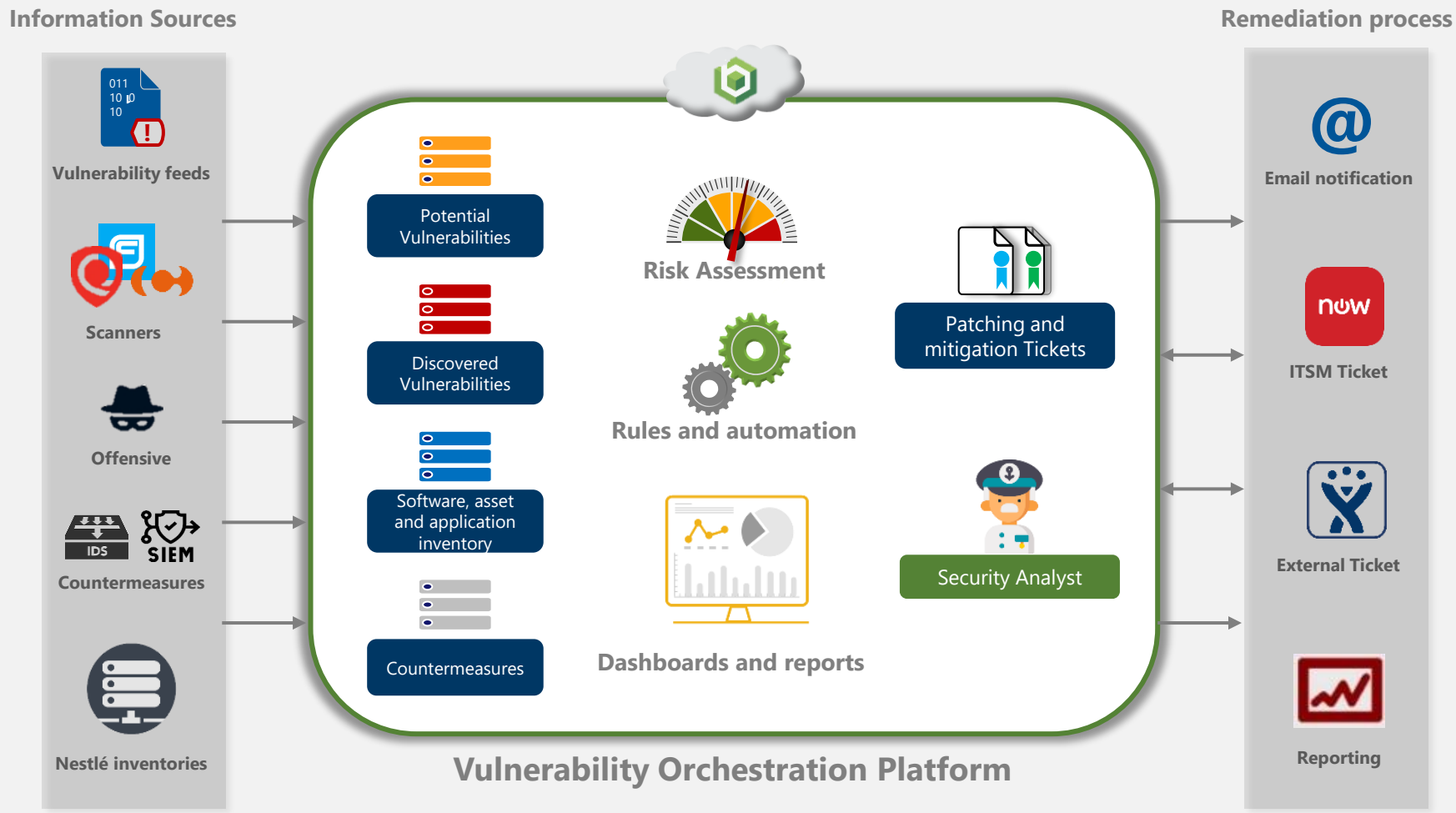
1. Single graph database based Vulnerability Orchestration Platform containing all data from previously mentioned Vulnerability Management products and related activities.
2. Security asset inventory combining information from various official and non-official sources, scan results and discovered security 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

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



Information Technology

Vulnerability Orchestration Platform



Information Technology

- ✓ 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

CYBER SECURITY OPERATIONS CENTER

Q&A

Thank you for your time and attention today!

CYBER SECURITY OPERATIONS CENTER