Apertar o botão vermelho? Tomada de decisão de acionamento do fluxo emergencial de tratamento de vulnerabilidades em situações de incerteza

—

Leonardo Sardinha Ferreira
Rafael Carduz Rocha
Tiago do Vale Saraiva
Sidney Gonçalves de Almeida

PETROBRAS

TLP:CLEAR

Introdução e Relevância do Tema no Contexto da Segurança Cibernética

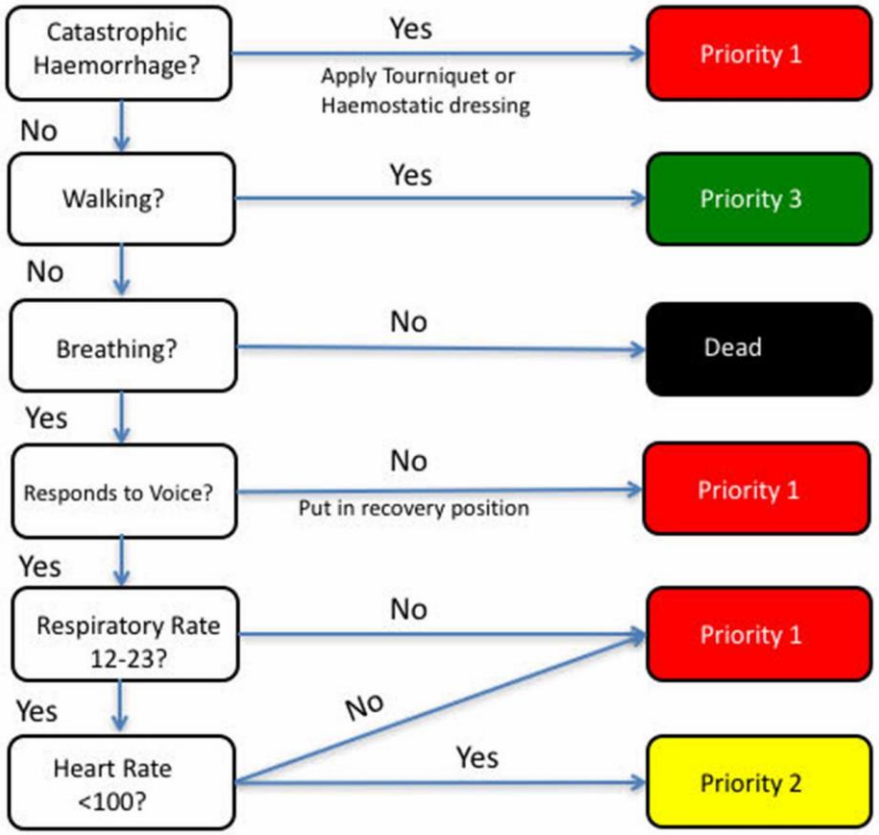
- Mais de 28 mil CVEs em 2023, uma média de 80 por dia.
- Dentre esses apenas uma parcela exigem priorização.
- Dentre esses, uma parcela menor ainda exige uma atenção imediata com ampla mobilização de recursos.
- Essa decisão é feita num ambiente de volatilidade, incerteza, complexidade e ambiguidade
- Muitas lições podem ser extraídas quando observamos como o campo da saúde lida com situações similares

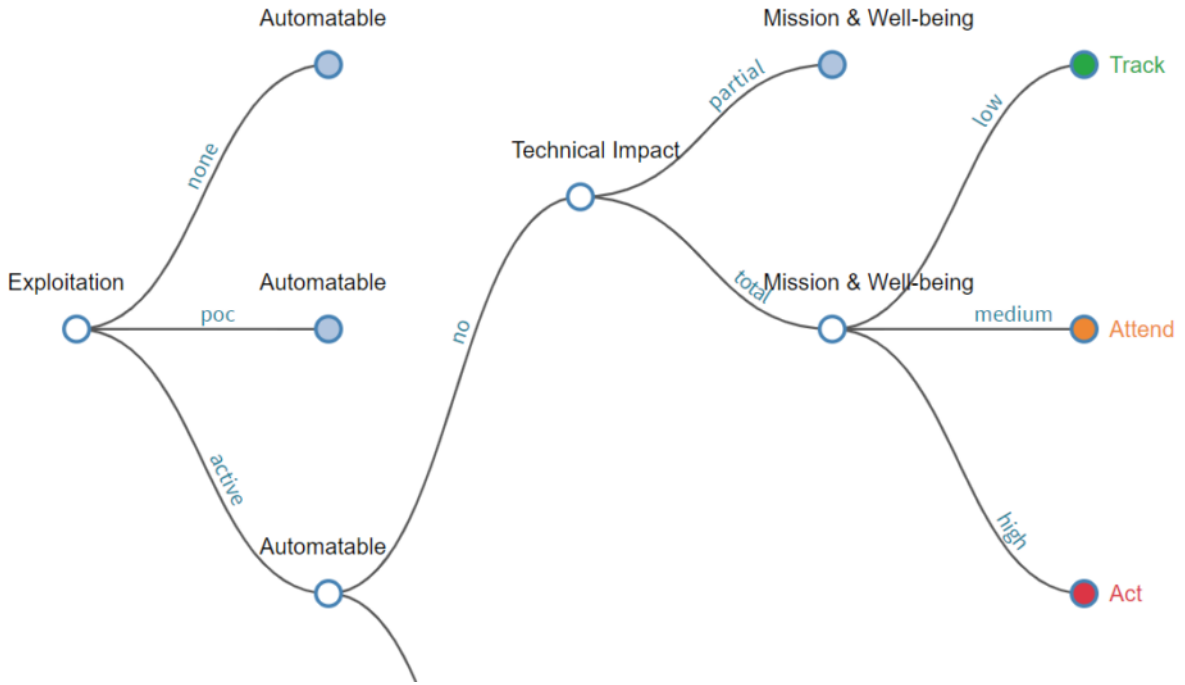
O conceito de triagem

Durante as guerras napoleônicas, Baron Dominique-Jean Larrey, o inventor da ambulância, propôs que os feridos fossem atendidos não mais numa ordem definida por sua patente ou nacionalidade, mas por critérios objetivos de gravidade do ferimento e risco de óbito.

Triagem no conceito da saúde

No contexto da saúde existem múltiplos algoritmos de triagem. O START, por exemplo, é pensado para o atendimento a acidentes com múltiplas vítimas. Podemos observar as semelhanças dele com o SSVC.





TLP:CLEAR

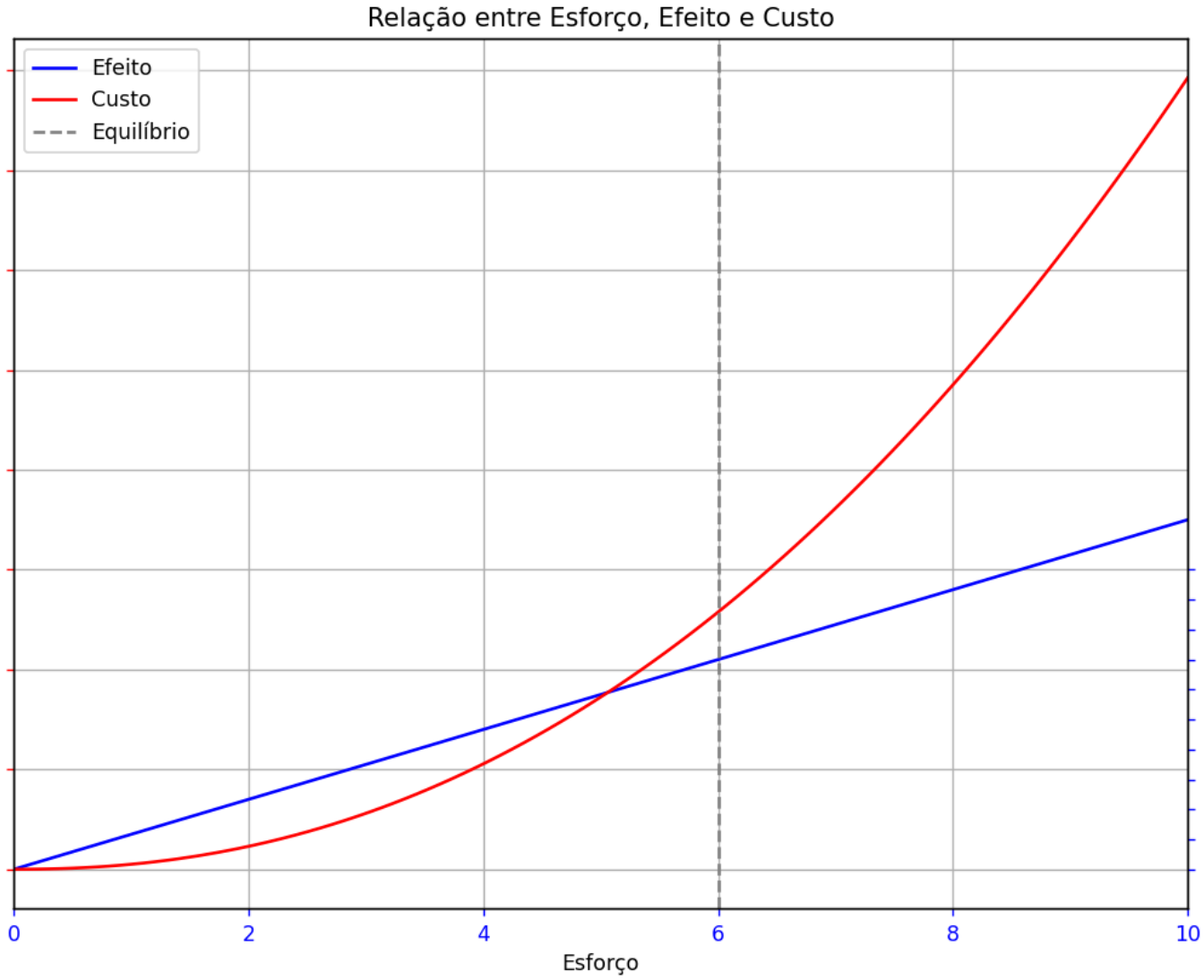
Falsos positivos e falsos negativos e os riscos de sub e supertriagem

No caso da saúde, a subtriagem pode levar a atrasos no diagnóstico e tratamento, o que pode ter consequências graves para o paciente. Já o supertriagem pode levar a um desperdício de recursos e a um aumento do tempo de espera para os pacientes que realmente precisam de atendimento.

Na segurança cibernética, o subtriagem pode levar a ataques bem-sucedidos, o que pode causar danos financeiros e reputacionais às empresas. Já a supertriagem pode levar a falsos positivos, o que pode causar interrupções desnecessárias nos serviços e perda de produtividade.

TLP:CLEAR

Uma questão de custo benefício

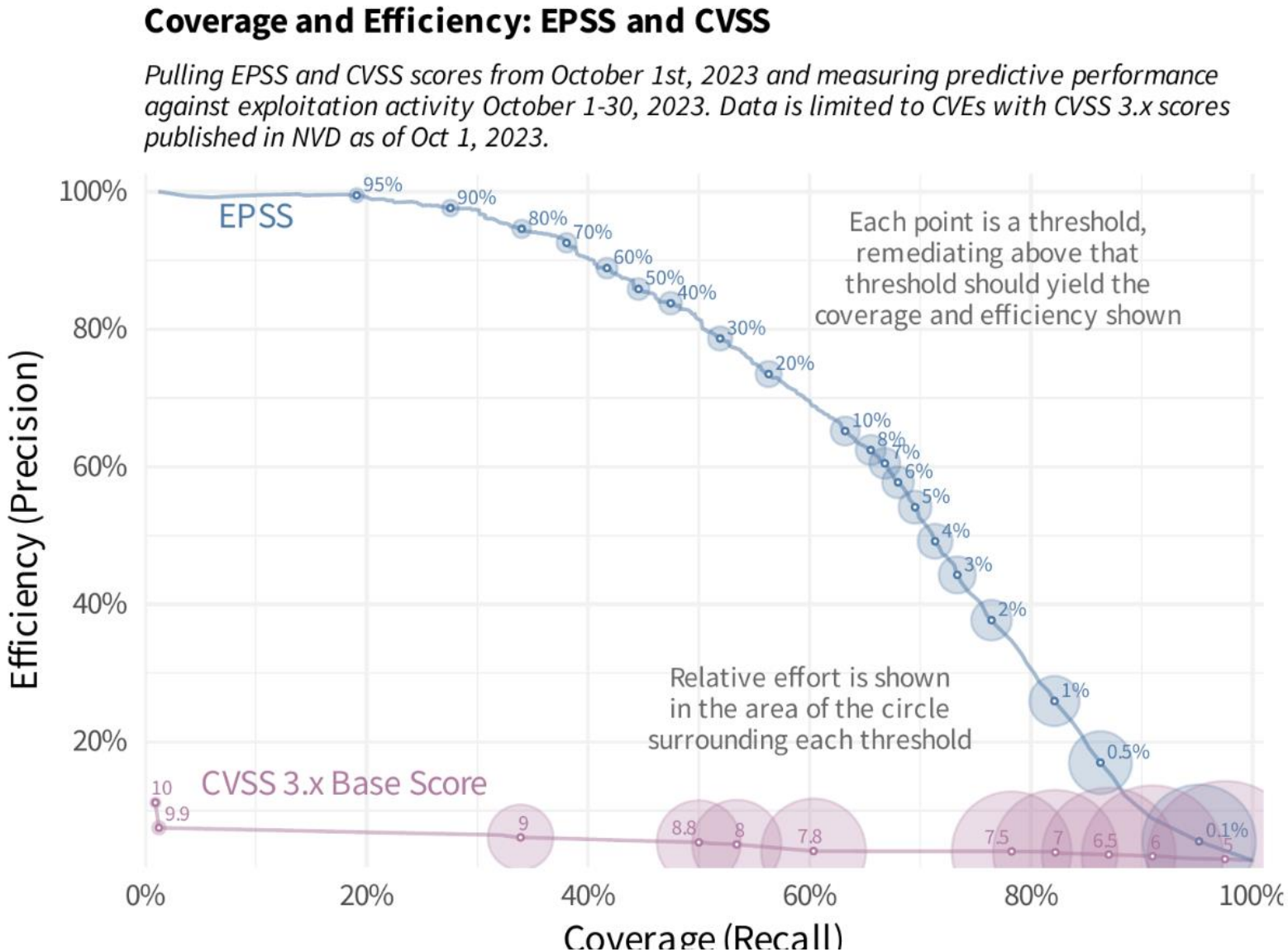


A diferença entre eficácia (capacidade de atingir resultados desejados em condições ideias), efetividade (impacto dos resultados na prática) e eficiência (uso otimizado dos recursos disponíveis é bastante discutida na área da saúde dentro da disciplina da Economia da Saúde.

Também deve ser levada em conta na Gestão de Vulnerabilidades.

TLP:CLEAR

Uma questão de custo benefício



TLP:CLEAR

O Processo emergencial e seu Contexto

Elevado número de tecnologias diferentes

- Sistemas de apoio
- Aplicações de negócio
- Ambientes de pesquisa

Ambientes IT x OT

- Diferentes requisitos
- Complexidade elevada
- Risco da informação X Risco humano

Equipes heterogêneas

- Times de infraestrutura de TIC
- Times de SI (GV, CSIRT, CTI, Riscos, OT)
- Desenvolvedores

Contexto

Elevado número de tecnologias diferentes

+

Ambientes IT x OT

+

Equipes heterogêneas

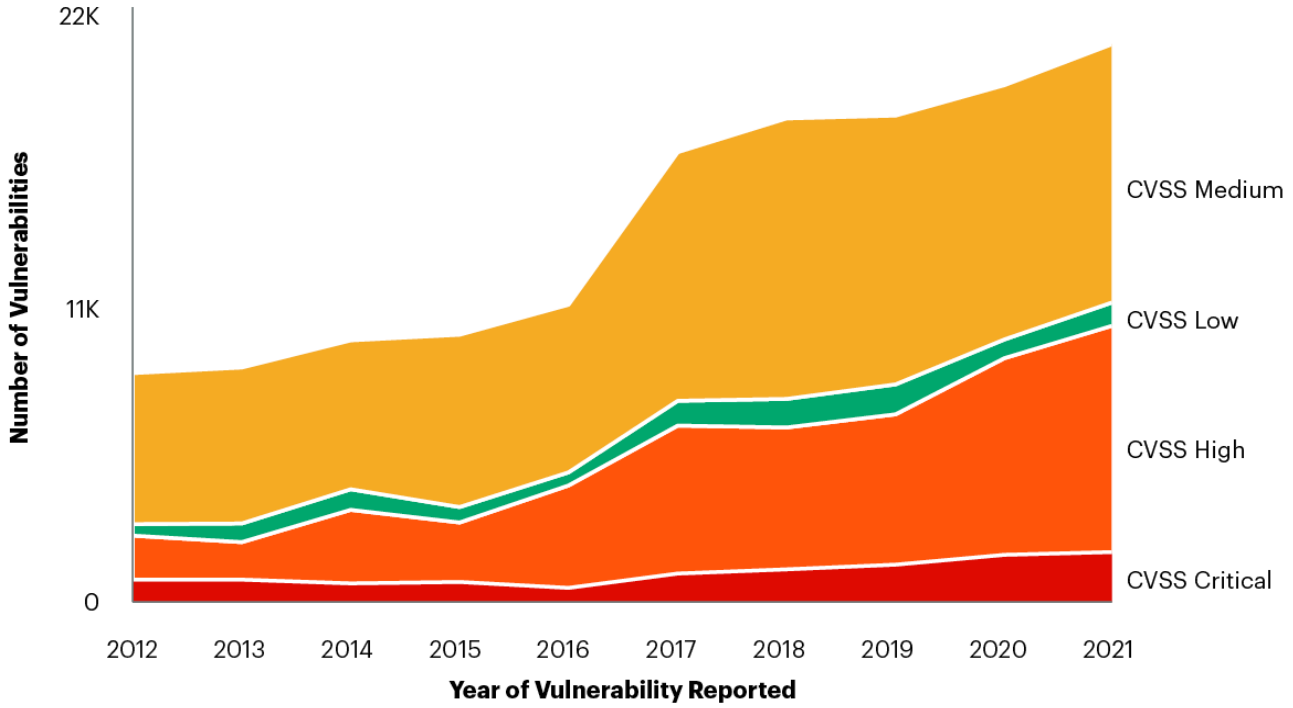
=

Inúmeras vulnerabilidades

TLP:CLEAR

Quantidade de vulnerabilidades reportadas por ano

Vulnerabilities Over The Last Decade Ranked by Severity



CVSS = common vulnerability scoring system

Source: Gartner (data drawn from the IBM X-Force vulnerability database)

777685_C

CVSS V3 Score Distribution

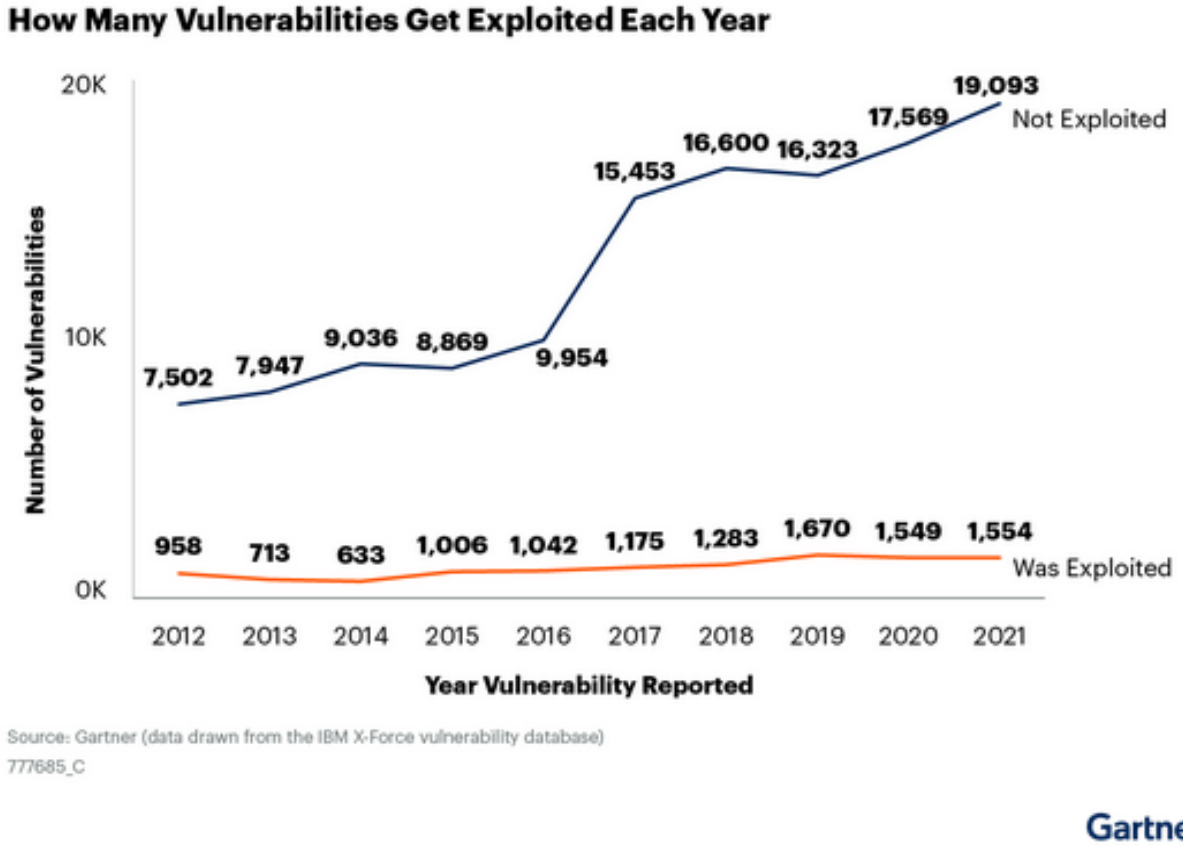
Severity	Number of Vulns
CRITICAL	21675
HIGH	58047
MEDIUM	56803
LOW	2444

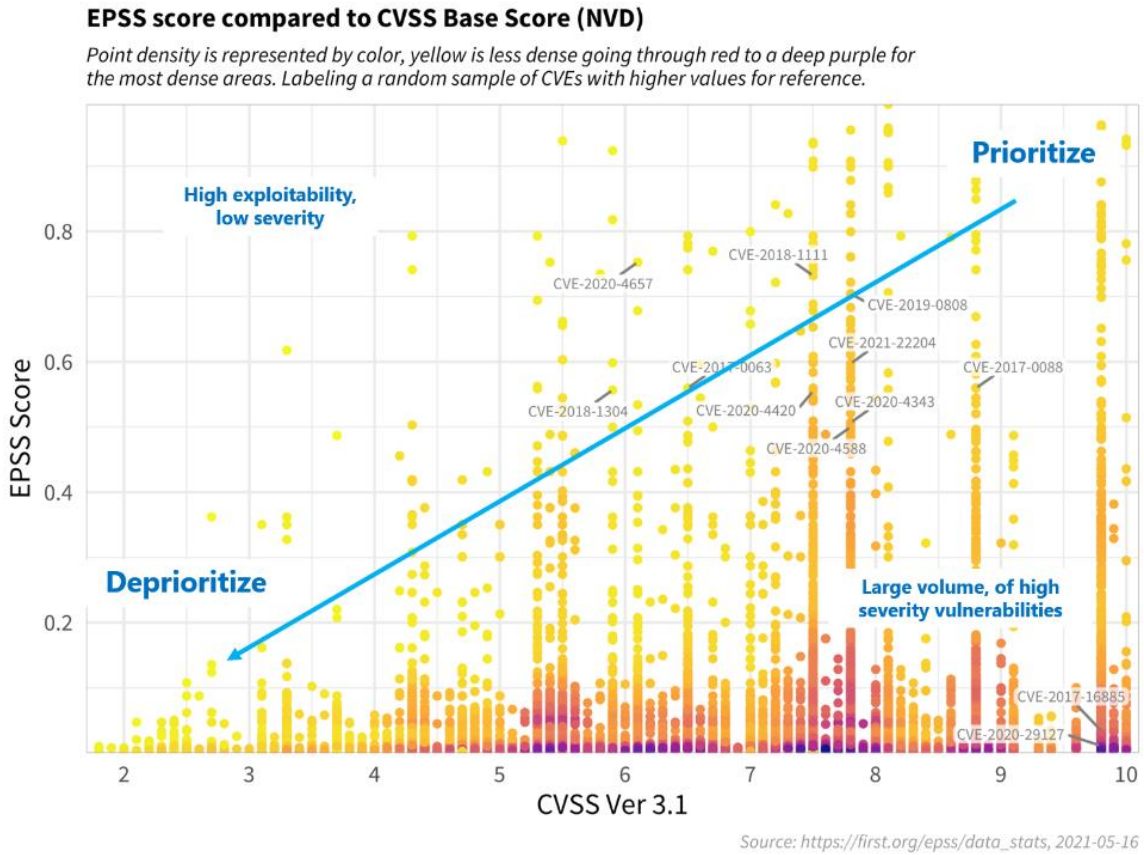
https://nvd.nist.gov/general/nvd-dashboard

Gartner

TLP:CLEAR

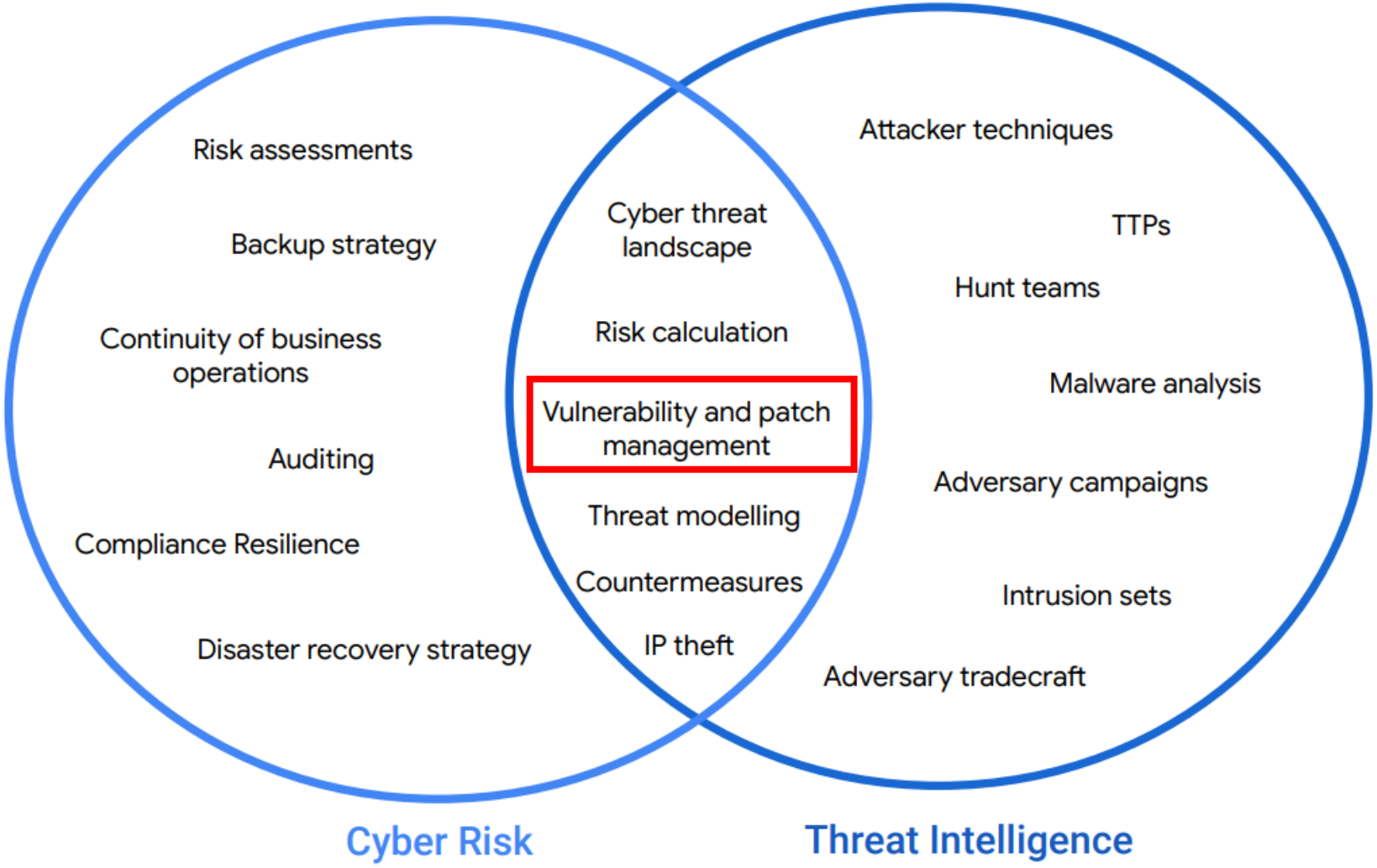
Necessidade de priorização





TLP:CLEAR

O que podemos fazer? (Construindo o entendimento mútuo)

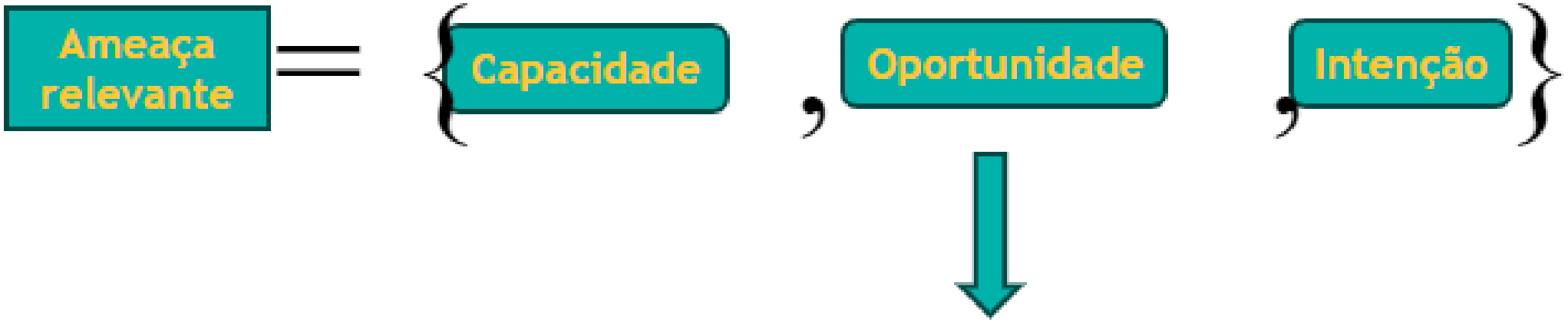


Google Cloud

[Solving CISO Headaches: How to Align CTI and Risk Management (first.org)]

TLP:CLEAR

O que podemos fazer? (Foco de ação)



Das três variáveis que influenciam no sucesso de uma ameaça relevante, temos controle apenas de uma!

Menos vulnerabilidades = Menor exposição = Menos Oportunidades

Solving CISO Headaches: How to Align CTI and Risk Management (first.org) - **Adaptado**

TLP:CLEAR

Referências - boas práticas / frameworks

Gartner

FORRESTER®

NIST

NATIONAL VULNERABILITY DATABASE
NVD

Cybersecurity Framework 2.0

VPR
VULNERABILITY PRIORITY RATING
tenable network security

FIRST

CSIRT Services Framework

EPSS
Exploit Prediction Scoring System

International Organization for Standardization
ISO
27000

OPEN THREAT EXCHANGE

CISA
Known Exploited Vulnerabilities Catalog

CVE
cve.mitre.org

CIRCL
CVE Search

TLP:CLEAR

NIST Cybersecurity Framework v2.0 - Identify (Risk Assessment)

ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded

ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources

ID.RA-03: Internal and external threats to the organization are identified and recorded

ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded

ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization

ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated

ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked

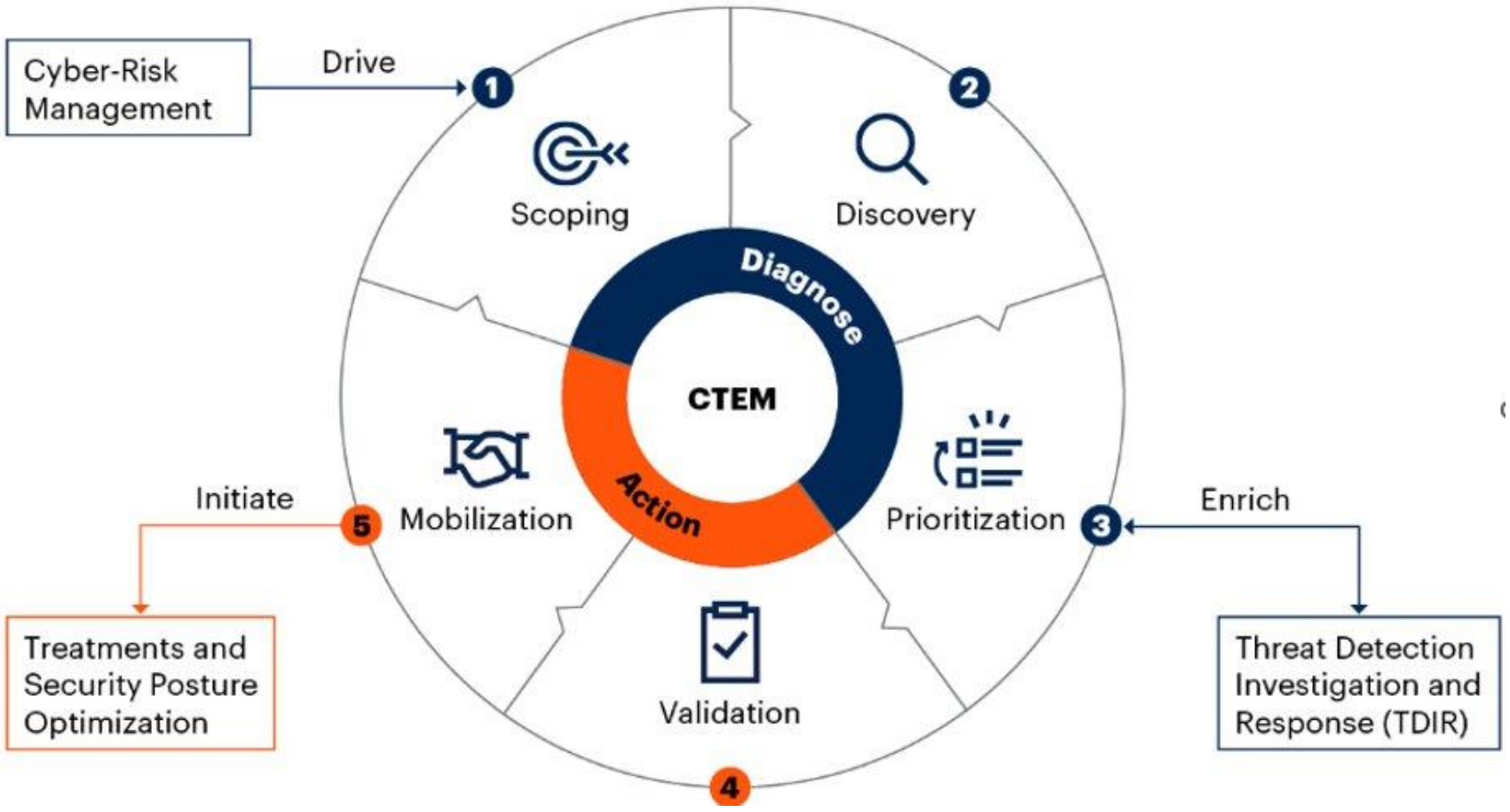
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established

ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use

ID.RA-10: Critical suppliers are assessed prior to acquisition

TLP:CLEAR

Gartner CTEM - Continuous Threat Exposure Management



Um programa integrado e iterativo para priorizar tratamentos adequadamente, de forma continua, para reduzir riscos, aperfeiçoando a postura de segurança.

Objetivo: Fornecer um direcionamento de remediação e melhorias de segurança, acionáveis e compreensível para executivos de negócios

TLP:CLEAR

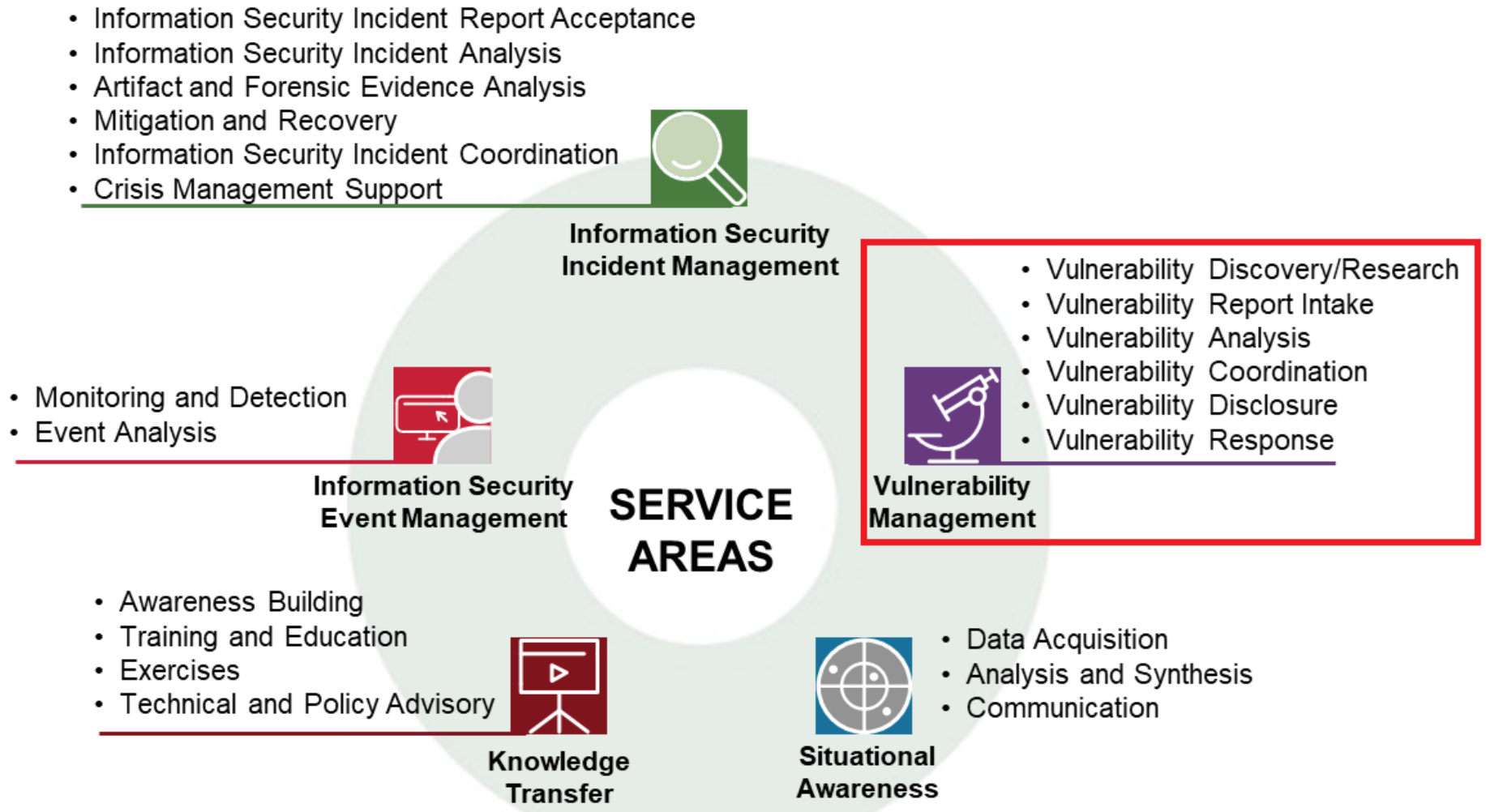
Gartner Top Five Recommendations for Vulnerability Management

		Recommendations
1	 **Discover and Classify Assets Continuously**	✓ Integrate Vulnerability Management With Asset Discovery and Management Program
2	 **Scan for Vulnerabilities at the Optimal Frequency**	✓ Remain In Sync With Patch Management Operations
3	 **Prioritize Vulnerability Remediation**	✓ Enrich Vulnerability Findings With Asset Context, Including Criticality ✓ Correlate Findings With Active Threats
4	 **Manage Exceptions**	✓ Register and Track Patch Exceptions ✓ Employ and Track Compensating Controls
5	 **Implement Actionable Metrics**	✓ Collect and Report Meaningful Metrics to Convey Risk and Promote Resourcing

Source: Gartner
775767_C

TLP:CLEAR

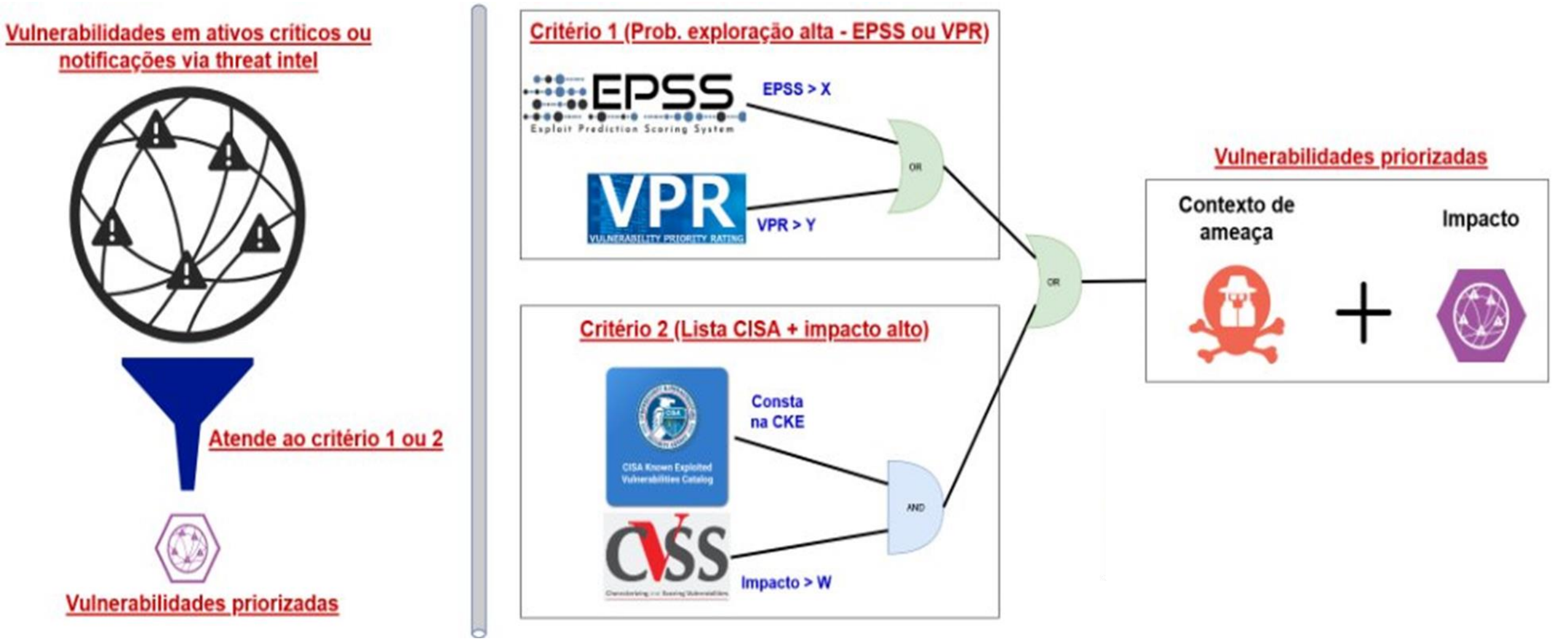
FIRST CSIRT Services Framework 2.1 - Vulnerability Management Service Area



Ex.: Um CSIRT pode focar na descoberta e divulgação sem esforços diretos de coordenação ou resposta.

TLP:CLEAR

Como fazemos? (Exemplo de Triagem Automatizada - pré-emergencial)



TLP:CLEAR

Onde a IA pode ajudar o analista na tomada de decisão ? (motivação)

Diversidade de informações sobre vulnerabilidades

- Como erradicar?
- É possível algum controle compensatório?
- Em quais cenários é explorável?
- Quais aplicações afetadas?
- Qual possível impacto?
- Etc...

Conhecimento heterogêneo

- Equipes de infraestrutura da TIC
- Equipes de GV e CSIRT da SI
- Equipes de riscos
- Visão técnica x gerencial

TLP:CLEAR

Já existe solução para essa finalidade?

Soluções de Mercado

- Uso de IA Generativa integrado com diversas soluções de segurança cibernética (Ex. Risk Management, EDR, Vulnerability Management)

Limitações

- Exige o conhecimento prévio de todo o parque
- Nem sempre utilizam todas os recursos disponíveis em fontes de referência (Ex.: EPSS, CISA, CTI, etc...)
- Resultados limitados para casos de uso específicos (Ex.: Riscos, Resposta a incidentes, GV, etc...)

Benefícios / ganhos da solução com IA

Benefícios para SI

- Maximiza o valor do Datalake de SI;
- Reduz o tempo de análise e remediação/mitigação de vulnerabilidades;
- Facilita a elaboração de relatórios técnicos, gerenciais e de riscos sobre vulnerabilidades especificas.

Benefícios para empresa

- Menor tempo de exposição em função de vulnerabilidades não tratadas
  - Tratamento mais efetivo, em menor tempo.

O que foi feito até o momento? (Protótipo VARIA - Vulnerabilidades, Ameaças e Riscos com Inteligência Aplicada)

Protótipo

- Testes de interface web com Gradio e Streamlite
- Uso da API aberta do GPT 3.5 turbo (analise apenas de dados públicos)
- Engenharia de prompts com instruções para atuar como especialista em relatórios técnicos e gerenciais sobre vulnerabilidades
- Conexão básica com o Datalake para identificação de superfície exposta considerando diferentes bases de infraestrutura, estações e aplicações.

TLP:CLEAR

O que foi feito até o momento? (Protótipo VARIA - Uso interno) Diagnóstico e Risco

Claro, vamos lá:

1 - Diagnóstico:
A vulnerabilidade CVE-2022-41915 afeta a biblioteca Netty, que é um framework de aplicação de rede assíncrona orientada a eventos. A vulnerabilidade ocorre quando a função `DefaultHttpHeaders.set(CharSequence, Iterator<?>)` é chamada com um iterador de valores, sem validação dos valores do cabeçalho, permitindo que valores maliciosos no iterador executem HTTP Response Splitting.

2 - Riscos:
O impacto dessa vulnerabilidade é considerado médio, com uma pontuação CVSS de 6.5. O vetor CVSS é AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N, o que significa que um atacante remoto não autenticado pode explorar a vulnerabilidade com baixa complexidade, sem interação do usuário, para comprometer a integridade e confidencialidade dos dados. O EPSS do CVE-2022-41915 é de 0.00065 (0.065%), o que indica uma baixa probabilidade de exploração nos próximos 30 dias. No entanto, é importante lembrar que essa pontuação pode mudar com o tempo.

TLP:CLEAR

O que foi feito até o momento? (Protótipo VARIA - Uso interno) Mitigações, Recomendação e Referências

3 - Possíveis mitigações:
A correção para essa vulnerabilidade está disponível na versão 4.1.86.Final do Netty. Caso não seja possível atualizar o ambiente, uma possível mitigação é alterar a chamada `DefaultHttpHeaders.set(CharSequence, Iterator<?>)` para uma chamada `remove()` e, em seguida, chamar `add()` em um loop sobre o iterador de valores.

4 - Recomendação:
Recomenda-se que os usuários afetados atualizem para a versão mais recente do Netty o mais rápido possível. Caso não seja possível atualizar, a mitigação mencionada acima pode ser aplicada.

5 - Referências:
- https://security.netapp.com/advisory/ntap-20230113-0004/
- https://github.com/netty/netty/security/advisories/GHSA-hh82-3pmq-7frp
- https://www.debian.org/security/2023/dsa-5316

O que foi feito até o momento? (Protótipo VARIA - Uso interno)
Exposição e Ameaças

Ativos de infraestrutura (servidores e elementos de rede) expostos a vulnerabilidade informada

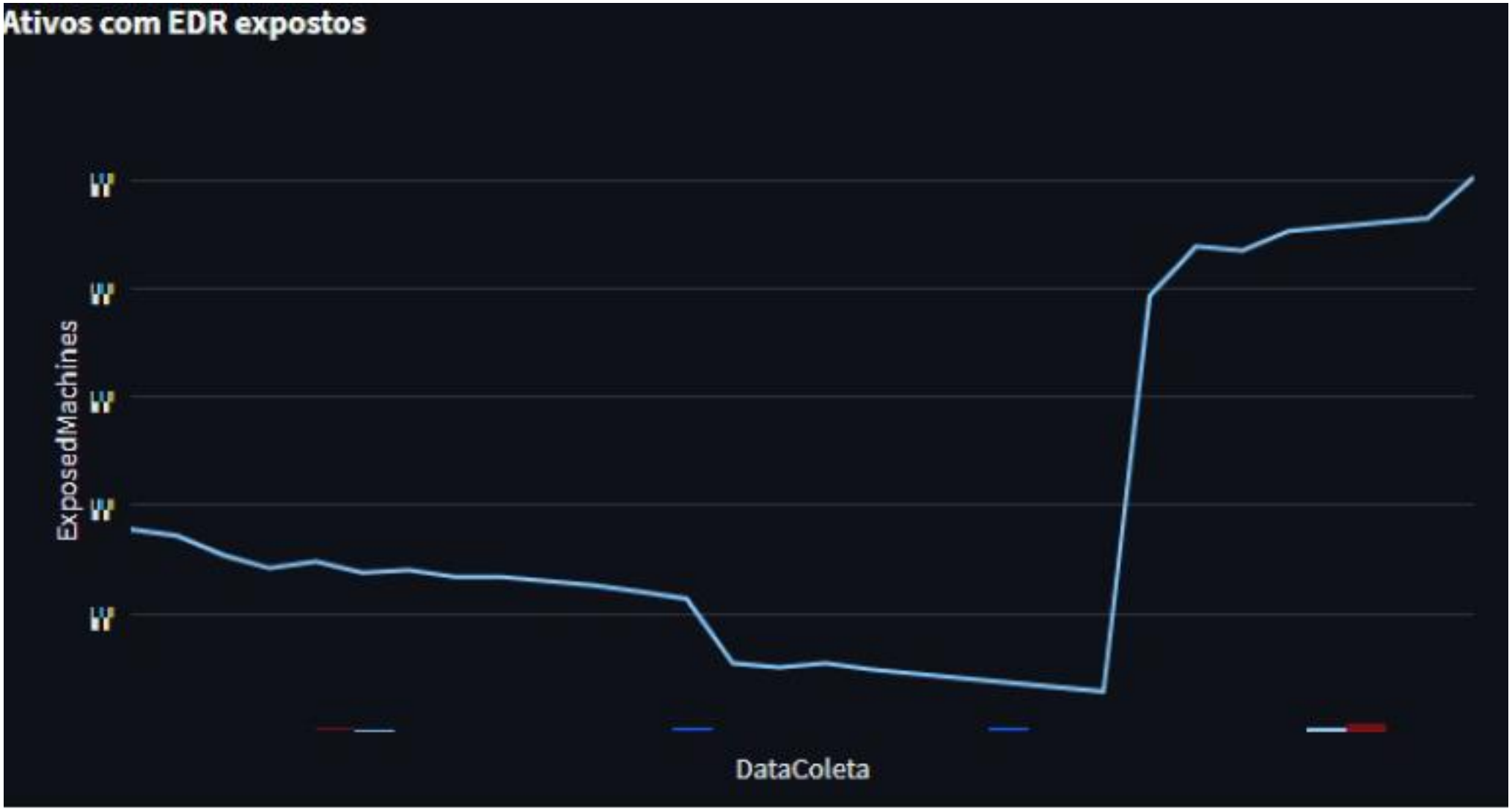
Categoria	Quantidade
	
	
	

Ameaças de acordo Alienvault OTX

Itens de ameaça	Tags
Bumblebee: New Loader Rapidly Assuming Central Position in Cybe	cobalt strike, bumblebee, avoslocker, ac
Vice Society: Profiling a Persistent Threat to the Education Sector	vice society, hellokitty, onionmail, printı
Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tool	black basta, fin7, ransomware, printnigh
#StopRansomware: Vice Society	Ransomware, Cobalt Strike, Powershell En
Kimsuky Group's APT Attacks	Kimsuky, spearphishing, Meterpreter, VI
Russian State-Sponsored Cyber Actors Gain Network Access by Explo	CISA, geopolitical conflict, FBI, PrintNigh
Conti Ransomware | CISA	Conti, TrickBot, IcedID

TLP:CLEAR

O que foi feito até o momento? (Protótipo VARIA - Uso interno)
Exposição - Evolução EDR



TLP:CLEAR

O que foi feito até o momento? (Protótipo VARIA - Uso interno)
Exposição - Aplicações de negócio

TLP:CLEAR

O que foi feito até o momento? (Protótipo VARIA - Uso externo)

VARIA - Vulnerabilidades, Ameaças e Riscos com Inteligência Aplicada

Versão de testes

Sugestões e críticas são bem vindas :-)

Digite um CVE ou termo(s) relacionado(s) a vulnerabilidade de interesse

CVE-YYYY-XXXXX

Analisar

Parâmetros de análise

Tipo de Analise

Categorias de análise

- Analise Padrao
- Analise Tecnica
- Analise Executiva

Criterios de ameaça

Criterios relacionados ao contexto de ameaça.

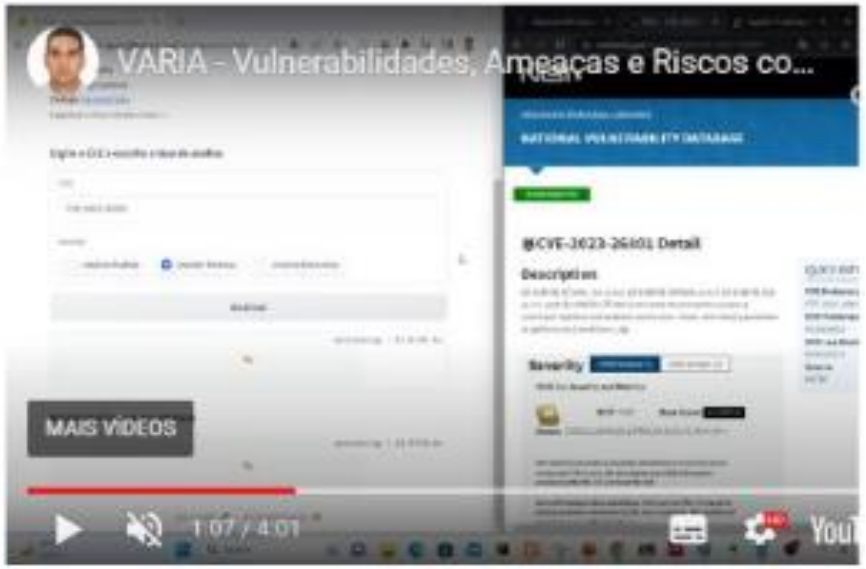
- CISA KEV
- EPSS > 0.8
- Mídia
- Exploit

Criterio de acesso/comunicação

Nível de acesso necessário para comunicação

Tanto faz (indiferente)

Apresentação



TLP:CLEAR

Triagem Manual

Conhecimento tácito é aquele que a pessoa adquiriu ao longo da vida, pela experiência. Geralmente é difícil de ser formalizado ou explicado a outra pessoa, pois é subjetivo e inerente às habilidades de uma pessoa.

O feeling do analista que não é passível de ser exteriorizado ou codificado. Modelos de linguagem e machine learning podem capturar padrões de comportamento e linguagem, mas estão restritos a extrapolações dos seus datasets.

Exemplo: Às vezes uma desconfiança em uma informação oriunda de alguma ferramenta leva a uma confirmação e a descoberta do uso de uma tecnologia não homologada nem catalogada no parque.

TLP:CLEAR

Temos essa vulnerabilidade no parque?

Essa pergunta dificilmente pode ser inteiramente automatizada.

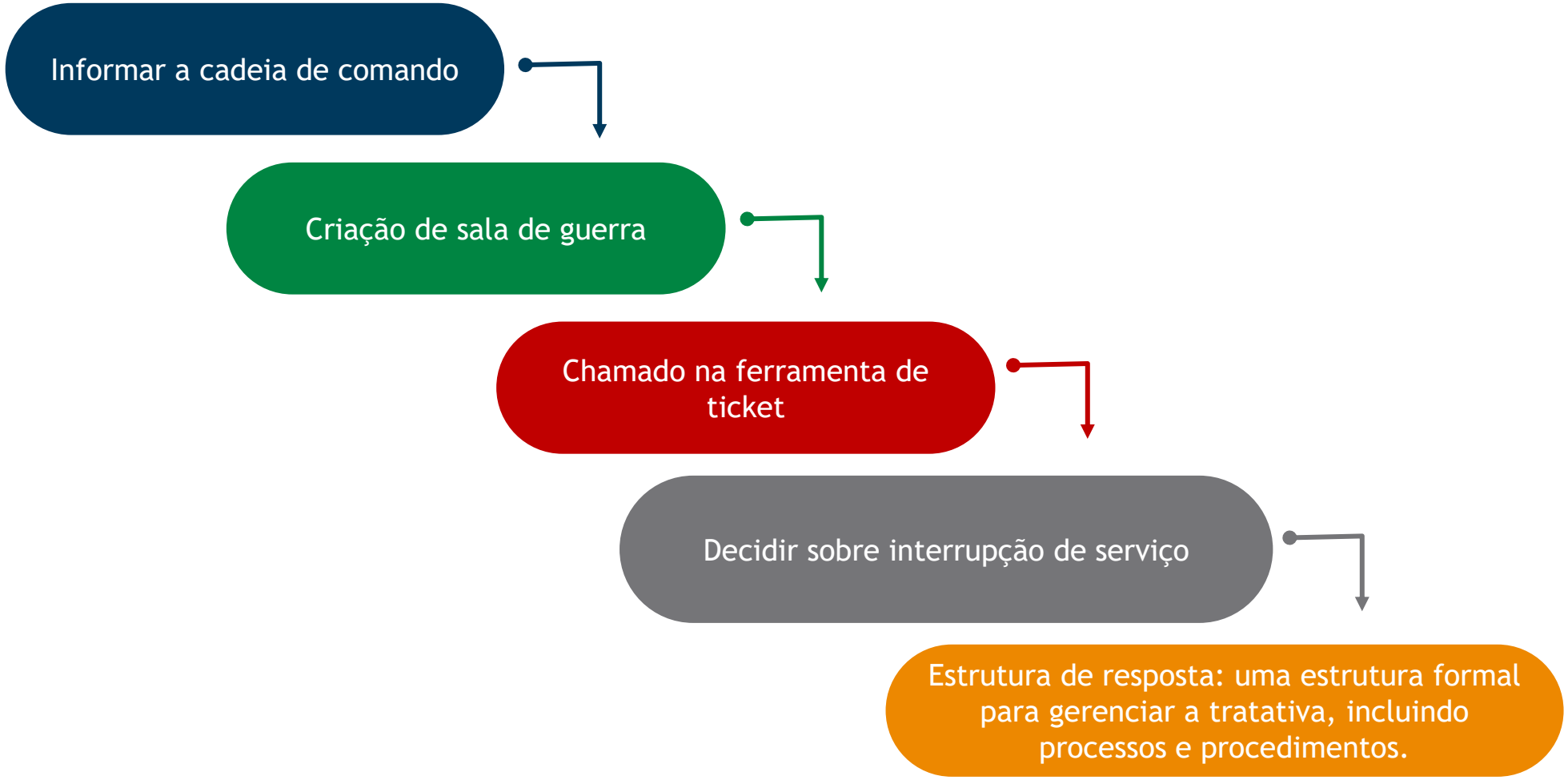
Ativos

- **Complexidade dos BDGCs:** Base de Dados de Gestão de Configuração (BDGCs) são frequentemente incompletas e nem todas as informações são catalogadas.
- **Dispersão dos Ativos:** Informações podem estar espalhadas por várias ferramentas como EDR, ferramentas de varredura, entre outras.
- **Reconciliar Ativos:** Soluções de mercado e scripts podem ser usados para consolidar informações de ativos dispersos.

Detecções

- **Fontes de Detecção:** Uso de varreduras, EDRs e pesquisa para identificar vulnerabilidades.
- **Tempo de Detecção:** Atrasos na publicação de scripts ou assinaturas de detecção são comuns.
- **Monitoramento Contínuo:** Importância de manter monitoramento prolongado devido a fatores variantes como EPSS e disponibilidade de exploits.

Apertamos o botão: Que comecem as tratativas



TLP:CLEAR

Acompanhar o tratamento e o pós tratamento

- **Tratamento**

  Nem sempre Patch é a melhor opção.

  Importância do hardening.

  Considerar controles mitigatórios.

  Gestão de Riscos Aceitos.

- **Pós tratamento**

Ter ciência de que a vulnerabilidade pode ressurgir no parque (Ex. GPOs).

Investigar máquinas que nunca recebem o patch.

Novos problemas que vão sendo revelados.

TLP:CLEAR

Vulnerabilidades desclassificadas: como aproveitá-las?

- A grande maioria dos casos serão desclassificados, porém não necessariamente as detecções e informações levantadas devem ser deixadas de lado.
- Vulnerabilidades alertadas pelos serviços de Threat intel, ou com alto EPSS e que podem ser exploradas por Worms e Ransomwares que se espalham com facilidade, devem ser acompanhadas mesmo quando não estão nos ativos prioritários (joias da coroa).

Obrigado!

TLP:CLEAR