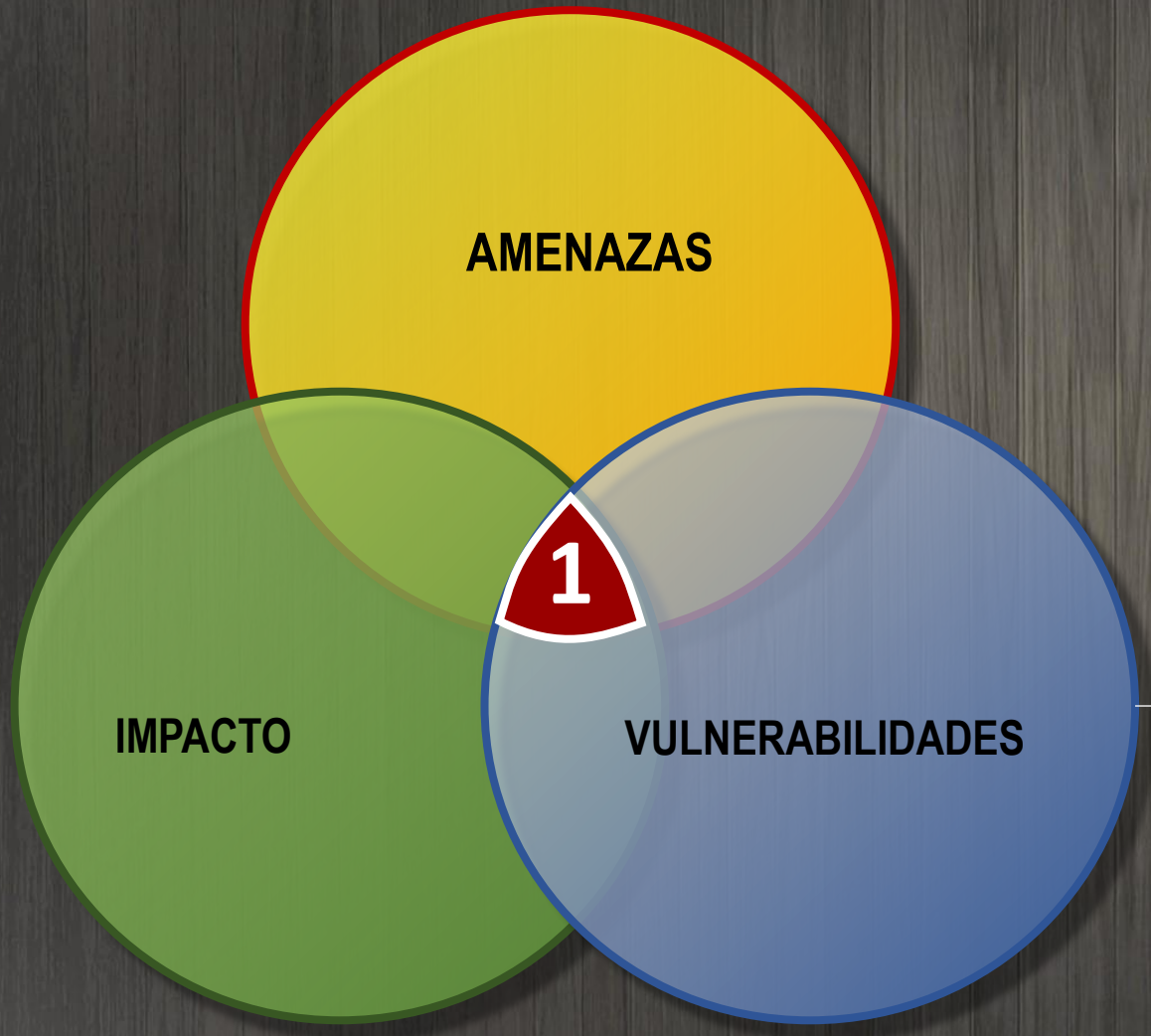

XVIII JORNADAS STIC CCN-CERT
VI JORNADAS DE CIBER_ DEFENSA ESPDEF-CERT
Cuidado, Tienes Extraños Merodeando
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
20 ANIVERSARIO
Centro Criptológico Nacional
CCN-CERT
centro criptológico nacional
ESPDEF-CERT
Mando Conjunto del Ciberespacio
/RootedCON
CIBERDEFENSA ACTIVA PARA UN MUNDO DIGITAL

RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



GESTION DE VULNERABILIDADES

Subdominio de la gestión de riesgos de TI, responsable del descubrimiento, la priorización y la resolución continua de vulnerabilidades de seguridad en la infraestructura y el software de TI de una organización

Proceso de Gestión de vulnerabilidades

Validación

Se verifica la efectividad. A menudo se realizan pentesting para garantizar que los esfuerzos hayan abordado las vulnerabilidades de manera suficiente.

Inventario de activos

Los equipos deben identificar y documentar los sistemas, las aplicaciones y los activos dentro del alcance del programa

Remediación

Es la fase más crucial. Puede implicar aplicar parches, reconfigurar sistemas, actualizar versiones de software, cambiar controles de acceso o implementar otras medidas

Escaneo de Vulnerabilidades

Se utilizan herramientas de escaneo automatizadas para detectar vulnerabilidades, que comparan y correlacionan el software y las configuraciones con una base de datos de vulnerabilidades

Priorización

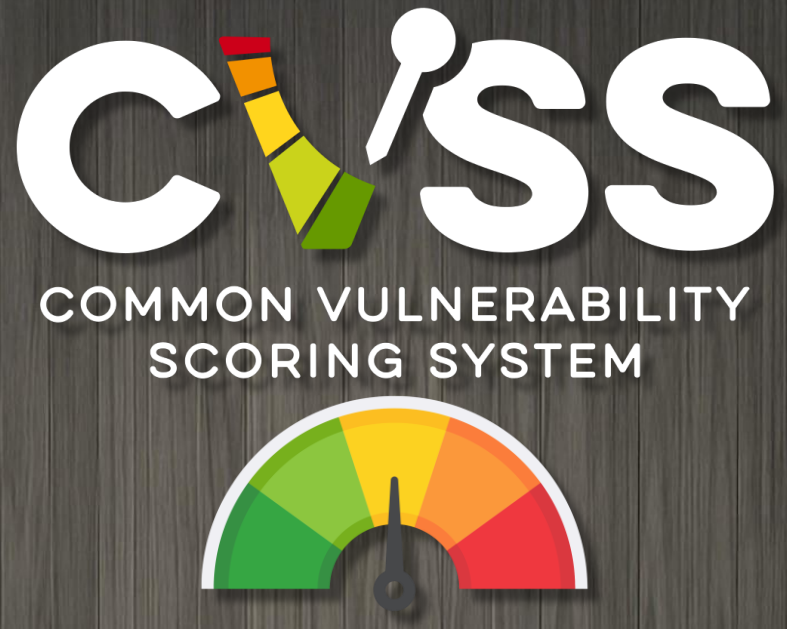
Se revisa y se prioriza la lista según el riesgo, el impacto y el costo de la reparación. Esto les permite asignar los recursos para maximizar la reducción del riesgo y el retorno de la inversión

Evaluación de Vulnerabilidades

Se evalúan para determinar el nivel de riesgo. Se suele utilizar el Common Vulnerability Scoring System (CVSS) para clasificar el impacto potencial y la gravedad de cada vulnerabilidad

2004

https://www.first.org/cvss/



- El Sistema de Puntuación de Vulnerabilidades Comunes (CVSS) ofrece una manera de capturar las características principales de una vulnerabilidad y generar una puntuación numérica que refleje su gravedad.
- La puntuación numérica puede traducirse en una representación cualitativa (como baja, media, alta y crítica)
- OBJETIVO: ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.

CVSS

COMMON VULNERABILITY SCORING SYSTEM

Base Metrics

Exploitability Metrics

- Attack Vector (AV)
- Attack Complexity (AC)
- Attack Requirements (AT) NEW
- Privileges Required (PR)
- User Interaction (UI)

Vulnerable System Impact Metrics

- Confidentiality (VC)
- Integrity (VI)
- Availability (VA)

Subsequent System Impact Metrics

- Confidentiality (SC) NEW
- Integrity (SI) NEW
- Availability (SA) NEW

Threat Metrics

- Exploit Maturity (E)

Supplemental Metrics NEW

- Safety (S):
- Automatable (AU):
- Recovery (R):
- Value Density (V):
- Vulnerability Response Effort (RE):
- Provider Urgency (U):

4.0 - Noviembre 2023

Ambiental Metrics

- Confidentiality RQs (CR):
- Integrity RQs (IR):
- Availability RQs (AR):

Modified Base Metrics

- Attack Vector (MAV)
- Attack Complexity (MAC)
- Attack Requirements (MAT)
- Privileges Required (MPR)
- User Interaction (MUI):

- Vulnerable Confidentiality (MVC)
- Vulnerable Integrity (MVI)
- Vulnerable Availability (MVA)

- Subsequent Confidentiality (MSC)
- Subsequent Integrity (MSI)
- Subsequent Availability (MSA)

https://www.first.org/cvss/

CVE-2020-3947

VMware Workstation (15.x anterior a 15.5.2) y Fusion (11.x anterior a 11.5.2). Contiene una vulnerabilidad de uso posterior en vm.net.dhcp. La explotación exitosa de este problema puede provocar la ejecución de código en el host desde el invitado o puede permitir a los atacantes crear una condición de denegación de servicio del servicio vm.net.dhcp que se ejecuta en la máquina host.

Métrico	Valor	Comentarios
Explotar la madurez	Prueba de concepto (P)	Está disponible una prueba de concepto

CVE-2020-3947 Detail

8,8

Description

VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine.

Metrics

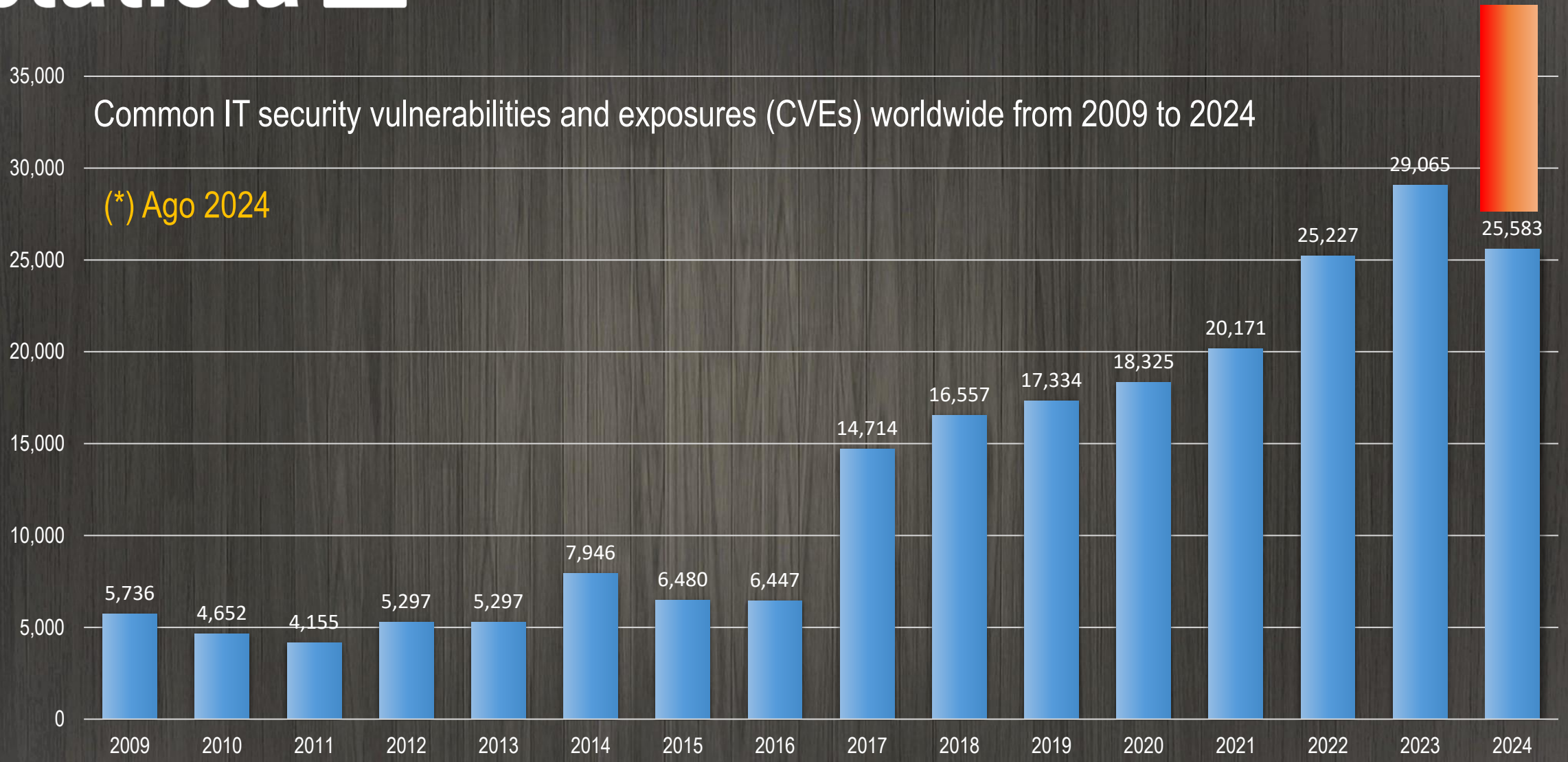
CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 8.8 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

statista



https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

“Un gran problema de la gestión de las vulnerabilidades es la existencia de parches”

- Los equipos de TI aplican el protocolo existente
- Pero **NO** se hace una adecuada gestión del riesgo

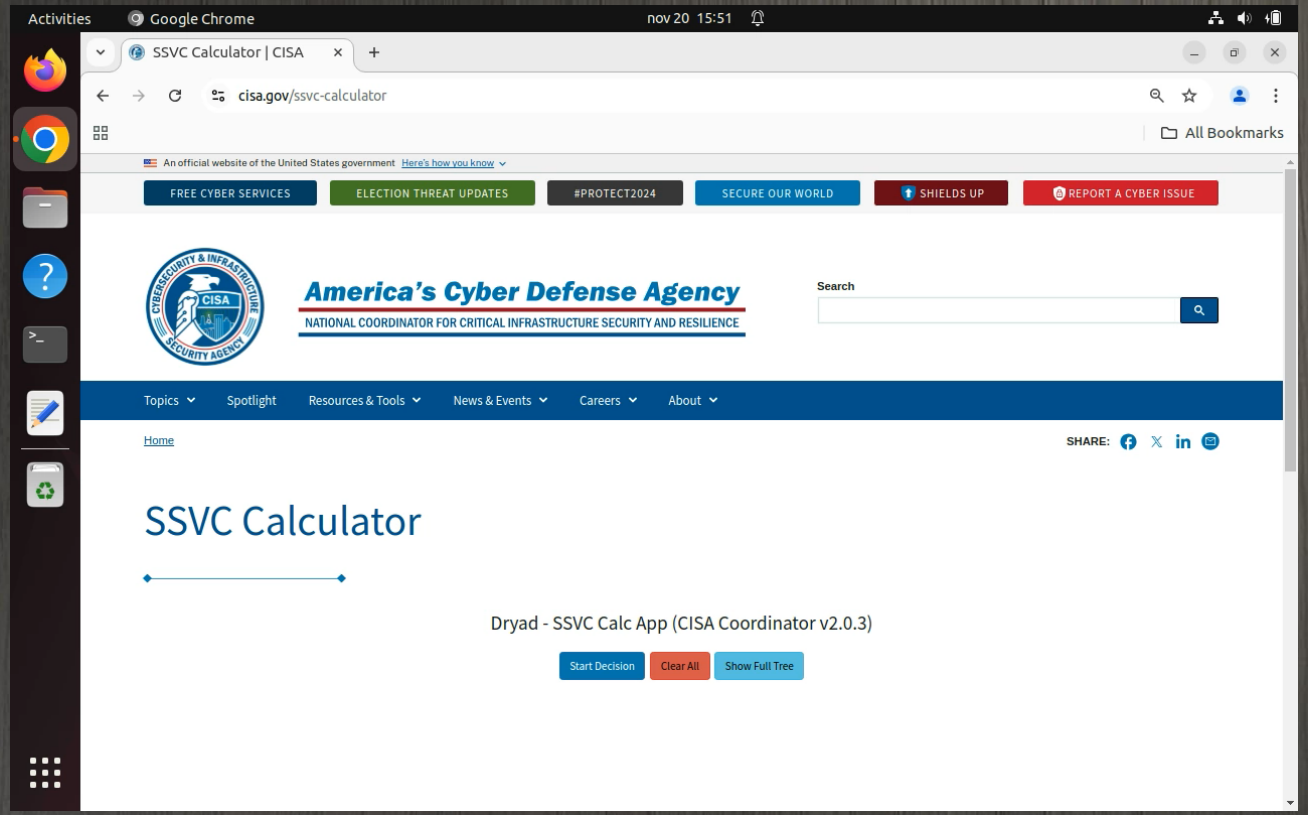
- El hecho de que exista una vulnerabilidad no significa que aplicar parches sea la respuesta.
  - A veces, son los cambios de configuración, actualizaciones, o controles compensatorios.
- El volumen de esfuerzo requerido y la diversidad de problemas conducen a una “fatiga” que dificulta la interpretación adecuada del riesgo, limitando su utilidad

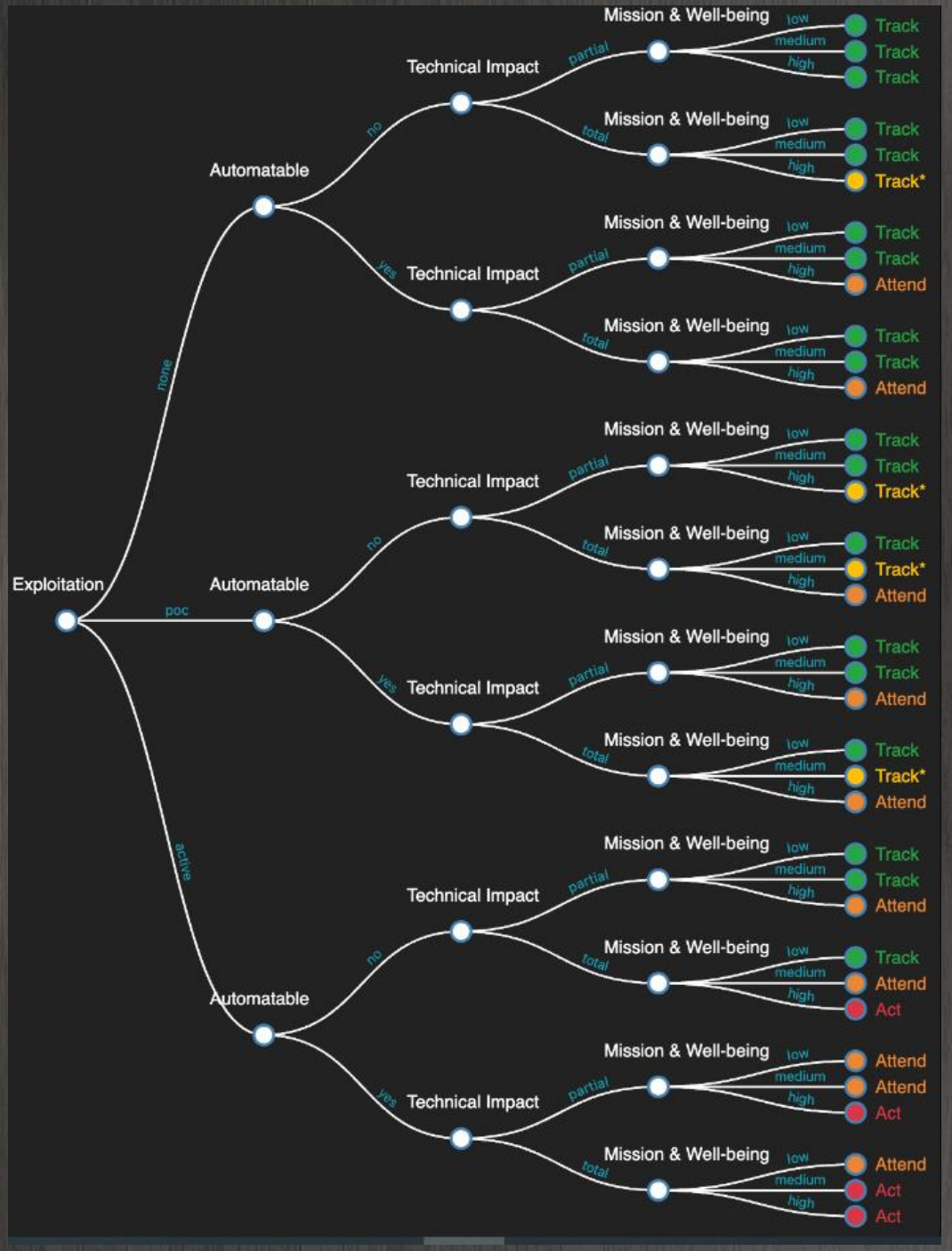
CISA SSVC

Stakeholder-Specific Vulnerability Categorization

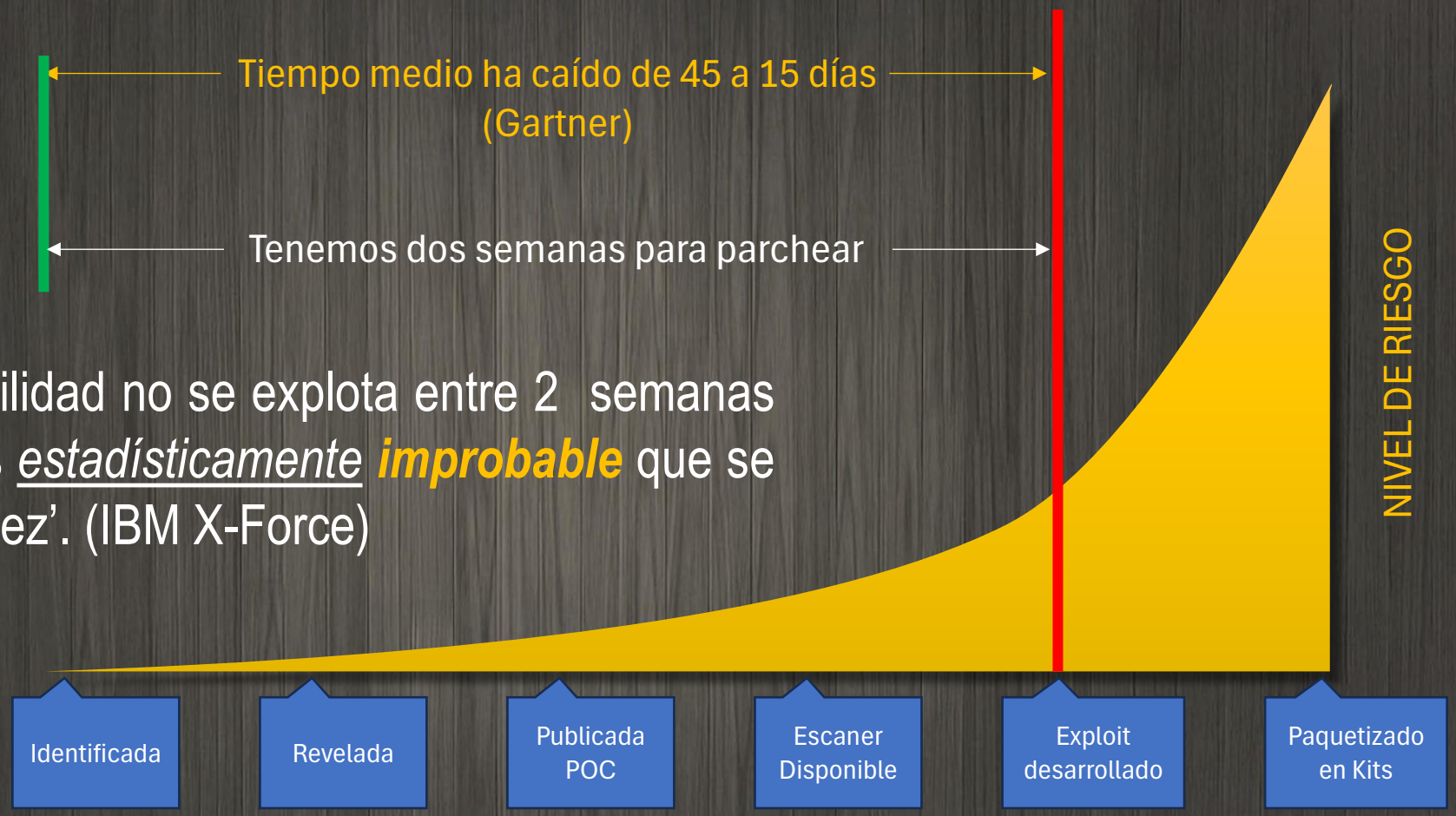
- **Seguimiento** (Track): La vulnerabilidad no requiere ninguna acción en este momento.
- **Pista** (Track +): La vulnerabilidad contiene características específicas que pueden requerir un seguimiento más minucioso para detectar cambios.
- **Asistir** (Attend): la vulnerabilidad requiere atención. Puede incluir acciones, solicitar asistencia o información extra. CISA recomienda remediar antes de plazo standar.
- **Actuar** : La vulnerabilidad requiere atención de la organización (niveles de supervisión y de liderazgo). Las acciones son necesarias. Los grupos internos se reúnen para determinar la respuesta general y ejecutar las acciones acordadas. CISA recomienda remediar ASAP las vulnerabilidades

CISA SSVC


Activities
Google Chrome
nov 20 15:51
SSVC Calculator | CISA
cisa.gov/ssvc-calculator
All Bookmarks
An official website of the United States government
FREE CYBER SERVICES
ELECTION THREAT UPDATES
#PROTECT2024
SECURE OUR WORLD
SHIELDS UP
REPORT A CYBER ISSUE
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
Home
SHARE:
SSVC Calculator
Dryad - SSVC Calc App (CISA Coordinator v2.0.3)
Start Decision
Clear All
Show Full Tree


Exploitation
none
poc
active
Automatable
Automatable
Automatable
no
yes
Technical Impact
partial
total
Mission & Well-being
low
medium
high
Track
Track*
Attend
Act

Incremento del riesgo



'Si una vulnerabilidad no se explota entre 2 semanas y tres meses, es *estadísticamente* ***improbable*** que se explote alguna vez'. (IBM X-Force)

El riesgo real aumenta drásticamente cuando las vulnerabilidades se convierten en un arma

"¿Qué hace que una vulnerabilidad sea más (o menos) propensa a ser explotada?"

FIRST

EPSS

Exploit Prediction Scoring System

- Sirve para estimar la probabilidad de que una vulnerabilidad sea explotada en los siguientes **30 días**.
- Objetivo: ayudar a priorizar mejor los esfuerzos de reparación de vulnerabilidades

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

EPSS

Exploit Prediction Scoring System

Información sobre las amenazas

La información de vulnerabilidad que recopila:

- Proveedor (CPE, vía NVD)
- Métricas CVSS (vector base de CVSS 3.x, a través de NVD)
- Debilidad en la vulnerabilidad (CWE, vía NVD)
- Edad de la vulnerabilidad (Días desde que CVE se publicó en la lista MITRE CVE)
- Referencias con etiquetas categóricas que definen su contenido (Lista MITRE CVE, NVD)
- Expresiones normalizadas extraídas de la descripción de la vulnerabilidad (Lista MITRE CVE)
- Se discute entre compañías y profesionales (CISA KEV, Google Project Zero, Zero Day Initiative (ZDI), …)
- Código de explotación disponible públicamente (Exploit-DB, GitHub, MetaSploit)
- Herramientas y escáneres de seguridad ofensivas: Intrigue, sn1per, jaeles, nuclei

Experiencia real

EPSS

Exploit Prediction Scoring System

Proceso

1. Recopilar **información** sobre vulnerabilidades de una variedad de fuentes.
2. Recopilar evidencias de la **actividad** de explotación diaria
3. Entrenar un modelo ML para descubrir la relación entre vulnerabilidad y actividad de explotación
4. Medir el **rendimiento** del modelo, ajustar y repetir para optimizar.
5. Actualizar la información y **estimar** la probabilidad de explotación (a 30 días).

El modelado EPSS aprovecha el aprendizaje automático (ML) para identificar patrones y relaciones entre la información de vulnerabilidad y la actividad de explotación recopilada

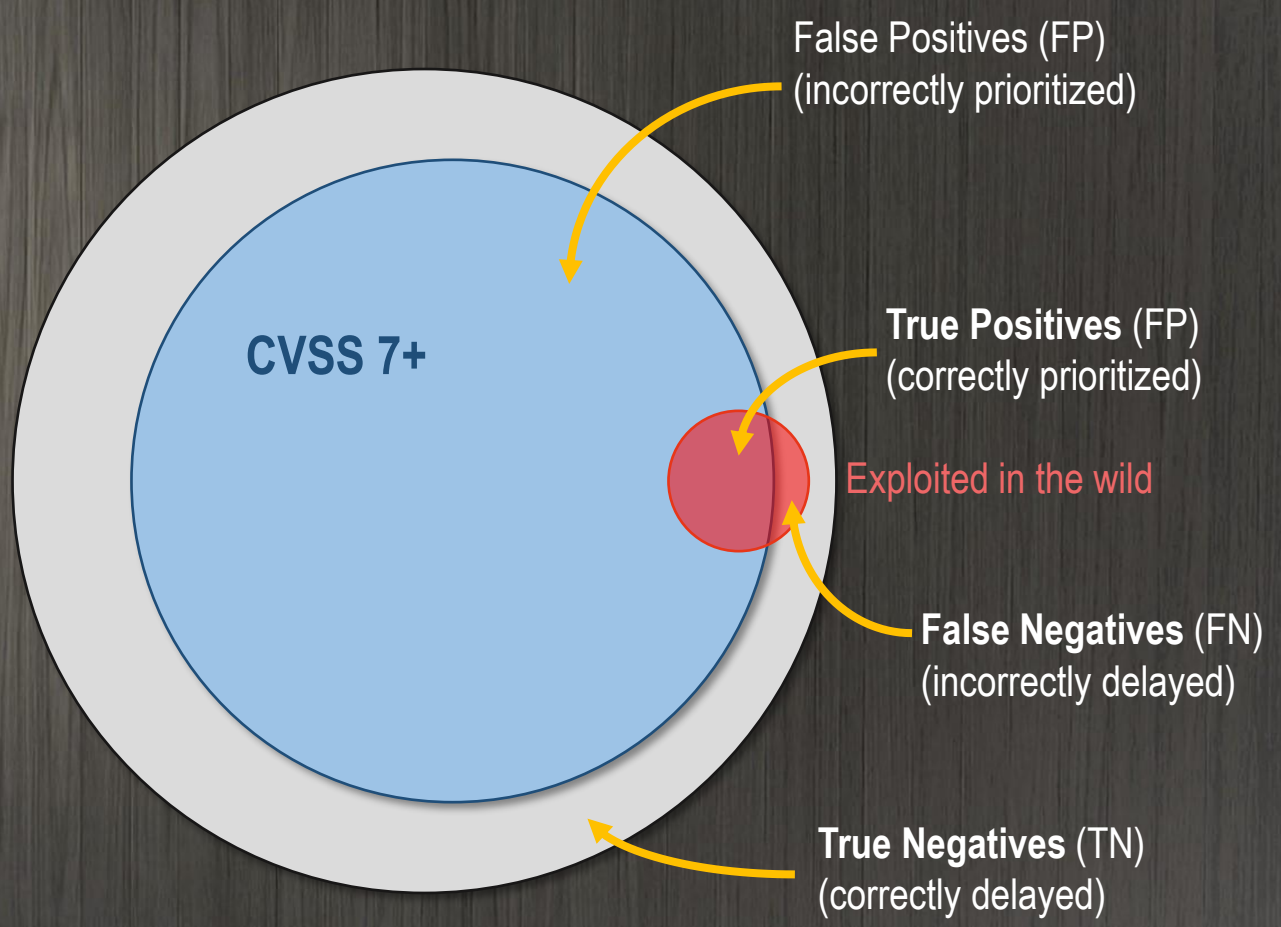
EPSS

Exploit Prediction Scoring System

- October 1st, 2023
- NVD published 139.473 CVSS

Política: **Remediar CVSS de 7+**

	Observado	No Observado
Remediate (CVSS 7+)	**3.166** (2,23%) True Positives (**TP**)	**76.858** (55,1%) False Positives (**FP**)
Delay (< CVSS 7)	**686** (0,5%) False Negatives (**FN**)	**58.763** (42,1%) True Negatives (**TN**)



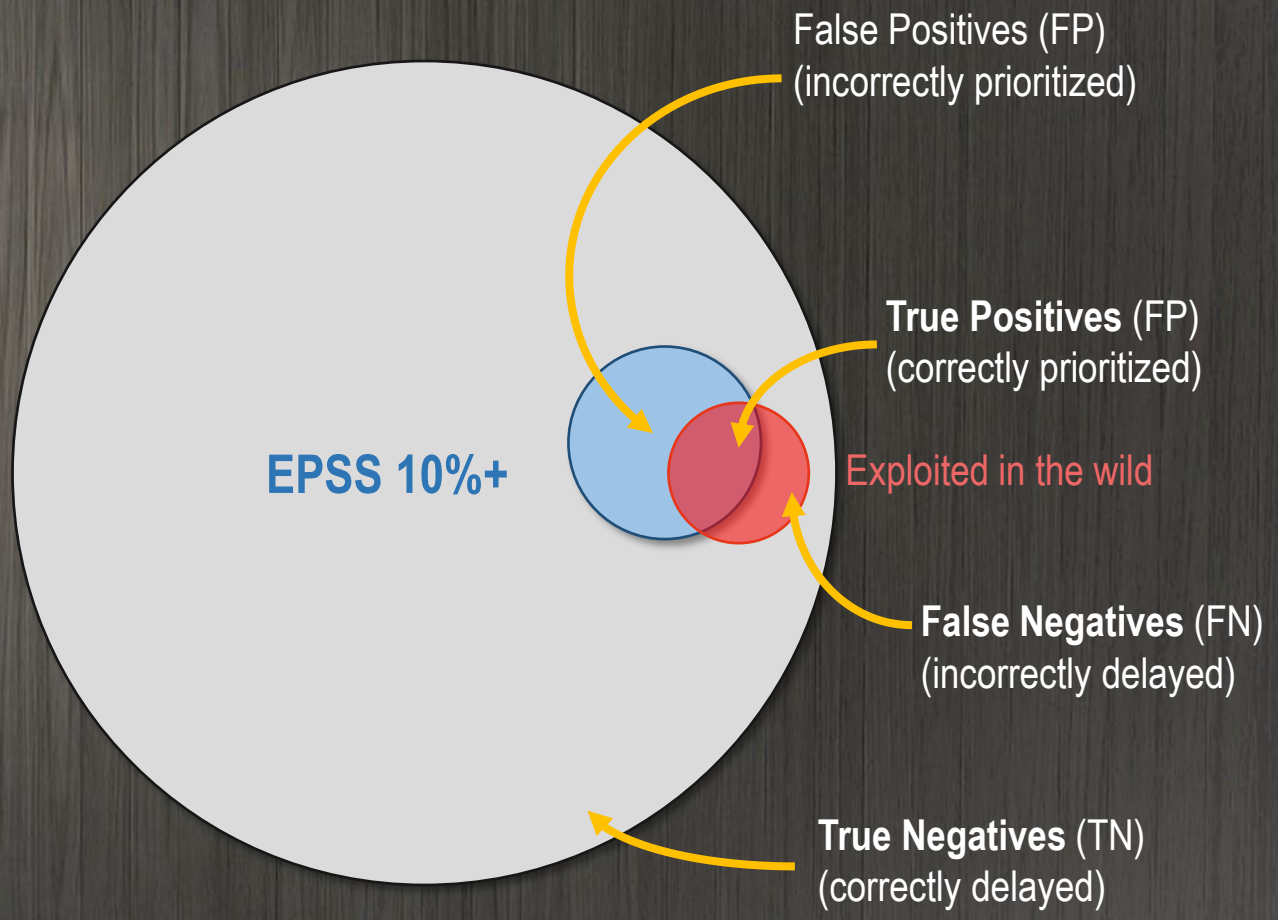
EPSS

Exploit Prediction Scoring System

- October 1st, 2023
- NVD published 139.473 CVSS

Política: **Remediar 10% priorizadas**

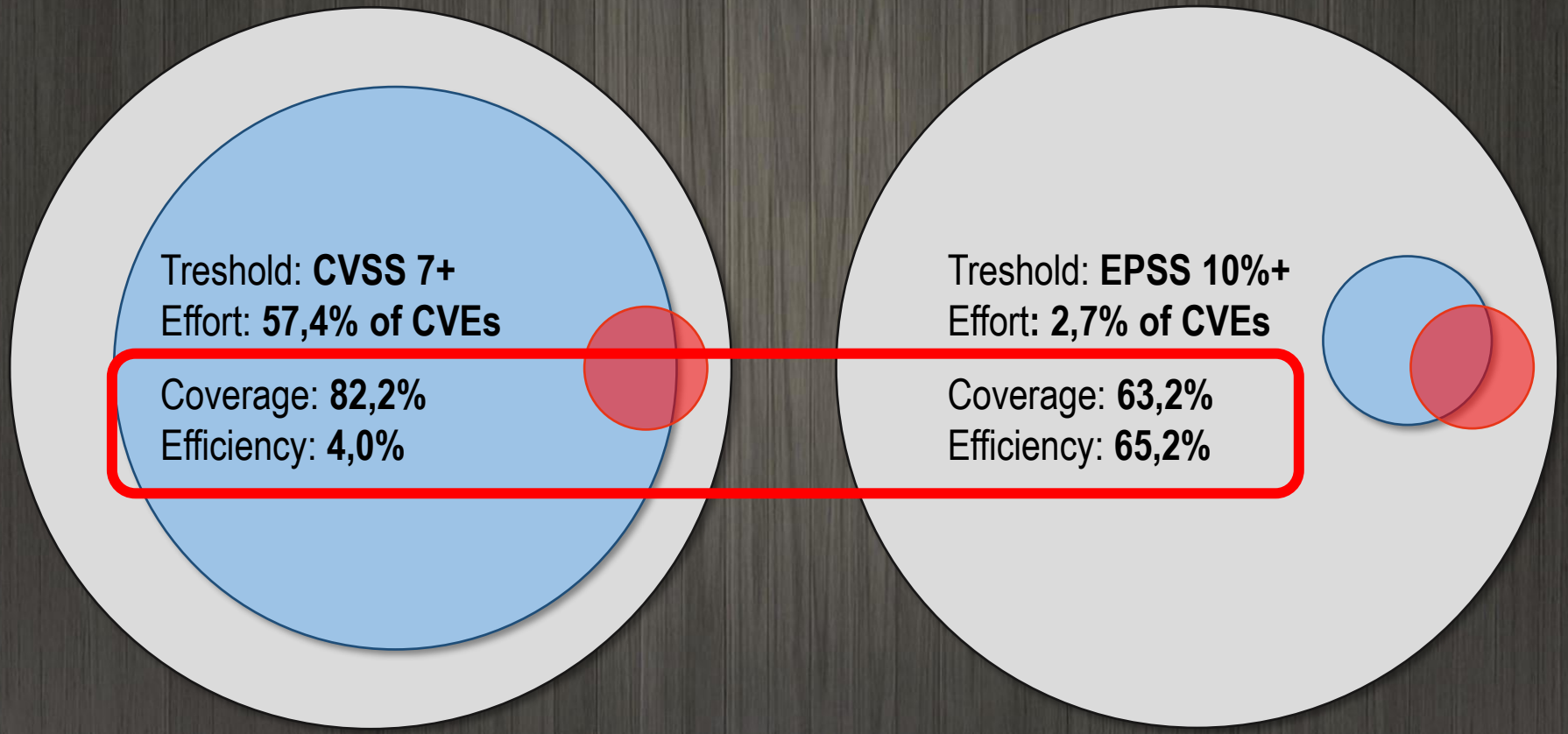
	Observado	No Observado
Remediate (EPSS 10%+)	**2.435** (1,8%) True Positives (**TP**)	**1.300** (0,9%) False Positives (**FP**)
Delay (< CVSS 10%)	**1.417** (1%) False Negatives (**FN**)	**134.321** (96,3%) True Negatives (**TN**)



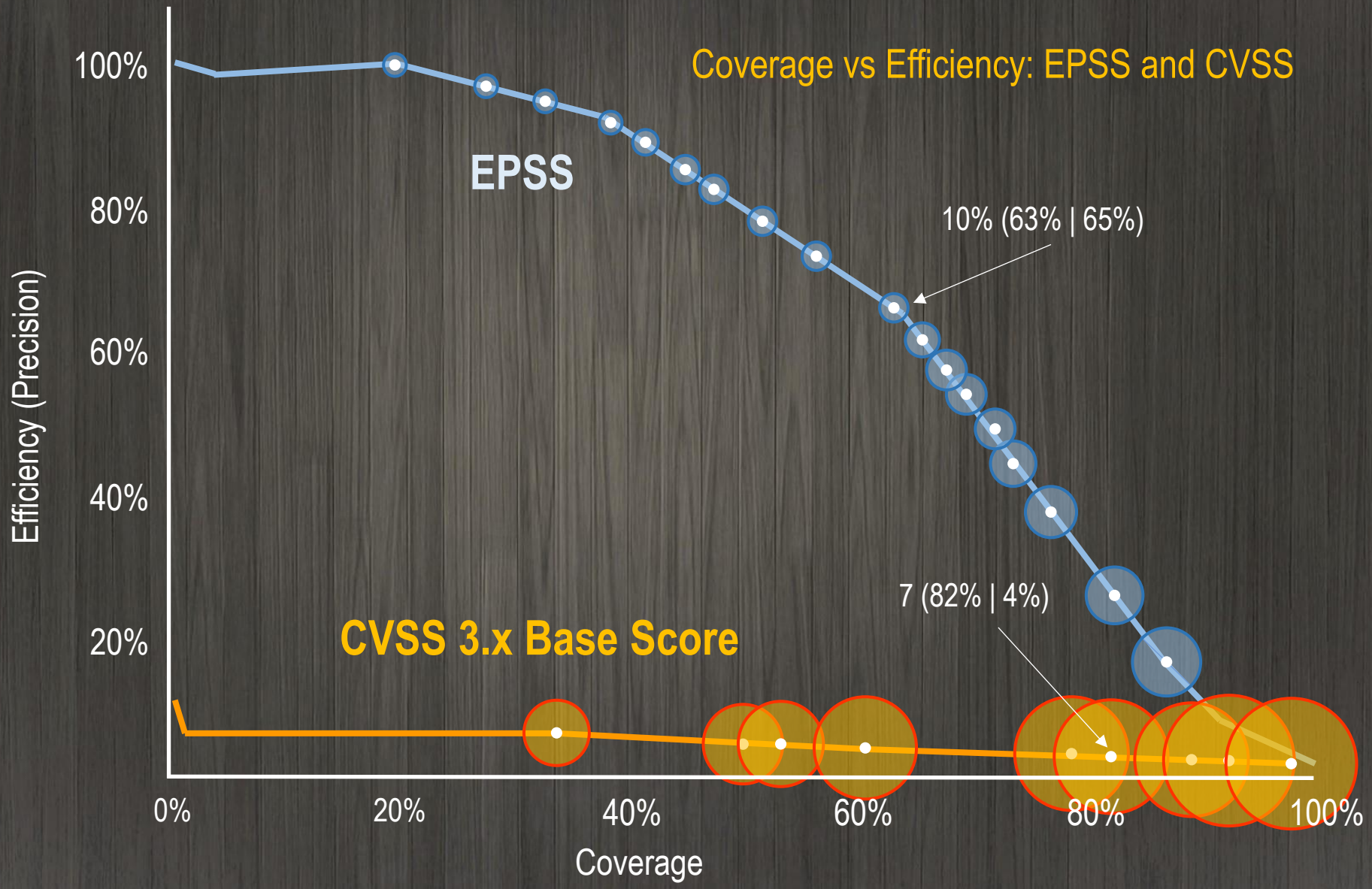
EPSS

Exploit Prediction Scoring System

Comparativa **CVSS** vs **EPSS**



EPSS


Coverage vs Efficiency: EPSS and CVSS
EPSS
10% (63% | 65%)
7 (82% | 4%)
CVSS 3.x Base Score
Efficiency (Precision)
100%
80%
60%
40%
20%
0%
20%
40%
60%
80%
100%
Coverage

EPSS

Top rated CVEs from the last thirty days

We selected the 48 highest rated CVEs published in the last

CVE-2024-9474 97.4%	CVE-2024-9935 1.0%	CVE-2024-50317 0.4%
CVE-2024-0012 96.6%	CVE-2024-50329 0.8%	CVE-2024-50318 0.4%
CVE-2024-51567 40.1%	CVE-2020-26073 0.7%	CVE-2024-50319 0.4%
CVE-2024-10915 19.7%	CVE-2024-49039 0.7%	CVE-2024-50320 0.4%
CVE-2024-10914 16.9%	CVE-2024-50324 0.6%	CVE-2024-50321 0.4%
CVE-2024-47575 5.2%	CVE-2024-50498 0.5%	CVE-2024-10599 0.4%
CVE-2024-44625 4.3%	CVE-2024-10919 0.5%	CVE-2024-11238 0.4%
CVE-2024-0875 1.9%	CVE-2024-43451 0.5%	CVE-2024-50326 0.4%

Detalle de CVE-2024-9474

7,2

Descripción

Una vulnerabilidad de escalada de privilegios en el software PAN-OS de Palo Alto Networks permite que un administrador de PAN-OS con acceso a la interfaz web de administración realice acciones en el firewall con privilegios de raíz. Cloud NGFW y Prisma Access no se ven afectados por esta vulnerabilidad.

Métrica

Versión 4.0 de CVSS | Versión 3.x de CVSS | Versión 2.0 de CVSS

NIST: NVD **Puntuación base:** 7.2 ALTO **Vector:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

0.4% 0.3% 0.2%

Detalle de CVE-2024-47575

9,8

Descripción

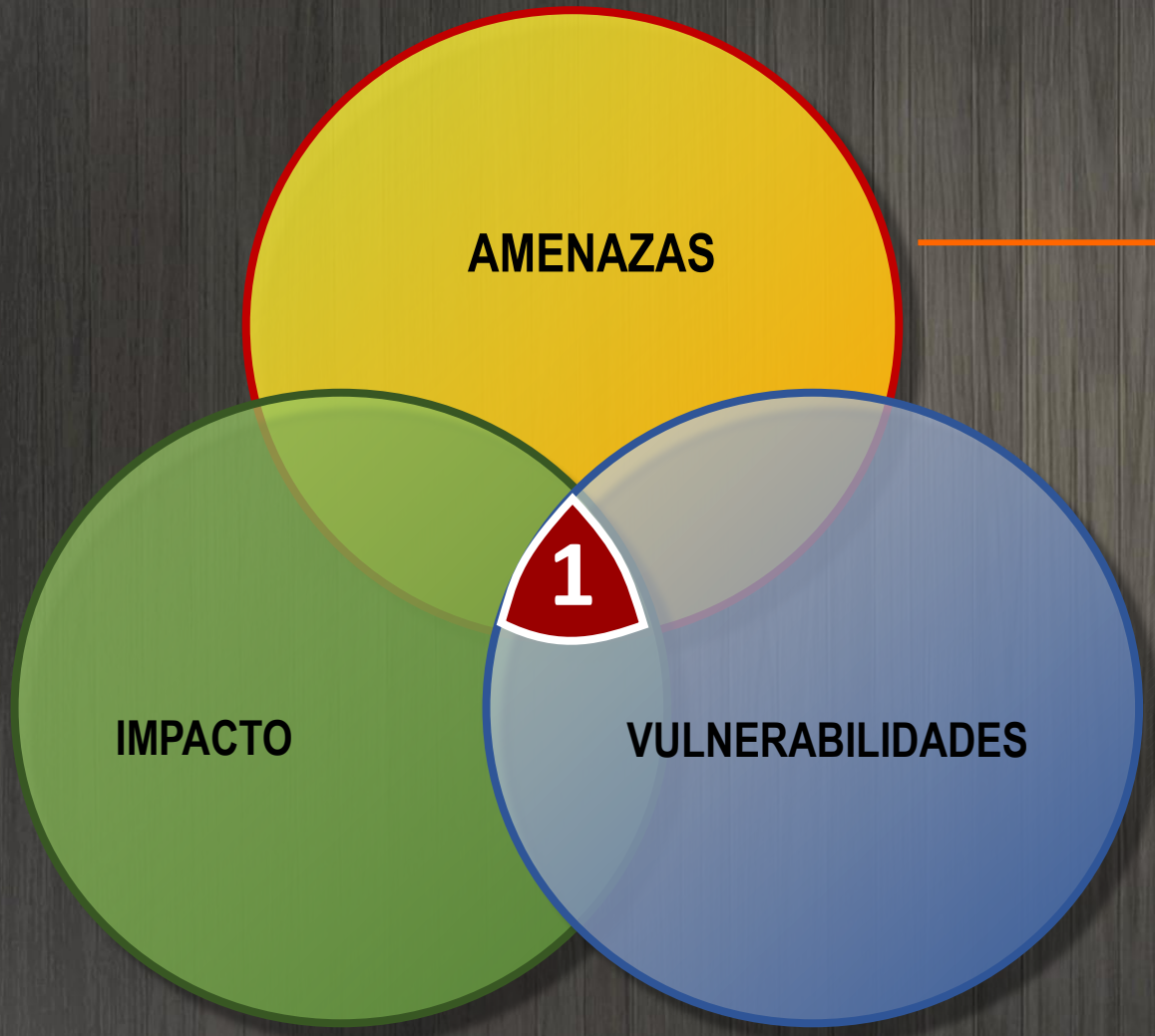
Una autenticación faltante para una función crítica en FortiManager 7.6.0, FortiManager 7.4.0 a 7.4.4, FortiManager 7.2.0 a 7.2.7, FortiManager 7.0.0 a 7.0.12, FortiManager 6.4.0 a 6.4.14, FortiManager 6.2.0 a 6.2.12, Fortinet FortiManager Cloud 7.4.1 a 7.4.4, FortiManager Cloud 7.2.1 a 7.2.7, FortiManager Cloud 7.0.1 a 7.0.12, FortiManager Cloud 6.4.1 a 6.4.7 permite a un atacante ejecutar código o comandos arbitrarios a través de solicitudes especialmente diseñadas.

Métrica

Versión 4.0 de CVSS | Versión 3.x de CVSS | Versión 2.0 de CVSS

CNA: Fortinet, Inc. **Puntuación base:** 9.8 CRÍTICO **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



CAPACIDAD

Habilidad de un adversario para lograr el efecto deseado

OPORTUNIDAD

Momento para hacerlo: cuando pueda o cuando más daño haga

INTENCION

Objetivo o finalidad del adversario

EXPOSICION A LAS AMENAZAS

- Una **VULNERABILIDAD** es una debilidad que se puede explotar para obtener acceso no autorizado a un sistema o red.

- Una **EXPOSICION** se refiere a las condiciones que permiten a los actores de amenazas hacer uso de la vulnerabilidad.

La gestión de vulnerabilidades ya no es sostenible

La forma tradicional de gestionar las vulnerabilidades parte de un enfoque REACTIVO

Busquemos la forma de aplicar remediciones después de haber encontrado una **AMENAZA** y no ante la aparición de una VULNERABILIDAD

INVENTEMOS ALGO NUEVO, CON NUEVAS PREMISAS:

- La ciberseguridad debe ser un proceso ininterrumpido
- Debe adaptarse a las amenazas emergentes y al cambio tecnológico, no en las vulnerabilidades.
- El impacto potencial se determina a través de un cálculo probabilístico
- Debe incluir el uso de tácticas y técnicas ofensivas

CTEM

Continuous Threat Exposure Management

Gestión Continua de la Exposición a Amenazas

- No es una herramienta
- No es un programa
- Es un conjunto de procesos y capacidades
- 2 Fases – 5 Tareas

FASE DE DIAGNOSTICO

- **DELIMITAR** (Scope):

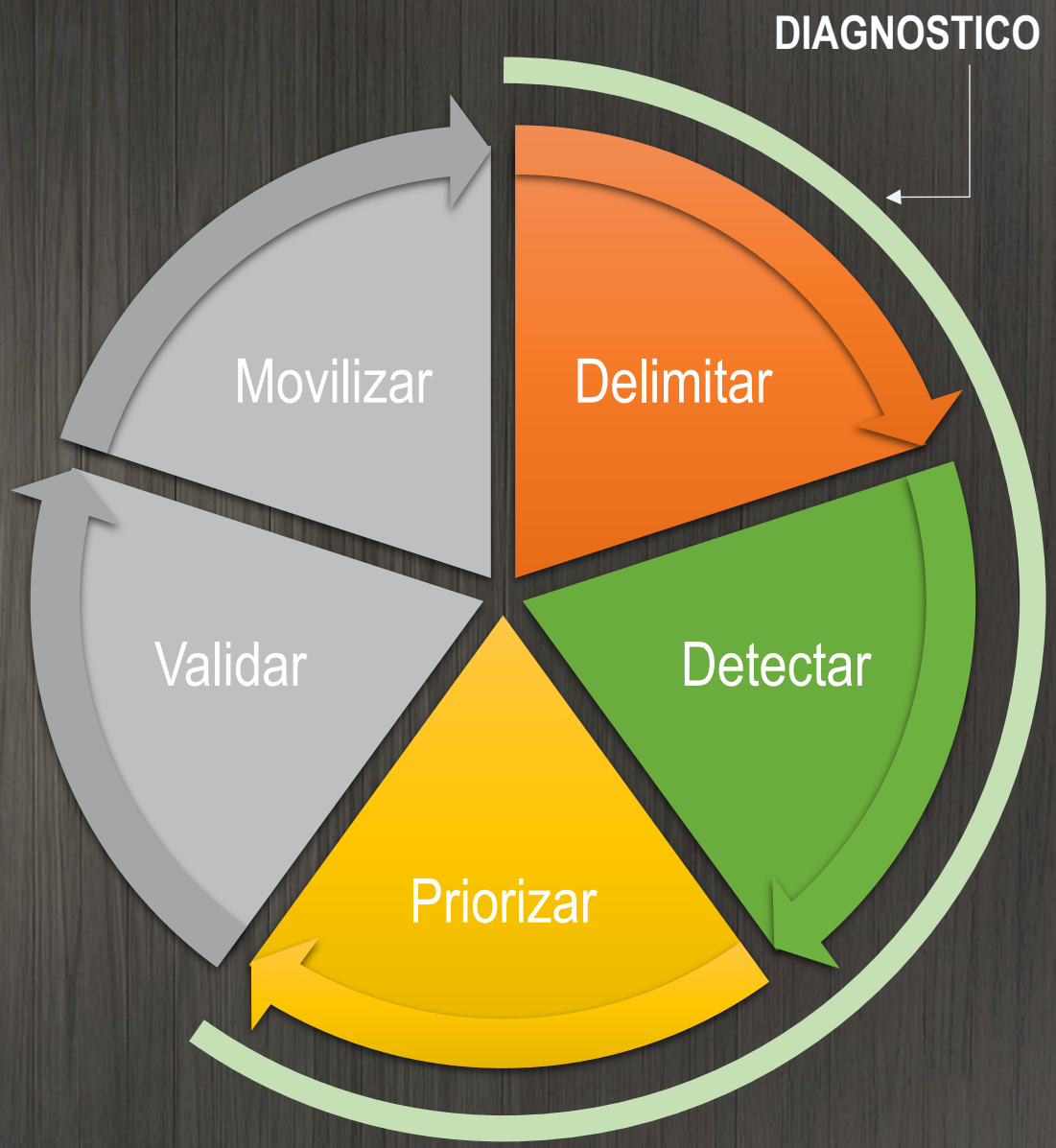
  Se mapea de la superficie de ataque, se enumeran los activos y se evalua su valor operativo, comunicando esta información para que tanto técnicos como ejecutivos entiendan qué activos son críticos.

- **DETECTAR**:

  Centrada en descubrir vulnerabilidades, brechas de seguridad y errores de configuración, **evaluando su riesgo** y asociándolas con sus activos específicos para una priorización eficaz.

- PRIORIZAR:

  Se abordan las brechas de seguridad con mayor probabilidad de ser explotadas, utilizando una perspectiva de adversario.



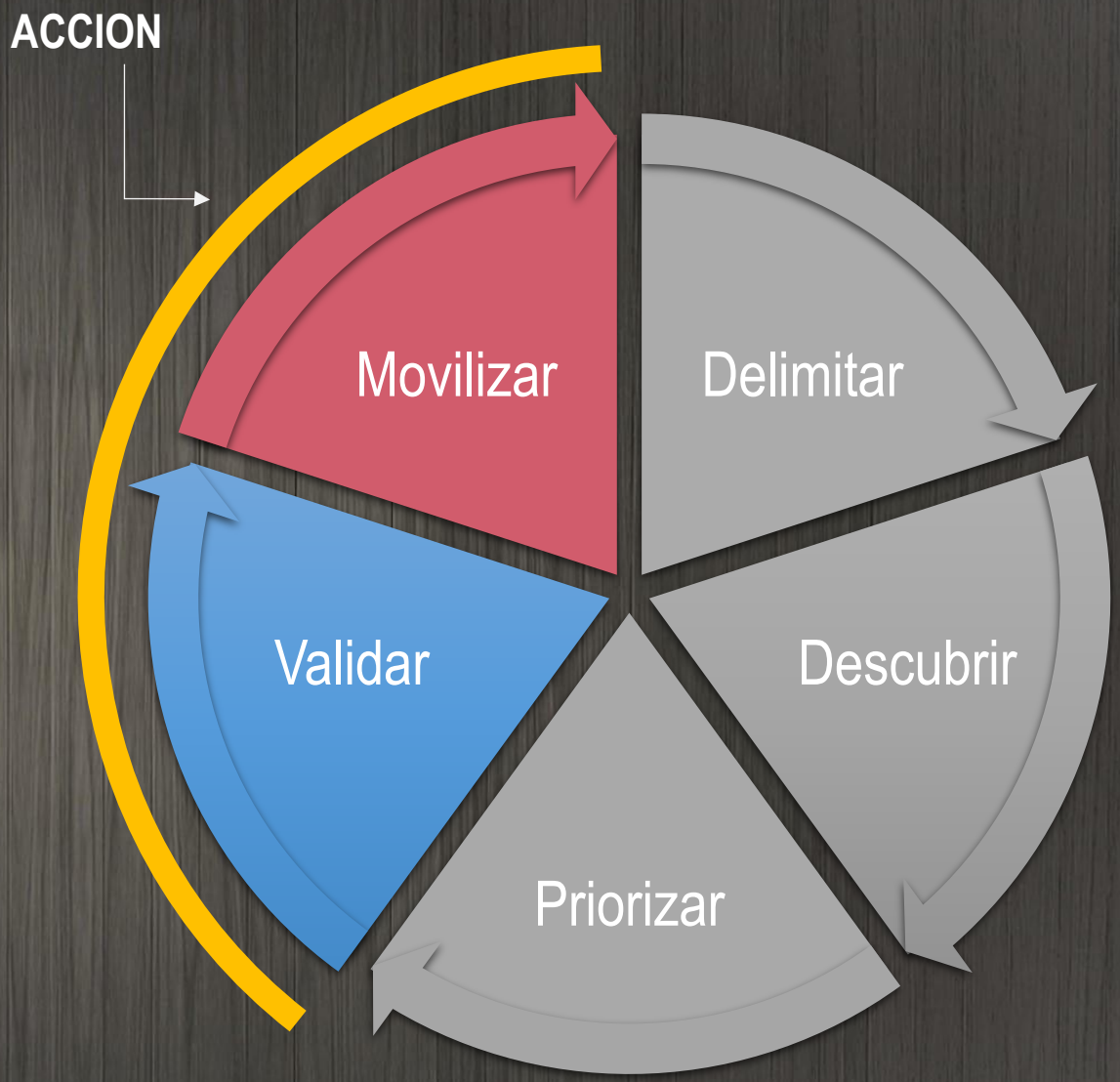
FASE DE ACCION

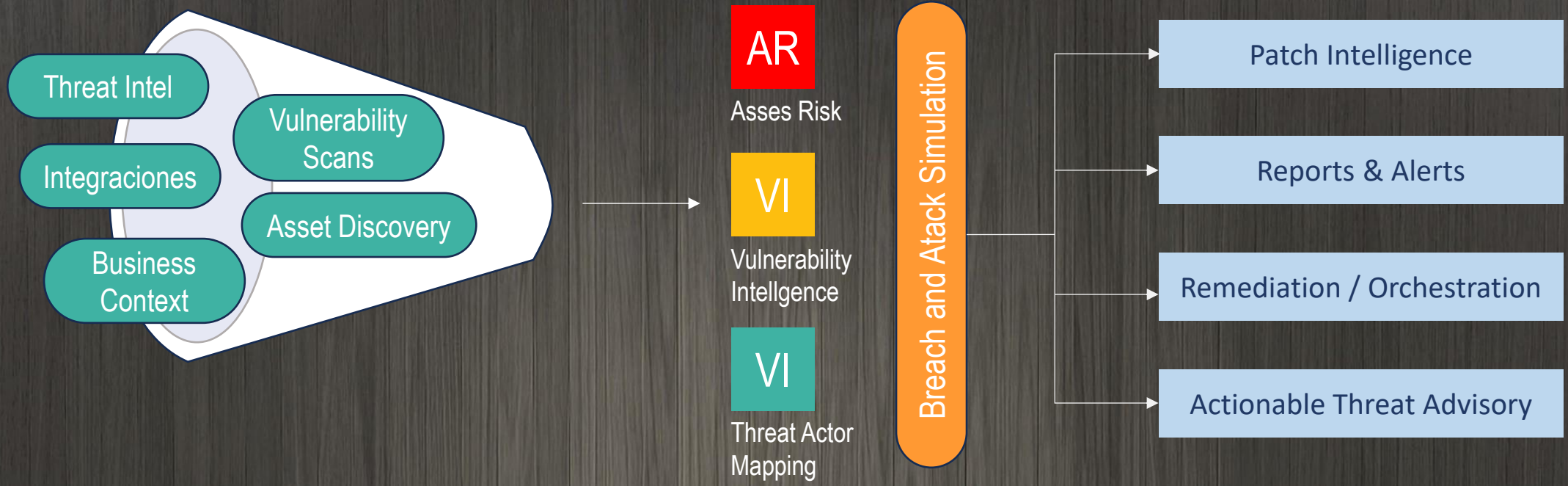
- **VALIDAR**:

  Tiene como objetivo determinar la probabilidad de éxito de un ataque, evaluar el **impacto** potencial del ataque y **comprobar la eficacia** de los sistemas de detección y respuesta existente.

- **MOVILIZAR**:

  Cuando sea necesario, desarrollará e implementará un **programa de remediación** que integre soluciones automáticas y manuales. Este programa se desarrolla en colaboración con los departamentos técnicos y ejecutivos para asegurar que las necesidades operativas y de seguridad estén alineadas.




Threat Intel
Vulnerability Scans
Integraciones
Asset Discovery
Business Context
AR
Asses Risk
VI
Vulnerability Intellgence
VI
Threat Actor Mapping
Breach and Atack Simulation
Patch Intelligence
Reports & Alerts
Remediation / Orchestration
Actionable Threat Advisory
Map Your Assets & Security Environment
Test Your Threats & Prioritize Your TRUE Vulnerabilities
Patch, Alert, Remediate & Report
Prioritize
Enrich
Inform
Drive
Initiate
Validate
Threat Detection and Response
Governance Risk and Compliance (GRC)
Treatment and Security Posture Optimization

¿Cómo pueden las organizaciones medir el éxito de sus programas ciber?

METRICAS PROPUESTAS

1. **Tiempo medio de detección (MTTD):** Tiempo medio para detectar nuevas vulnerabilidades, amenazas o exposiciones en su entorno. Un MTTD más bajo indica una detección más rápida y un programa exitoso.
2. **Tiempo medio de respuesta (MTTR):** Mide el tiempo medio que se tarda en responder y remediar las vulnerabilidades o amenazas identificadas. Un MTTR más bajo indica una respuesta y resolución eficientes.
3. **Tiempo de respuesta a incidentes:** Esta métrica puede ayudar a evaluar la capacidad del programa para gestionar amenazas en tiempo real.
4. **Índice de corrección de vulnerabilidades:** Supervise la tasa a la que se corrigen las vulnerabilidades identificadas. Puede expresarse como porcentaje y si es alto, indicaría una mitigación oportuna.
5. **Reducción del riesgo:** ¿Utiliza sistemas de puntuación de riesgos? Cuantifique la reducción del riesgo asociado a las vulnerabilidades y exposiciones a lo largo del tiempo y compruebe si mejora.
6. **Tasa de falsos positivos:** Una tasa (porcentaje) de falsos positivos baja sugiere que su programa reduce el ruido y se centra en las amenazas auténticas.
7. **Tasa de Cobertura de activos:** Mida el porcentaje de activos de su organización (servidores, puntos finales, aplicaciones) supervisados continuamente por su sistema. Una alta cobertura de activos garantiza una seguridad integral.

CIBER CONSEJOS

- Ninguna organización puede protegerse contra todos los eventos de ciberseguridad.
- El éxito no se basa en la cantidad de vulnerabilidades descubiertas, sino en la profundidad de los análisis
- Comprometámonos a abordar las exposiciones que (más) amenazan a nuestro negocio / empresa.

- Gestionemos las AMENAZAS de ciberseguridad, no los episodios

EMILIO RICO RUIZ

Security Advisor

@Emilio_RR

Emilio Rico Ruiz

https://github.com/3MlioRR

trc


XVIII JORNADAS STIC CCN-CERT
VI JORNADAS DE CIBER_ DEFENSA ESPDEF-CERT
MUCHAS GRACIAS
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
20 ANIVERSARIO
Centro Criptológico Nacional
ccn-cert
centro criptológico nacional
espdef-cert
Mando Conjunto del Ciberespacio
/RootedCON
CIBERDEFENSA ACTIVA
PARA UN MUNDO DIGITAL