Passare dalla "scansione" alla "gestione" delle vulnerabilità

Igor Falcomatà | Consulente Cyber Security, *Greenbone AG*
Dirk Boeing | Security Engineer, *Greenbone AG*

Igor Falcomatà

Consulente Cyber Security, Greenbone AG

- **Attività professionale:**
  - **analisi delle vulnerabilità**
  - **simulazioni di attacco**
  - **consulenza**
  - **formazione**
- **Altro:**
  - **fondatore sikurezza.org**
  - **attivo in vari Linux User Group**
  - **ISACA Venice**

Dirk Boeing

Security Engineer, Greenbone AG

- **Esperto tedesco di sicurezza informatica con oltre 25 anni di esperienza.**
- **Specializzato in sicurezza delle reti, strategie di cybersecurity e sviluppo del mercato internazionale.**
- **Con Greenbone, impegnato nella promozione di soluzioni di cybersecurity sostenibili a livello globale.**

Agenda

In questa sessione vedremo come implementare una strategia efficace di Vulnerability Management, passando da un approccio una tantum o occasionale alla gestione continuativa delle vulnerabilità.

Analizzeremo come trasformare un mero requisito di compliance in un vero e proprio strumento per potenziare la resilienza e la cybersecurity aziendale.

Esploreremo i fattori critici per condurre scansioni efficaci e complete su infrastrutture complesse ed eterogenee e capiremo come prioritizzare le vulnerabilità più critiche per ottimizzare le strategie di remediation.

www.porcupine.org/satan/admin-guide-to-cracking.html 133%

Improving the Security of Your Site by Breaking Into it

1993

Dan Farmer
Sun Microsystems
zen@sun.com

Wietse Venema
Eindhoven University of Technology
wietse@porcupine.org

Introduction

Every day, all over the world, computer networks and hosts are being broken into. The level of sophistication of these attacks varies widely; while it is generally believed that most break-ins succeed due to weak passwords, there are still a large number of intrusions that use more advanced techniques to break in. Less is known about the latter types of break-ins, because by their very nature they are much harder to detect.

CERT. SRI. The Nic. NCSC. RSA. NASA. MIT. Uunet. Berkeley. Purdue. Sun. You name it, we've seen it broken into. Anything that is on the Internet (and many that isn't) seems to be fairly easy game. Are these targets unusual? What happened?

Fade to...

A young boy, with greasy blonde hair, sitting in a dark room. The room is illuminated only by the luminescense of the C64's 40 character screen. Taking another long drag from his Benson and Hedges cigarette, the weary system cracker telnets to the next faceless ".mil" site on his hit list. "guest -- guest", "root -- root", and "system -- manager" all fail. No matter. He has all night... he pencils the host off of his list, and tiredly types in the next potential victim...

http://www.porcupine.org/satan/admin-guide-to-cracking.html

www.porcupine.org/satan/

SATAN

(Security Administrator Tool for Analyzing Networks)

1995

SATAN Information

- What SATAN is about
- SATAN updates
- Bulletins from vendors etc.
- A SATAN demo with all documentation
- What you need in order to run SATAN
- Downloading your own SATAN copy

SATAN Hints and tips

- Workaround for Netscape
- Hints and tips for LINUX users

http://www.porcupine.org/satan/

Cos'è il Vulnerability Scanning?

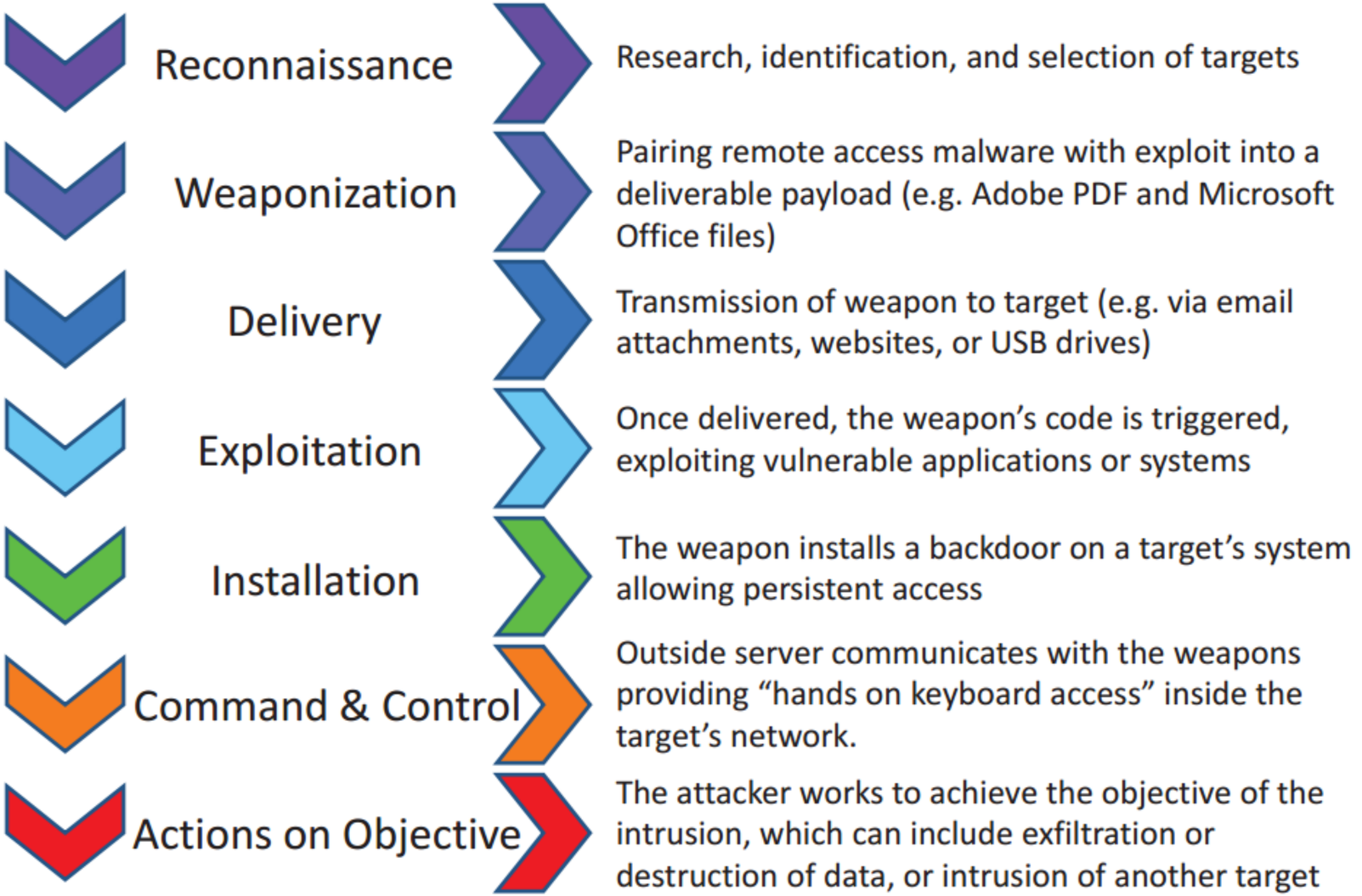
Il **Vulnerability Scanning** è un processo automatizzato di identificazione delle vulnerabilità di sicurezza in un sistema, rete o applicazione. Si avvale di strumenti specifici (scanner di vulnerabilità) per analizzare configurazioni, software e servizi alla ricerca di debolezze note che potrebbero essere sfruttate da attaccanti.

Caratteristiche del Vulnerability Scanning:

- **Automazione**: utilizza software dedicati per eseguire scansioni su larga scala.
- **Identificazione delle vulnerabilità note**: confronta il sistema con database di vulnerabilità (es. CVE, NVD).
- **Non intrusivo (o poco intrusivo)**: a differenza del penetration test, non sfrutta attivamente le vulnerabilità ma le rileva.
- **Rapporto sui rischi**: fornisce una valutazione del rischio associato a ogni vulnerabilità rilevata.

https://chatgpt.com/

Phases of the Intrusion Kill Chain



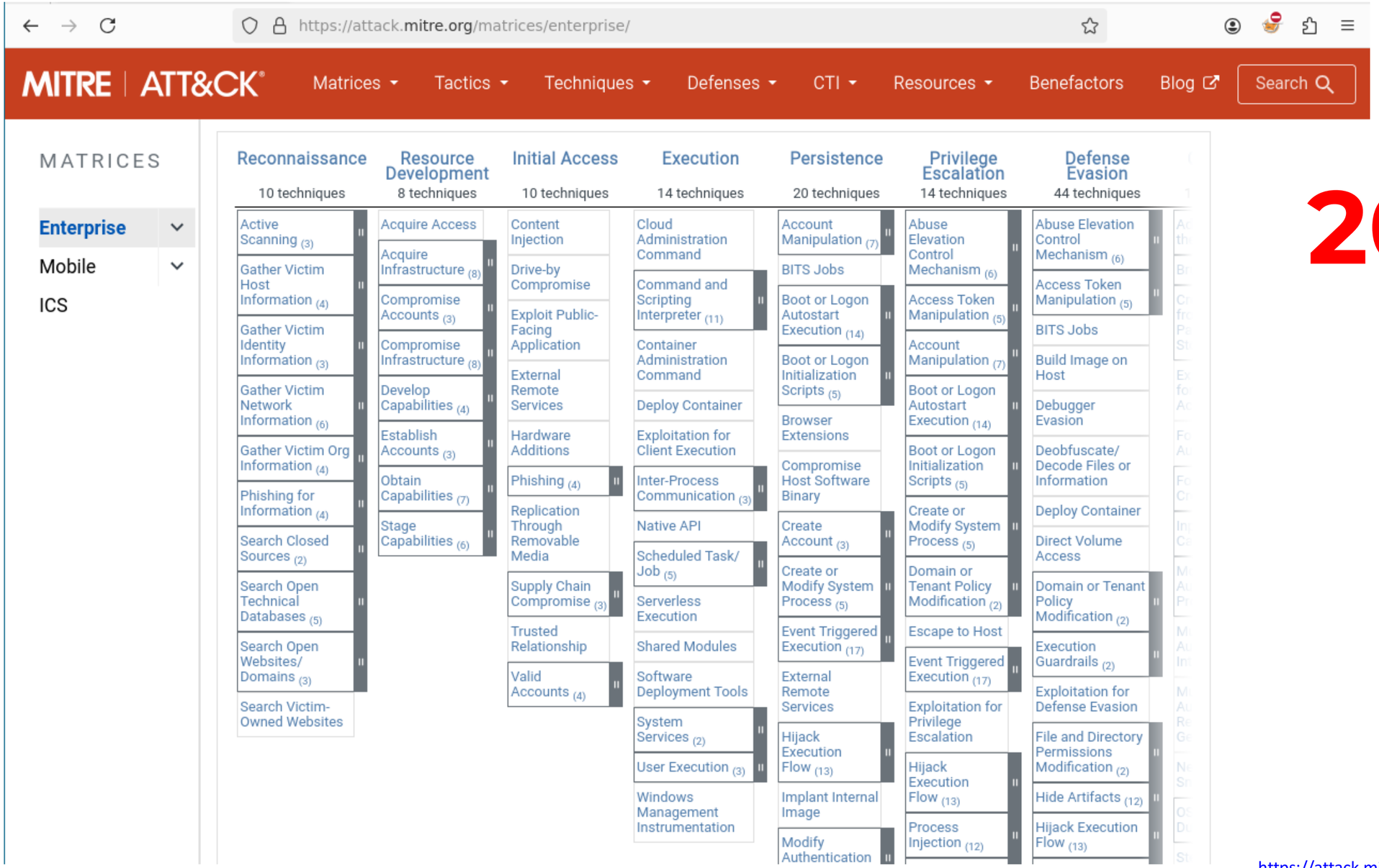
2011

https://en.wikipedia.org/wiki/Cyber_kill_chain

Phases of the Intrusion Kill Chain

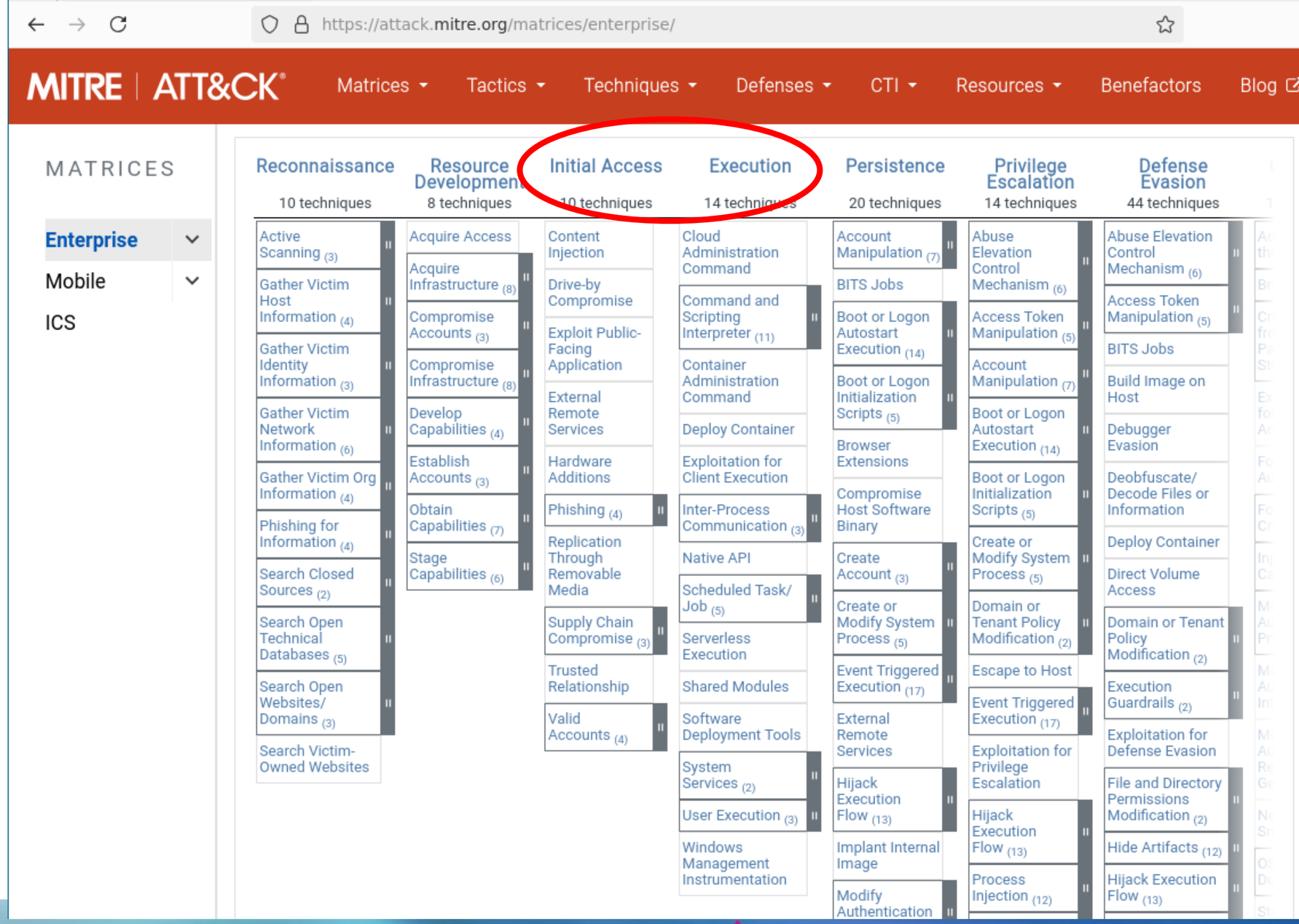
2011

https://en.wikipedia.org/wiki/Cyber_kill_chain



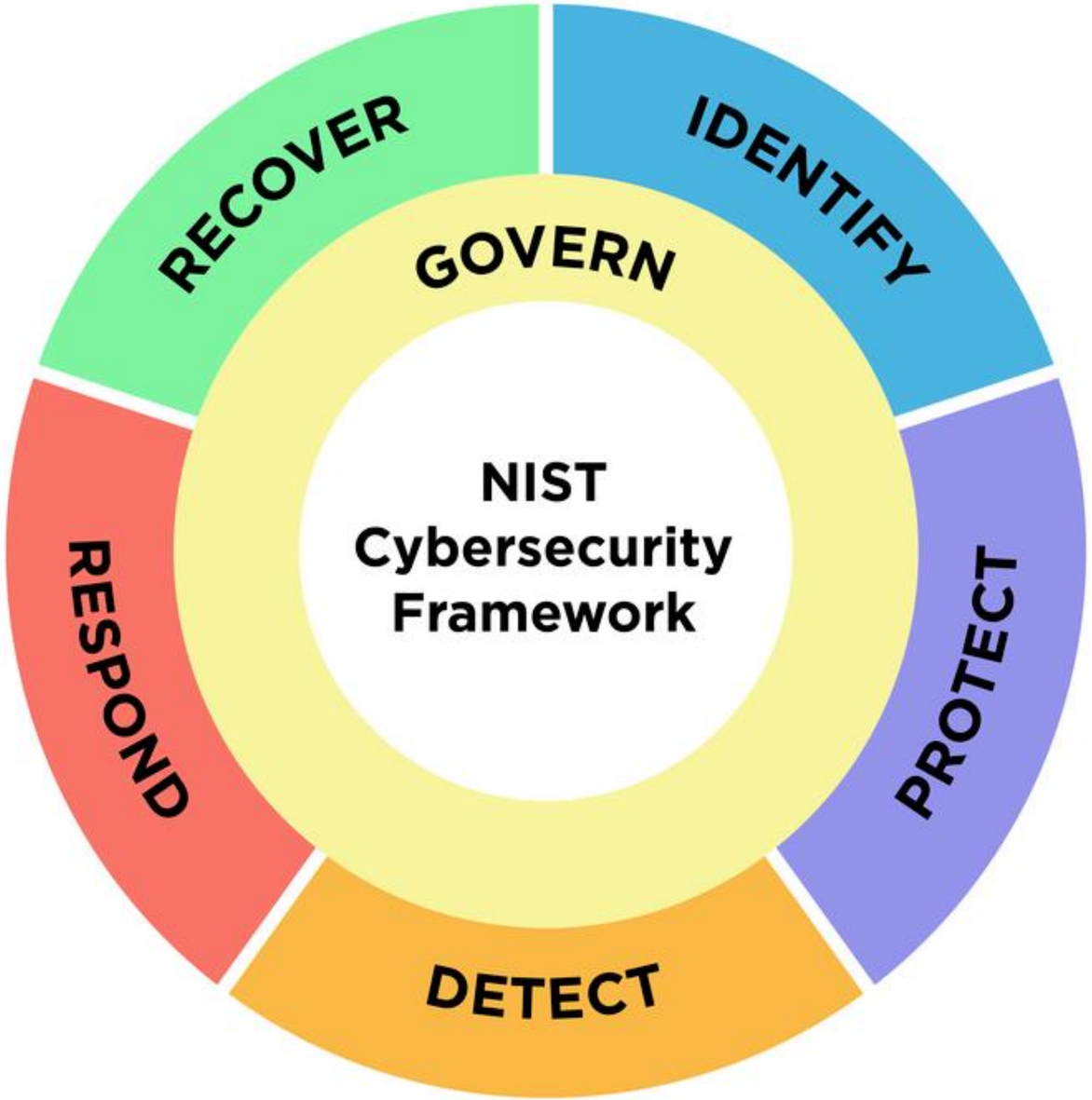
2013

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



2013

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



2014

https://www.nist.gov/cyberframework

2014

https://www.nist.gov/cyberframework

Vulnerability Scanning per:

- identificare (tutte) le vulnerabilità (note)
- senza causare impatti sull'infrastruttura
- prima che lo facciano i malintenzionati
- definire un livello di rischio (standard)

E dopo?

- prioritizzare le vulnerabilità
- risolvere le problematiche
- verificare la corretta risoluzione
- goto 1

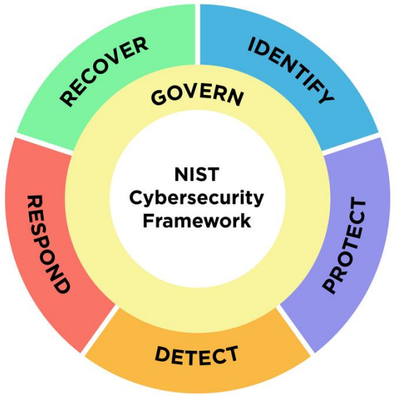
Vulnerability Management?

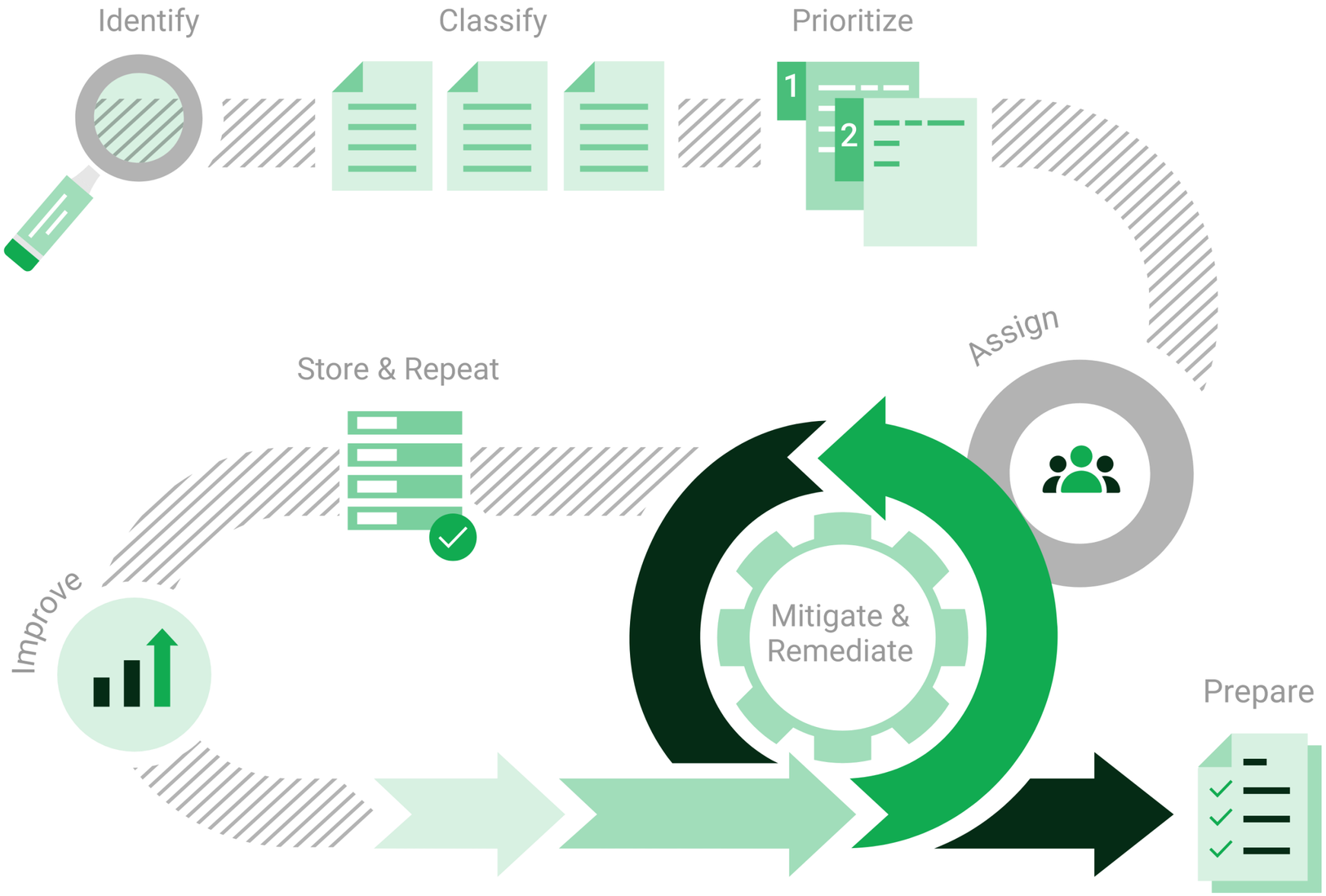
Vulnerability Scanning per:

- identificare (tutte) le vulnerabilità (note)
- senza causare impatti sull'infrastruttura
- prima che lo facciano i malintenzionati
- definire un livello di rischio (standard)

E dopo?

- prioritizzare le vulnerabilità
- risolvere le problematiche
- verificare la corretta risoluzione
- goto 1





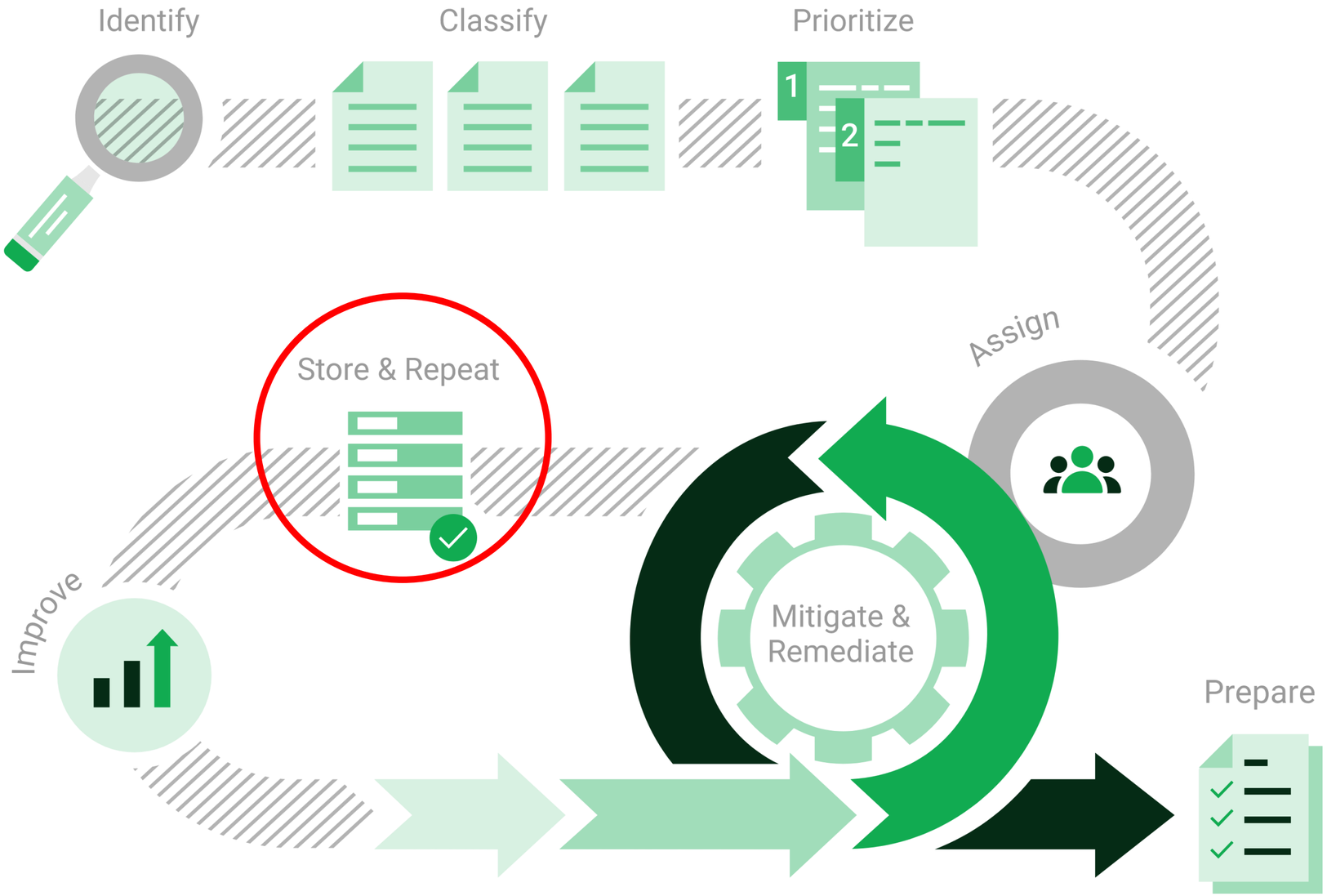
https://docs.greenbone.net/GSM-Manual/gos-24.10/en/introduction.html#vulnerability-management

Superare il "Vulnerability Scanning":

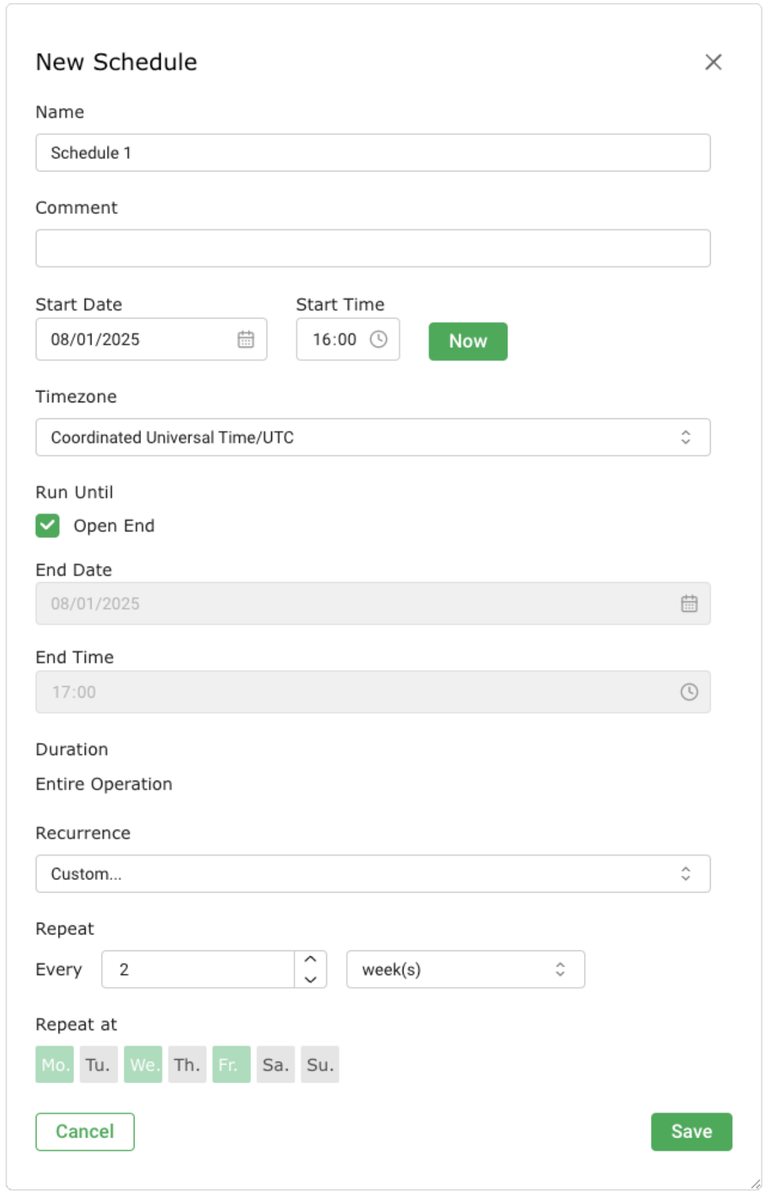
- eseguito su richiesta / una tantum
- livello di rischio reale non stimato
- solo per "compliance"
- report "nel cassetto"
- vulnerabilità di rischio "medio" o "basso" ignorate
- perimetro di scansione incompleto
- mancata verifica dei rientri

Superare il "Vulnerability Scanning":

- **eseguito su richiesta / una tantum**
- livello di rischio reale non stimato
- solo per "compliance"
- report "nel cassetto"
- vulnerabilità di rischio "medio" o "basso" ignorate
- perimetro di scansione incompleto
- mancata verifica dei rientri

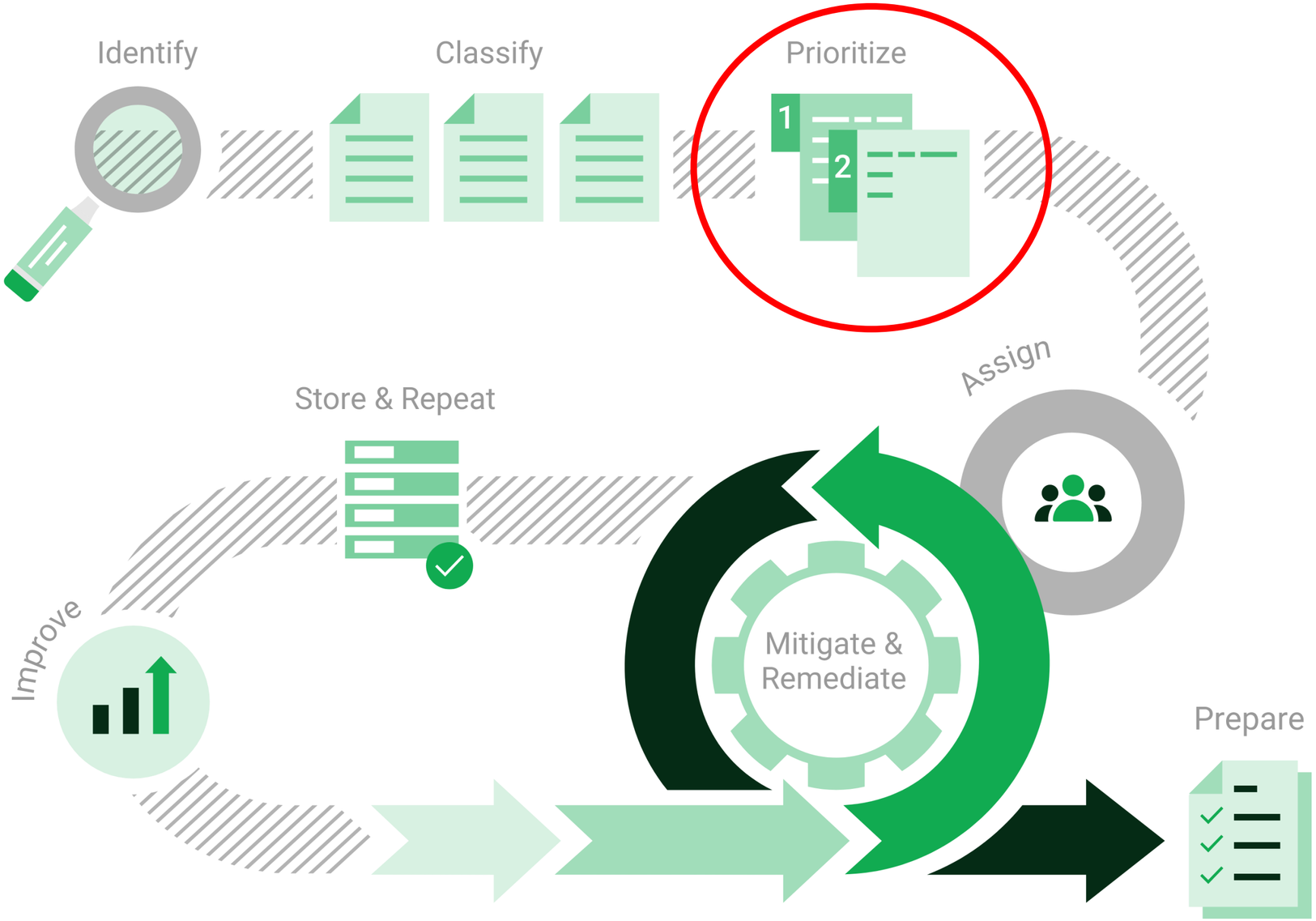


https://docs.greenbone.net/GSM-Manual/gos-24.10/en/introduction.html#vulnerability-management


New Schedule
Name
Schedule 1
Comment
Start Date
08/01/2025
Start Time
16:00
Now
Timezone
Coordinated Universal Time/UTC
Run Until
Open End
End Date
08/01/2025
End Time
17:00
Duration
Entire Operation
Recurrence
Custom...
Repeat
Every
2
week(s)
Repeat at
Mo.
Tu.
We.
Th.
Fr.
Sa.
Su.
Cancel
Save

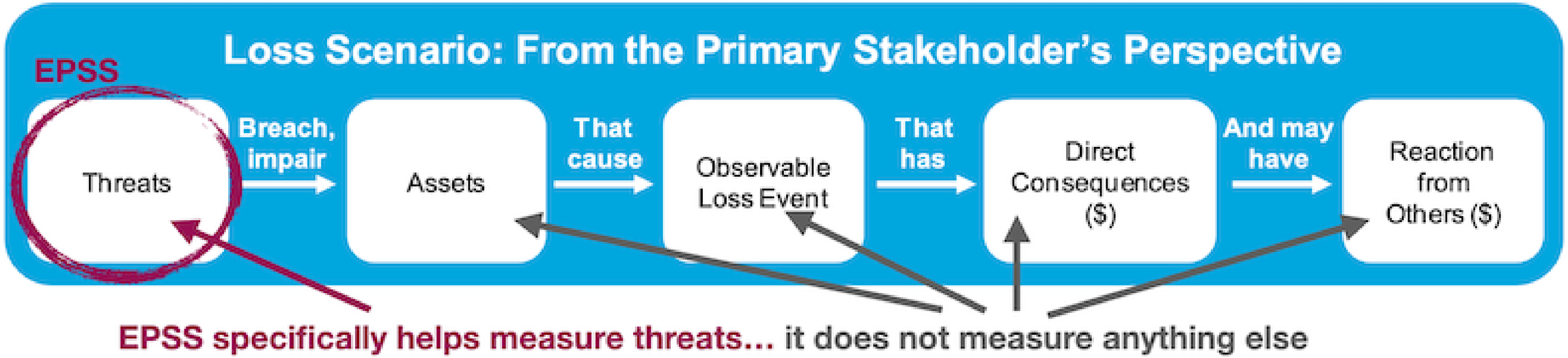
Superare il "Vulnerability Scanning":

- eseguito su richiesta / una tantum
- **livello di rischio reale non stimato**
- solo per "compliance"
- report "nel cassetto"
- vulnerabilità di rischio "medio" o "basso" ignorate
- perimetro di scansione incompleto
- mancata verifica dei rientri



https://docs.greenbone.net/GSM-Manual/gos-24.10/en/introduction.html#vulnerability-management

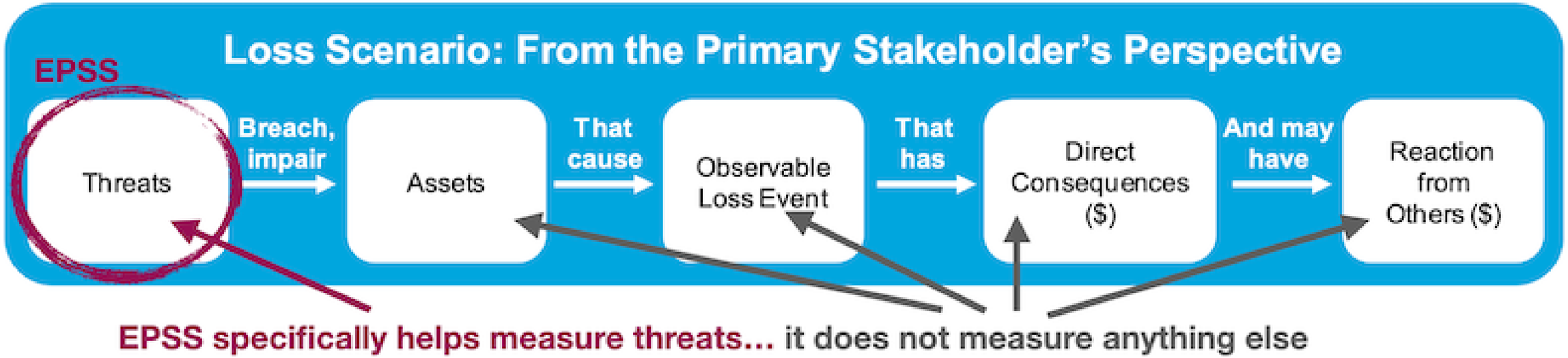
The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. Our goal is to assist network defenders to better prioritize vulnerability remediation efforts. While other industry standards have been useful for capturing innate characteristics of a vulnerability and provide measures of severity, they are limited in their ability to assess threat. EPSS fills that gap because it uses current threat information from CVE and real-world exploit data. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.



https://www.first.org/epss/faq

The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. Our goal is to assist network defenders to better prioritize vulnerability remediation efforts. While other industry standards have been useful for capturing innate characteristics of a vulnerability and provide measures of severity, they are limited in their ability to assess threat. EPSS fills that gap because it uses current threat information from CVE and real-world exploit data. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

Attenzione!



https://www.first.org/epss/faq

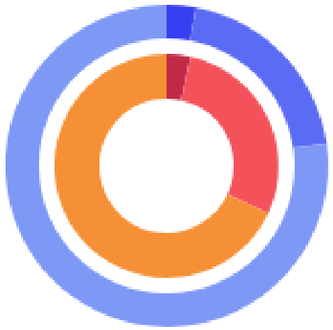
Superare il "Vulnerability Scanning":

- eseguito su richiesta / una tantum
- livello di rischio reale non stimato
- **solo per "compliance"**
- report "nel cassetto"
- vulnerabilità di rischio "medio" o "basso" ignorate
- perimetro di scansione incompleto
- mancata verifica dei rientri

"Le scansioni esterne devono essere eseguite almeno una volta ogni tre mesi e dopo ogni modifica significativa all'infrastruttura o alle applicazioni."

"Le scar … o essere eseguit… ogni tre me… fica signific… ra o alle

New/Updated CVEs



215 CVEs created, 384 CVEs updated since yesterday

1806 CVEs created, 2612 CVEs updated in the last 7 days

4295 CVEs created, 10167 CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
4	9	36

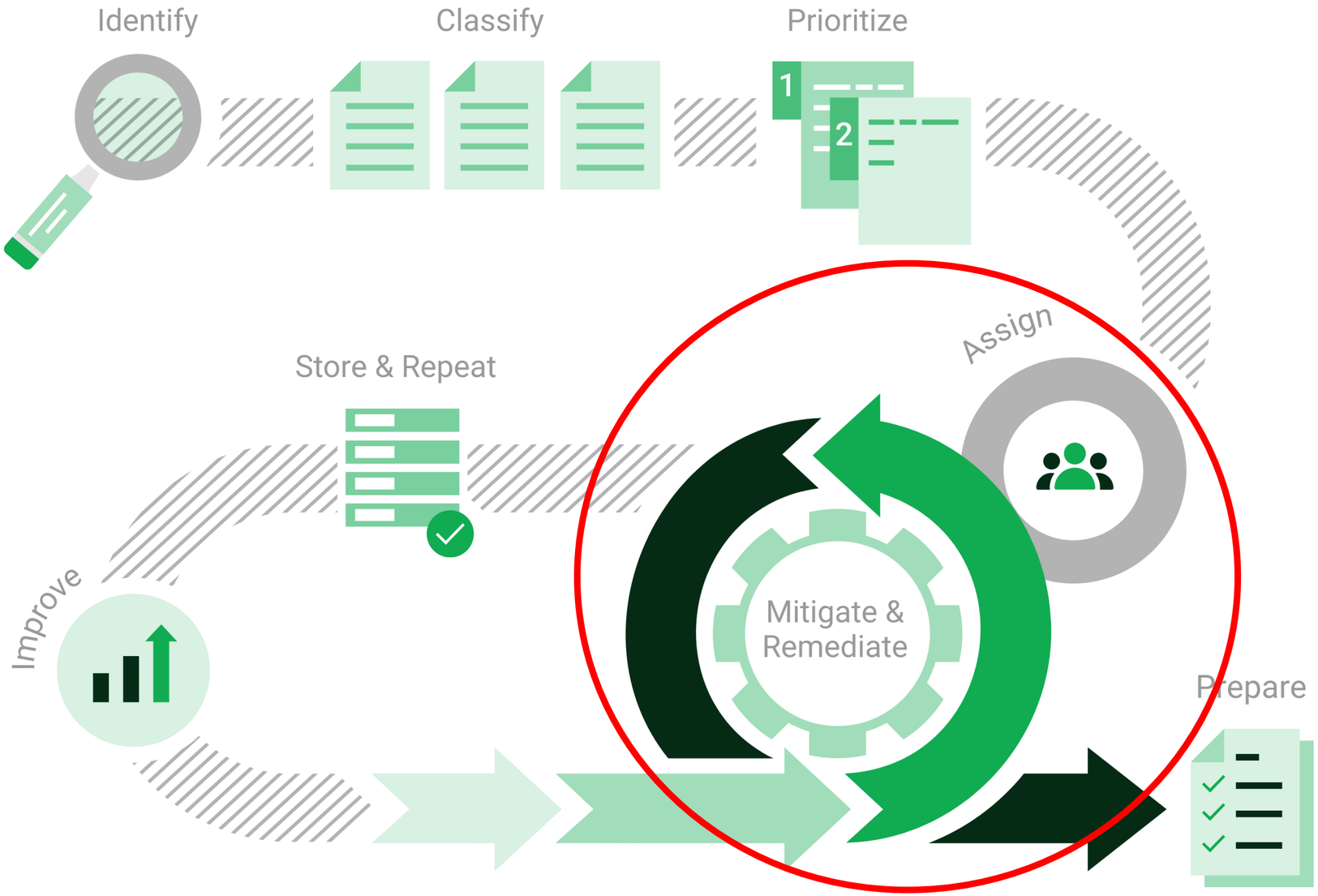
Recent EPSS score changes

>5%	>10%	>50%
6	2	2

https://www.cvedetails.com/

Superare il "Vulnerability Scanning":

- eseguito su richiesta / una tantum
- livello di rischio reale non stimato
- solo per "compliance"
- **report "nel cassetto"**
- vulnerabilità di rischio "medio" o "basso" ignorate
- perimetro di scansione incompleto
- mancata verifica dei rientri



https://docs.greenbone.net/GSM-Manual/gos-24.10/en/introduction.html#vulnerability-management

Superare il "Vulnerability Scanning":

- eseguito su richiesta / una tantum
- livello di rischio reale non stimato
- solo per "compliance"
- report "nel cassetto"
- **vulnerabilità di rischio "medio" o "basso" ignorate**
- perimetro di scansione incompleto
- mancata verifica dei rientri

https://docs.greenbone.net/GSM-Manual/gos-24.10/en/introduction.html#vulnerability-management

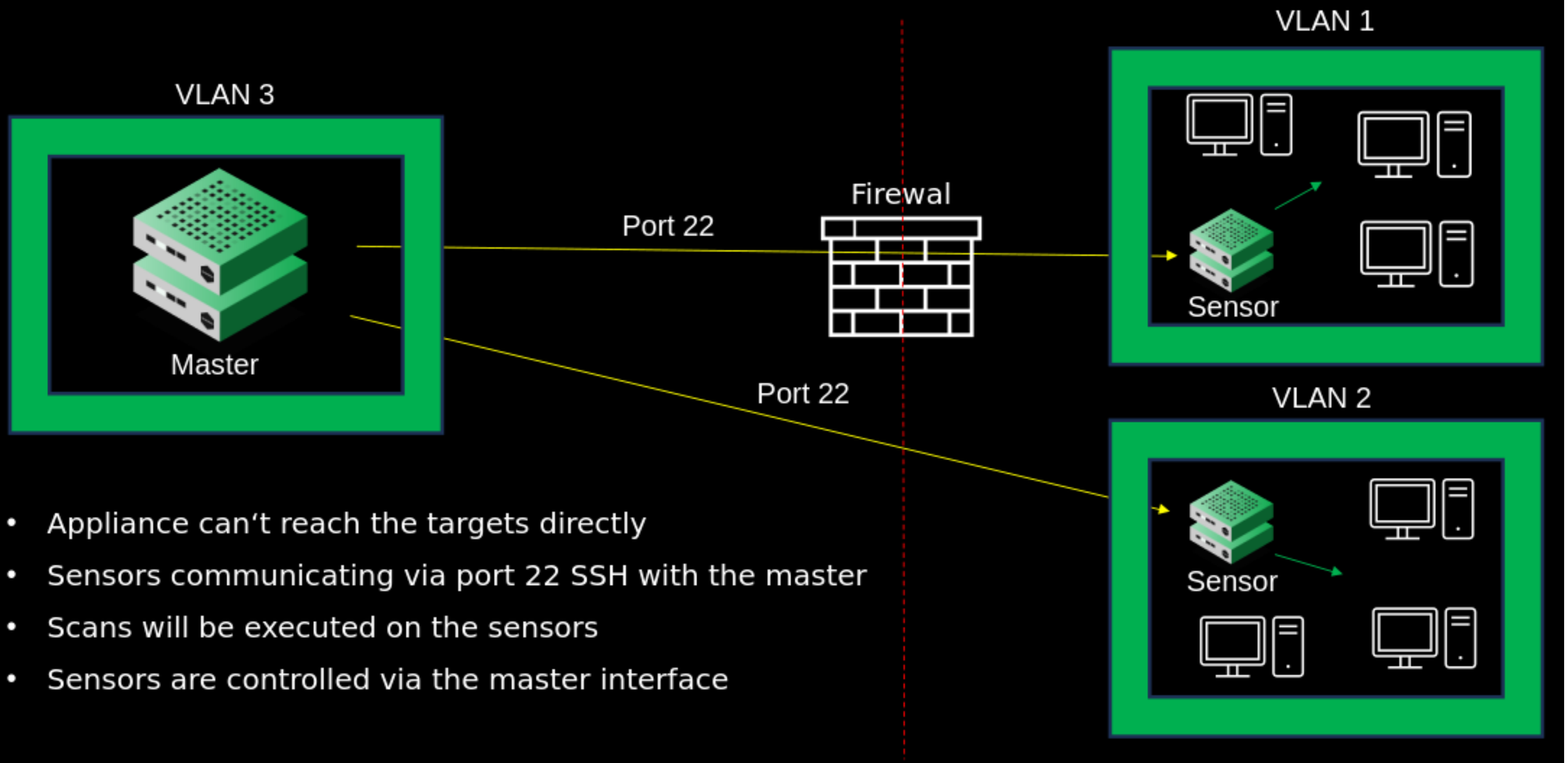
Superare il "Vulnerability Scanning":

- eseguito su richiesta / una tantum
- livello di rischio reale non stimato
- solo per "compliance"
- report "nel cassetto"
- vulnerabilità di rischio "medio" o "basso" ignorate
- **perimetro di scansione incompleto**
- mancata verifica dei rientri

Perimetro di scansione incompleto:

- Scansione solo da Internet (no LAN)
- Reti segmentate (VLAN, ecc)
- Reti remote (WAN, ecc)
- Sistemi in cloud (IaaS, ecc)
- Postazioni di lavoro
  - spente o non raggiungibili (es. "Road warrior")
  - firewallate
  - applicazioni "client"

SCENARIO: MASTER / SENSOR



- Appliance can‘t reach the targets directly
- Sensors communicating via port 22 SSH with the master
- Scans will be executed on the sensors
- Sensors are controlled via the master interface

Greenbone

9.3 Configuring an Authenticated Scan Using Local Security Checks

An authenticated scan can provide more vulnerability details on the scanned system. During an authenticated scan the target is both scanned from the outside using the network and from the inside using a valid user login.

During an authenticated scan, the appliance logs into the target system in order to run local security checks (LSC). The scan requires the prior setup of user credentials. These credentials are used to authenticate to different services on the target system. In some circumstances the results could be limited by the permissions of the users used.

The VTs in the corresponding VT families (local security checks) will only be executed if the appliance was able to log into the target system. The local security check VTs in the resulting scan are minimally invasive.

The appliance only determines the risk level but does not introduce any changes on the target system. However, the login by the appliance is probably logged in the protocols of the target system.

The appliance can use different credentials based on the nature of the target. The most important ones are:

- SMB

  On Microsoft Windows systems, the appliance can check the patch level and locally installed software such as Adobe Acrobat Reader or the Java suite.

- SSH

  This access is used to check the patch level on Unix and Linux systems.

- ESXi

  This access is used for testing of VMware ESXi servers locally.

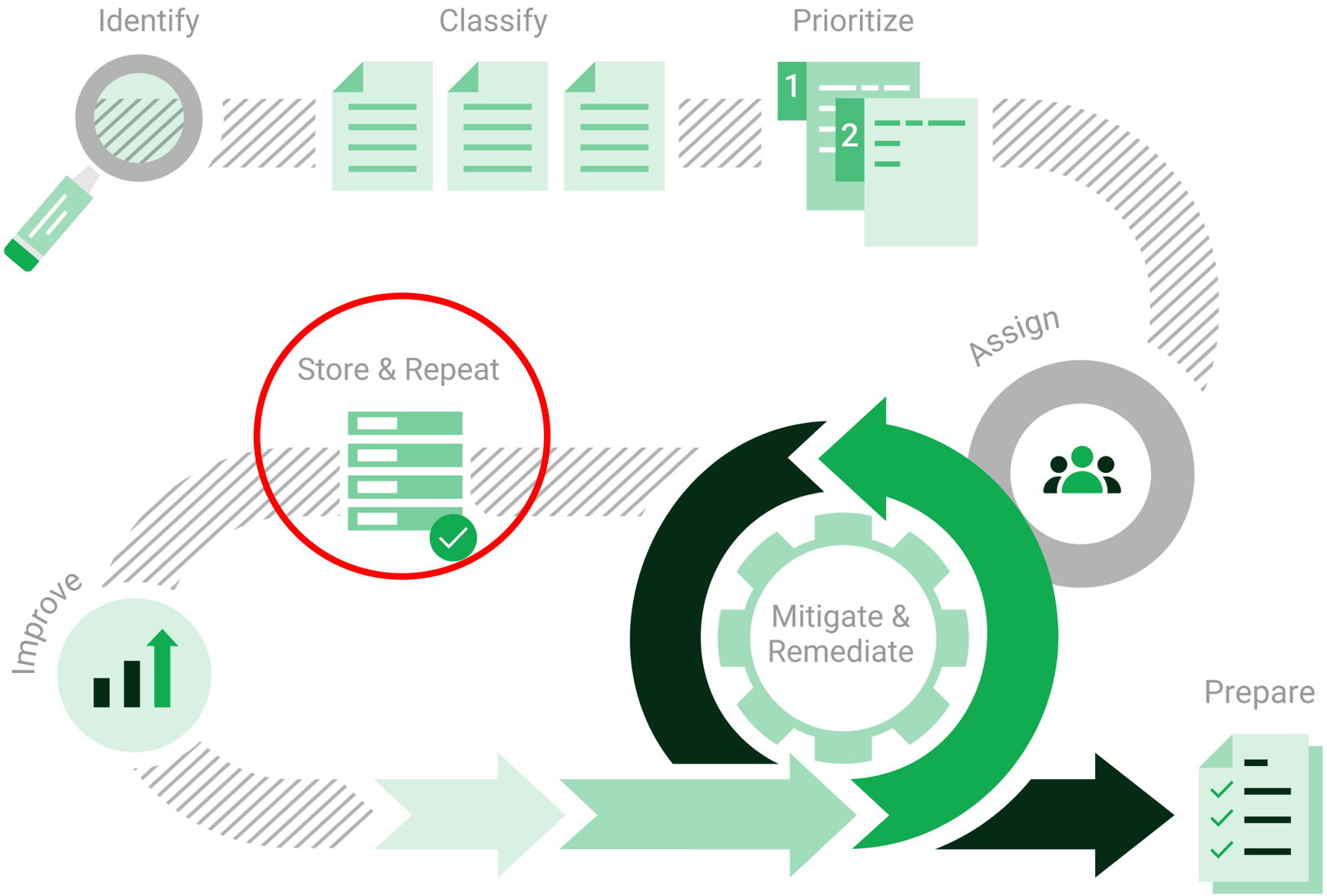
- SNMP

  Network components like routers and switches can be tested via SNMP.

https://docs.greenbone.net/GSM-Manual/gos-24.10/en/scanning.html#configuring-an-authenticated-scan-using-local-security-checks

Superare il "Vulnerability Scanning":

- eseguito su richiesta / una tantum
- livello di rischio reale non stimato
- solo per "compliance"
- report "nel cassetto"
- vulnerabilità di rischio "medio" o "basso" ignorate
- perimetro di scansione incompleto
- **mancata verifica dei rientri**



https://docs.greenbone.net/GSM-Manual/gos-24.10/en/introduction.html#vulnerability-management

Punti chiave

- Asset management
- Categorizzazione degli asset
- Prioritizzazione vulnerabilità / risoluzioni
- Automazione e orchestrazione
- Metriche e KPI
- Scansione frequente / continua
- Vulnerability feed completo e aggiornato

Bonus:

- Open Source
- Sovranità tecnologica

Open Source

History of the OpenVAS project

In 2005, the developers of the vulnerability scanner Nessus decided to discontinue the work under open-source licenses and switch to a proprietary business model.

At this point, developers from Intevation and DN-Systems – the two companies which would later found the Greenbone AG – were already contributing developments to Nessus, focusing on client tools. The works were primarily supported by the German Federal Office for Information Security (BSI).

In 2006, several forks of Nessus were created in response to the discontinuation of the open-source solution. Of these forks, only one has continued to show activity: OpenVAS, the Open Vulnerability Assessment System. OpenVAS was registered as a project at Software in the Public Interest, Inc. to hold and protect the domain “openvas.org”.

The years 2006 and 2007 brought little activity other than cleanups of the status quo. But in late 2008, the Greenbone AG, based in Osnabrück, Germany was founded to drive OpenVAS forward. Essentially, Greenbone’s business plan was about 3 cornerstones:

1. Go beyond plain vulnerability scanning towards a comprehensive vulnerability management solution.
2. Create a turn-key appliance product for enterprise customers.
3. Continue the open-source concept of creating a transparent security technology.

https://greenbone.github.io/docs/latest/background.html

Q&A

SECURITY SUMMIT

Security Summit

Milano 11-12-13 marzo 2025

Clusit 25 2000-2025

ASTREA

Contatti:

sales@greenbone.net

Vieni a trovarci al nostro stand!

Clusit 25 2000-2025

SECURITY SUMMIT