



A glitch in the Matrix - Attack as Déjà vu

Manoelito Filho

29 de agosto de 2025

Mais apoiadores:



00 Introduction

01 Security Operations Center (SOC)

02 Frameworks

03 Threat Scenarios

04 Conclusion and extras

05 References

Introduction

Who am I, motivation and scope



\$ whoami





Motivation





Motivation





Scope

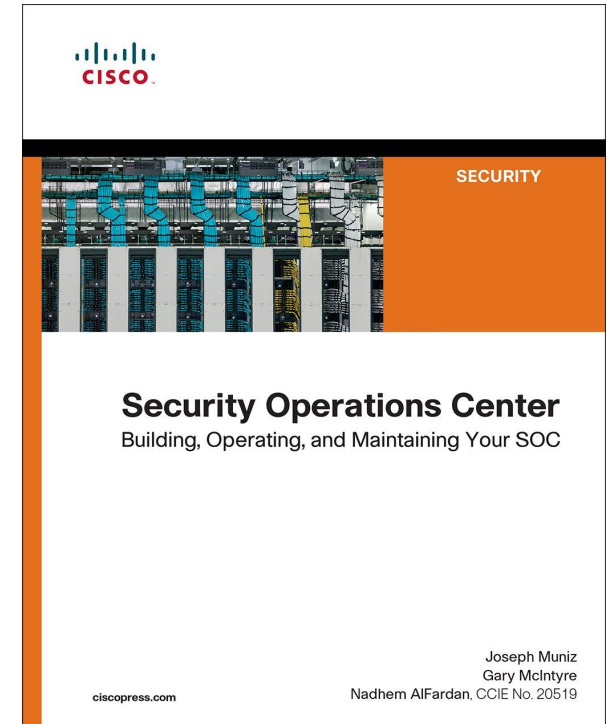
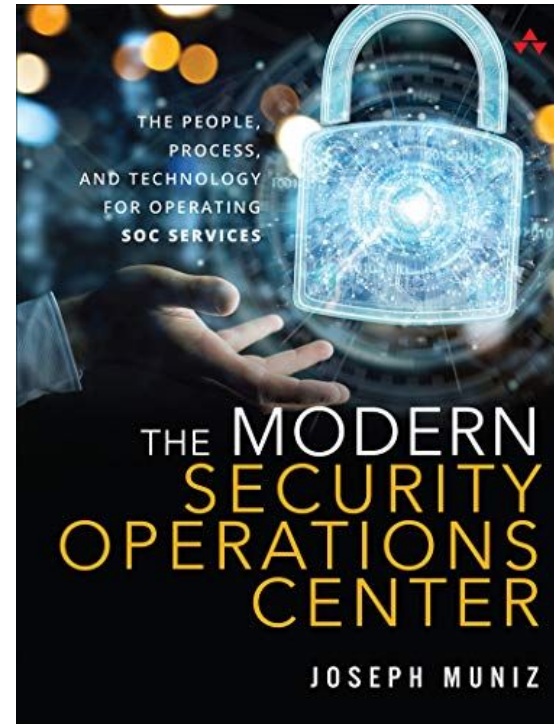
MITRE
ATT&CK™

NIST
National Institute of
Standards and Technology

CSA cloud
security
allianceSM



CISA
CYBER+INFRASTRUCTURE



Security Operations Center (SOC)

What is a SOC?



SOC, what is it?





SOC, what is it?

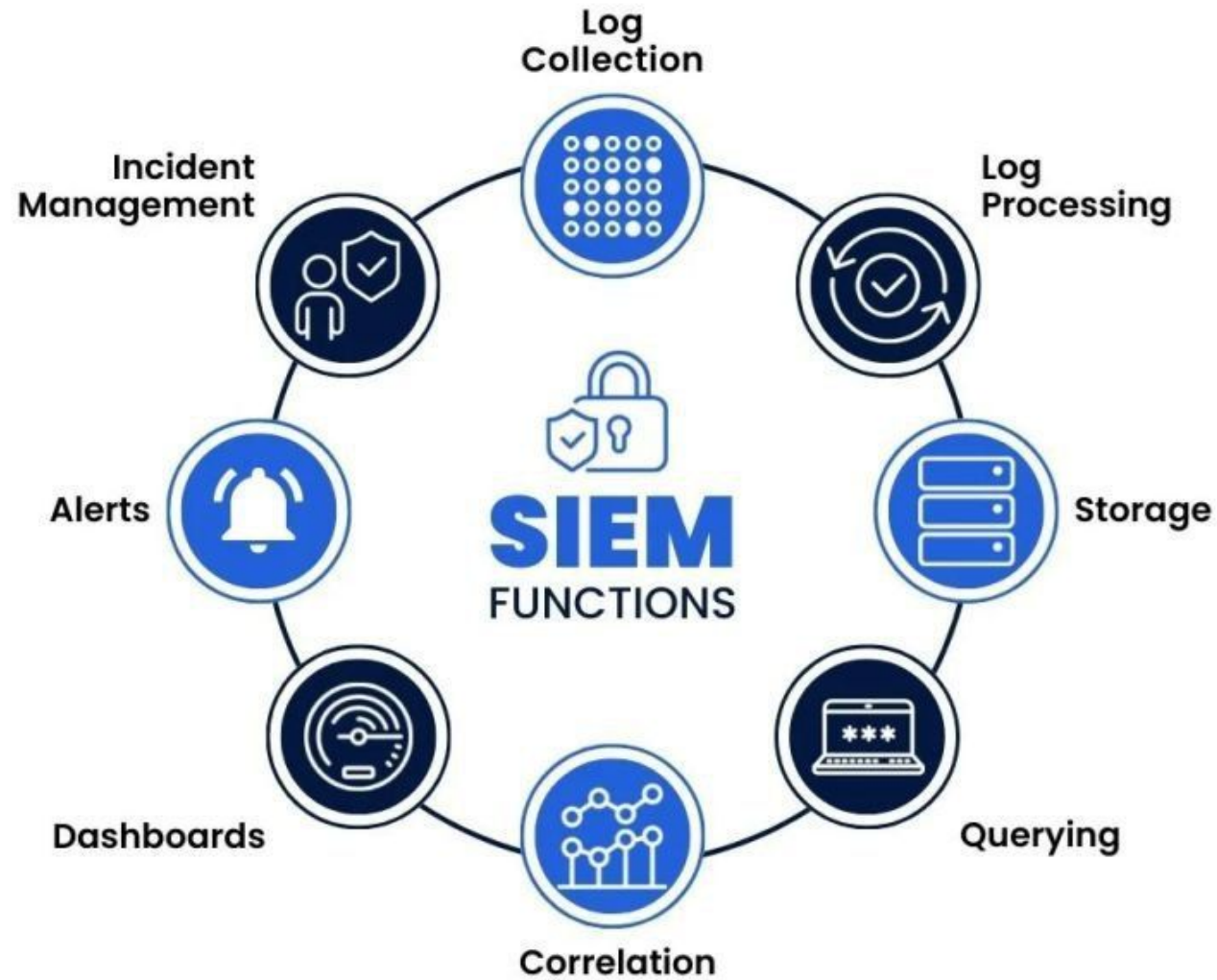
“SOC is not SIEM”

by someone smart

SIEM: Security Information and Event Management



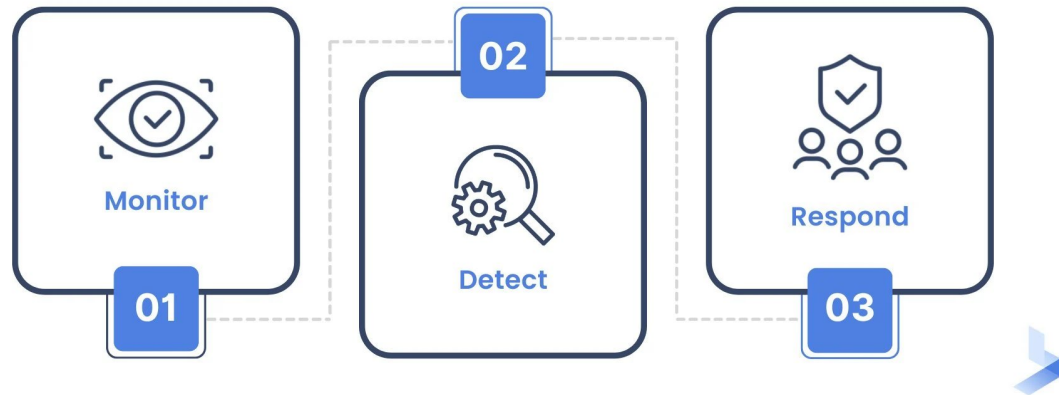
SOC, what is it?



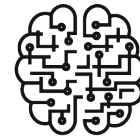


SOC, more than MDR

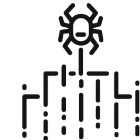
THREE STEPS OF MANAGED DETECTION AND RESPONSE



Detection Engineering



Threat Intelligence



Threat Hunting



Digital Forensics



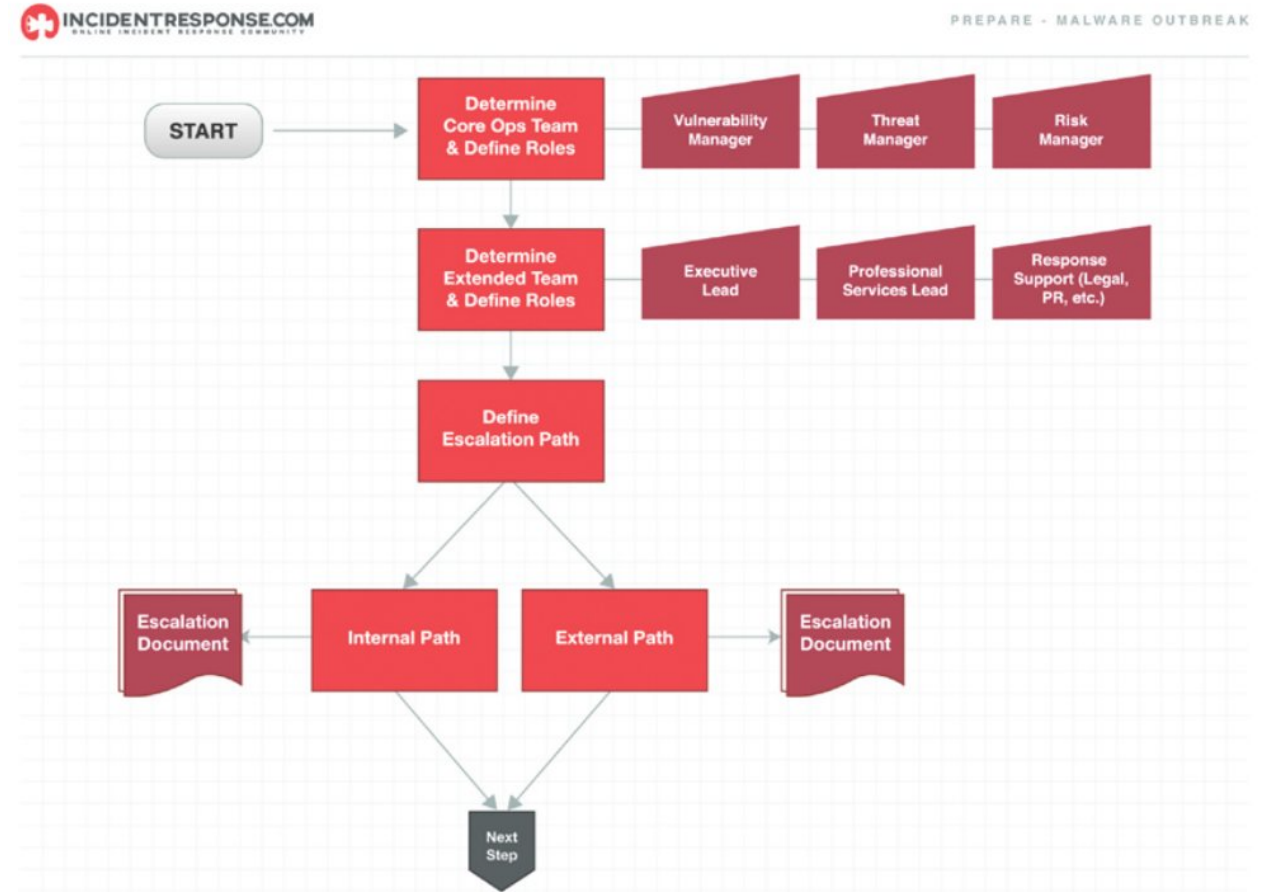
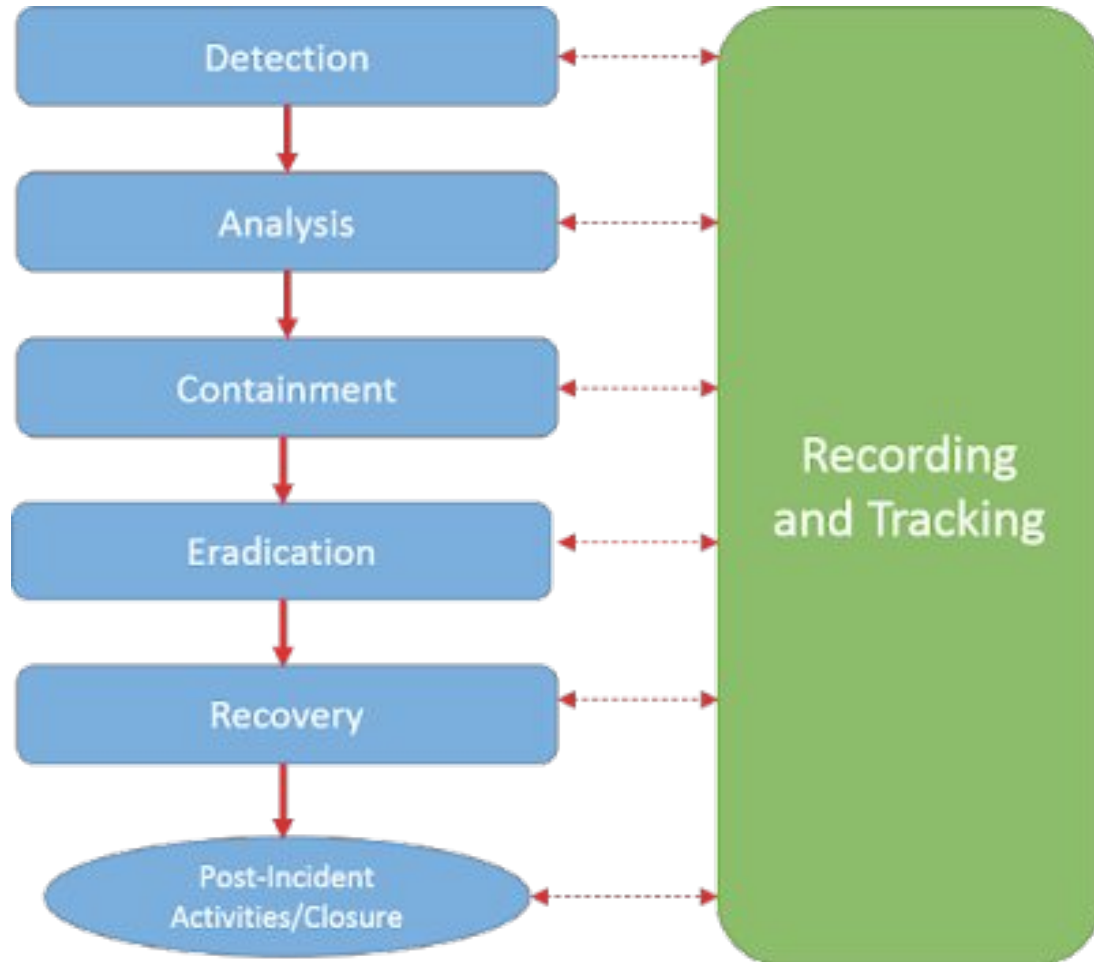
SOC, incident types

	Precursor	Indicator
Natural Disaster	Bad weather forecast	Multiple power interruptions
System Problems	<ul style="list-style-type: none">• Lag in response for multiple software services• Web server log entries that show vulnerability scanner usage	<ul style="list-style-type: none">• Multiple power interruptions• Noticeable period of fluctuation in power supply• Continuous period of temperature increase in direct current (DC)• Network intrusion detection sensor alerts when buffer overflow attempt occurs against database server
Man-made Person-made	<ul style="list-style-type: none">• Announcement of new exploit that targets vulnerability of organization's mail server• A threat from a group stating that the group will attack the organization	<ul style="list-style-type: none">• Antivirus software alerts when it detects that a host is infected with malware.• A system administrator sees a filename with unusual characters.





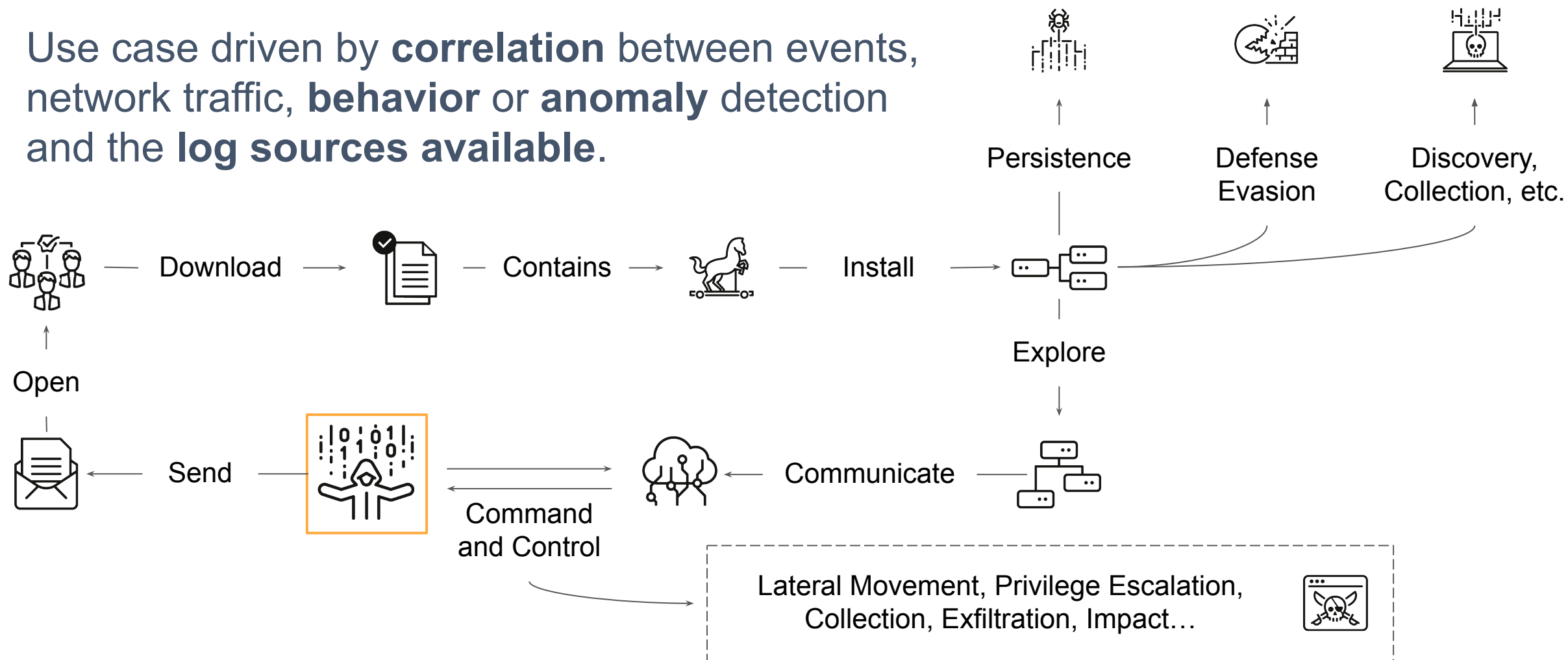
SOC, incident response and run/playbooks





SOC, attack path + intelligence

Use case driven by **correlation** between events, network traffic, **behavior** or **anomaly** detection and the **log sources** available.





SOC, incident characteristics and handling

Incident Prioritization Matrix

		Impact		
		High-System Wide Business Unit, Department, Location	Medium-Multiple Users Number of Users	Low-Single User Single User
Urgency	High Can no longer perform primary work functions	Critical	High	Moderate
	Medium Work functions impaired, the workaround in place	High	Moderate	Low
	Low Inconvenient	Moderate	Low	Low

- Severity (classification)
- Level / tag (enrichment);
- Incident handling (analysis);
- Runbook / Act / Call;
- Escalation (correlation / hunting);
- **Containment, Eradication, and Recovery;**
- Lessons learned.

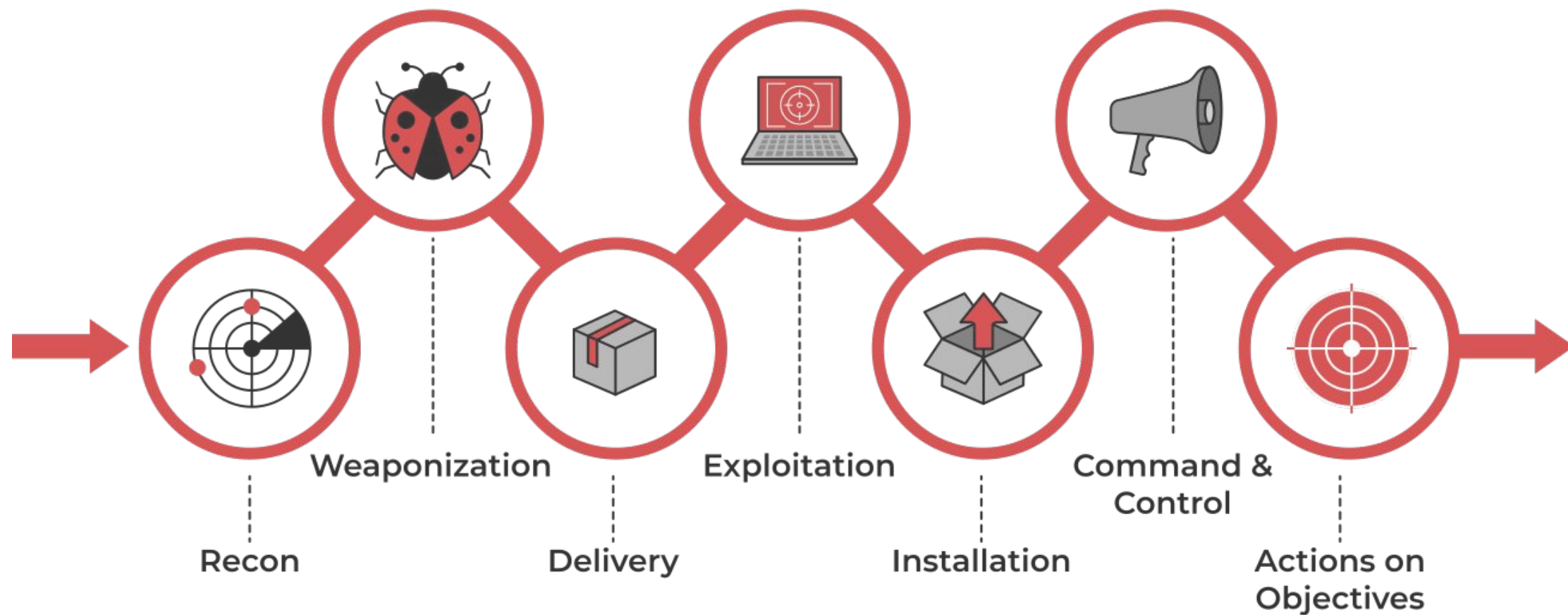
Frameworks

Attacker thinking and some frameworks:

Cyber Kill Chain, Insider Threat Kill Chain
and Mitre Att&ck.



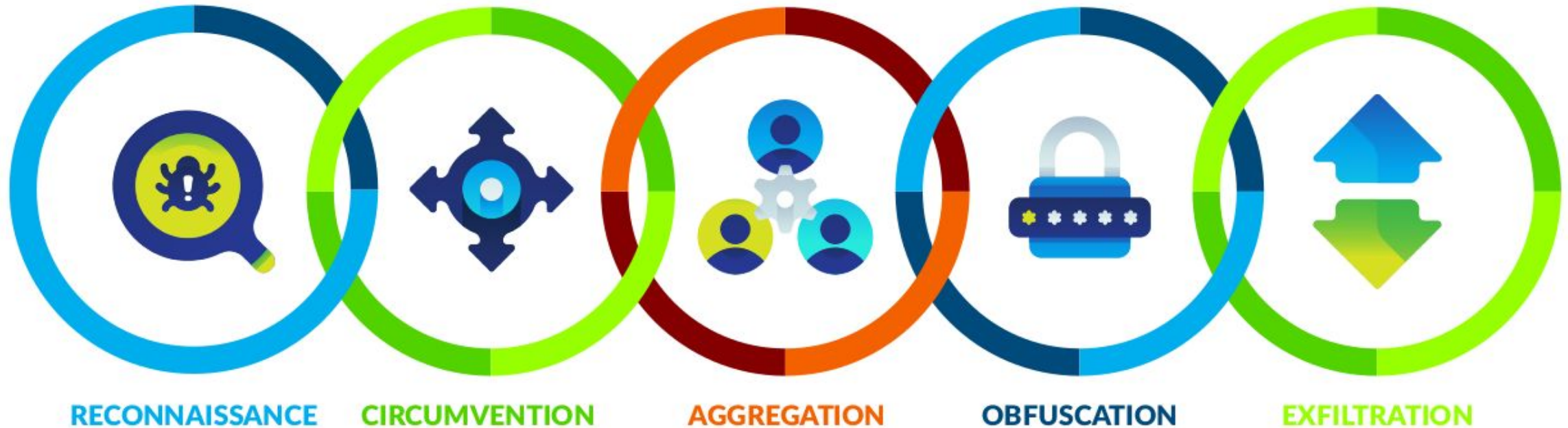
Insider Threat Kill Chain, by stage





Insider Threat Kill Chain, by stage

THE INSIDER THREAT KILL CHAIN





Mitre Att&ck, by tactics

MITRE ATT&CK Tactics in the Enterprise Matrix





Mitre Att&ck, disclaimer





Multiple attack mapped by **environment / sector** to **model threat scenarios** with **attacker mindset**.

Threat Scenarios

Modeling with knowledge of business




Threat scenarios, what are they?



threat scenario

Definitions:


 A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.

Sources:

[NIST SP 800-160 Vol. 2 Rev. 1](#) from [NIST SP 800-30 Rev. 1](#)

[NIST SP 800-161r1](#) from [NIST SP 800-30 Rev. 1](#)

[NISTIR 7622](#) under Threat Scenario from [NIST SP 800-30 Rev. 1](#)

 A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. Synonym for Threat Campaign.

Campaign may
imply insistence

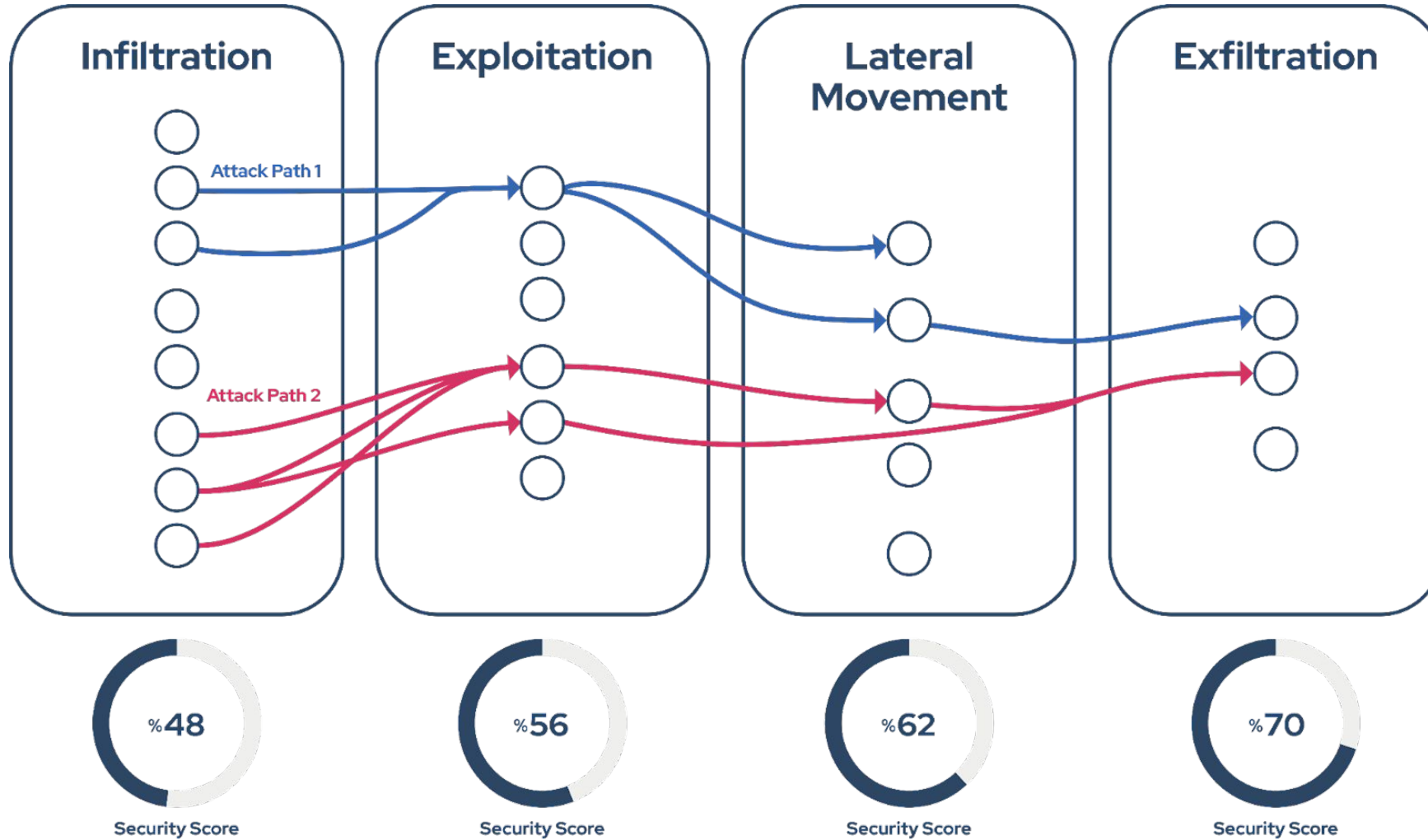
Sources:

[NIST SP 800-30 Rev. 1](#) under Threat Scenario

Fonte: csrc.nist.gov/glossary/term/threat_scenario



Threat scenarios, attack path and mindset





Threat scenarios, ex: phishing

- 1) Phishing detected with a **spreadsheet attached**, without macros, claiming to be confidential content for a specific department.
- 2) Phishing detected with a **link** to a **form** that may attempt to steal the user's credentials, to everyone.
- 3) Phishing detected with a **malware attached**, claiming to the execution.
- 4) Phishing detected **from a C-level account!!!**





Phishing, some techniques and tactics

([T1566](#))

Phishing

Tactic: **Initial Access**

Sub-techniques:

T1566.001,
T1566.002,
T1566.003,
T1566.004

([T1598](#))

Phishing for Information

Tactic: **Reconnaissance**

Sub-techniques:

T1598.001,
T1598.002,
T1598.003,
T1598.004

([T1534](#))

Internal Spearphishing

Tactic: **Lateral Movement**



Related tactics: Resource Development, Initial Access, Execution, Defense Evasion, Discovery, Lateral Movement... **always business-oriented!**



Threat scenarios, appropriate classification

Priority Code = Incident Scale	Incident Impact	Target Response Time	Target Resolution Time
1	Critical	< 5 min With a 24-hour response team	< 1 hour
2	High	< 15 mins during office hours < 2 hours after office hours for an office-hour response team. Otherwise, 4-8 hours depending on site.	< 4 hours
3	Medium	< 15 mins during office hours < 2 hours after office hours for an office-hour response team. Otherwise, 4-8 hours depending on site.	< 8 hours
4	Low	< 15 mins during office hours < 2 hours after office hours for an office-hour response team. Otherwise, 4-8 hours depending on site.	< 24 hours
5	Very Low	No response needed with system auto-filter.	--

Considering:

- Priority;
- Impact;
- Responsible team;
- Resolution time;
- **Mitigation!**



Threat scenarios, business-oriented

- Knowledge of business;
- Specific behavior detection;
- Special anomaly detection;
- Cross-department correlation (DLP, NAC, etc.);

etc.



Conclusion

Because conclusion is also important



Conclusion, complex and abstract





Conclusion, what have we learned?

- Appropriate classification <3;
- Threat modeling mapped by environment / sector;
- Balance between cost, risk and maturity;
- Attacker mindset is very useful;
- Use cases business-oriented;
- Deep details making the difference;
- Efficient and effective incident handling;
- There are no bugs in the matrix... really? :)



Thank you!



by Manoelito Filho ([LinkedIn](#))
Suggestions and questions?
ping me ;)





References

Let's deeper dive into :)



References

CISA - Cybersecurity and Infrastructure Security Agency. Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Available at: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf. Accessed on: Nov 02, 2023.

MUGHAL, Arif Ali. [Building and Securing the Modern Security Operations Center \(SOC\)](#). International Journal of Business Intelligence and Big Data Analytics, v. 5, n. 1, p. 1-15, 2022.

MUNIZ, Joseph. The modern security operations center. Addison-Wesley Professional, 2021.

CLOUD SECURITY ALLIANCE. Cloud Incident Response (CIR) Framework. Available from: <https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/>. Accessed: Nov 13, 2023.

TOIT, Dominique Du. What is the Balance between Cost and Risk in terms of Cyber Security Maturity?. Available from: <https://www.linkedin.com/pulse/what-balance-between-cost-risk-terms-cyber-security-maturity-du-toit/>. Accessed Nov 11, 2023.



References

TRICKS ON FLICKS. Security Operation Centre. Available from:
<<https://tricksonflicks.blogspot.com/2018/03/security-operation-centre.html>>. Accessed: Nov 07, 2023.

TEMPEST. What is and what are the benefits of a SOC (Security Operations Center)?. Available from:
<<https://www.tempest.com.br/o-que-e-e-quais-sao-os-beneficios-de-um-soc-security-operations-center/>>. Accessed: Nov 14, 2023.

BITLYFT. What is Managed Detection and Response (MDR)? Security 101. Available from:
<<https://www.bitlyft.com/resources/what-is-managed-detection-and-response-mdr-security-101>>. Accessed: Nov 14, 2023.

INVGATE. Incident Severity Levels. Available from: <<https://blog.invgate.com/incident-severity-levels>>. Accessed: Nov 25, 2023.

HAIRCUTFISH. TryHackMe Cyber Kill Chain Room. Available from:
<<https://medium.com/@haircutfish/tryhackme-cyber-kill-chain-room-a0ebcff024a9>>. Accessed: Nov 25, 2023.



References

DTEXSYSTEMS. Dtex Insider Threat Kill Chain. Available from:
<<https://www2.dtexsystems.com/Dtex-Insider-Threat-Kill-Chain>>. Accessed: Nov 03, 2023.

F5 NETWORKS. MITRE ATT&CK: What It Is, How It Works, Who Uses It, and Why. Available from:
<<https://www.f5.com/labs/learning-center/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why>>. Accessed: Nov 12, 2023.

BLACKBERRY. MITRE ATT&CK vs Cyber Kill Chain. Available from:
<<https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack/mitre-attack-vs-cyber-kill-chain>>. Accessed: Nov 15, 2023.

LOCKHEED MARTIN. Gaining the Advantage: Cyber Kill Chain. Available from:
<https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf>. Accessed: Nov 01, 2023.

DELINEA. What is the MITRE ATT&CK Framework? Available from:
<<https://delinea.com/blog/what-is-the-mitre-attack-framework>>. Accessed: Nov 01, 2023.



References

OSIBeyond. USB Drop Attacks Cause Cybersecurity Incidents. Available from:
<<https://www.osibeyond.com/blog/usb-drop-attacks-cause-cybersecurity-incidents/>>. Accessed: Nov 12, 2023.

PICUS SECURITY. What is an Attack Path? Available from:
<<https://www.picussecurity.com/resource/blog/what-is-attack-path>>. Accessed: Nov 11, 2023.

LOCKEDBYTE. Tweet: CVE-2021-3156 Exploit. Available from:
<<https://twitter.com/lockedbyte/status/1355265699455893504>> | Repository:
<<https://github.com/lockedbyte/CVE-Exploits/tree/master/CVE-2021-3156>>. Accessed: Nov 17, 2023.

PYRALINK. SIEM: What it is and Why it's Critical for Cybersecurity? Available from:
<<https://pyralink.co.uk/blog/siem-critical-for-cybersecurity/>>. Accessed: Ago 27, 2025.

– Images –

RAWPIXEL. Free Matrix Background - Public Domain CC0 Photo. Available at:
<<https://www.rawpixel.com/image/5901986/free-matrix-background-public-domain-cc0-photo>>. Accessed on: Nov 17, 2023.



References

SHMECTOR. Neo Matrix Vector Illustration - CC1 Universal. Available at:
<https://shmector.com/free-vector/people/neo_matrix/4-0-1050>. Accessed on: Nov 17, 2023.

GARCIA, Hector. Red or blue pill Image - CC BY-NC-SA 2.0 Deed. Available at:
<<https://www.flickr.com/photos/torek/4444673930>>. Accessed on: Nov 17, 2023.

PATTERSON, Richard. Phishing Image Image - CC BY-NC-SA 2.0 Deed. Available at:
<<https://www.flickr.com/photos/torek/4444673930>>. Accessed on: Nov 17, 2023.

A black and white photograph of a typewriter keyboard, showing several rows of keys. The keys are dark with light-colored lettering. A prominent vertical tear in the paper separates the keyboard image from the text on the right. The tear is jagged and irregular, running from the top to the bottom of the page.

Extra!

Do you want to dive a little deeper?



Extra, EnSI - 02 e 03 de Outubro



Encontro de Segurança em Informática
do CERT.Bahia

Comemore conosco os nossos 15 anos!
Em breve, disponibilizaremos a programação completa.

35

DIAS

8

HORAS

41

MINUTOS

33

SEGUNDOS



Extra, HackBahia - 04 de Outubro de 2025

hackbahia

Seguindo ▾

Enviar mensagem



hackbahia

20 publicações

374 seguidores

6 seguindo

HackBahia

hackbahia.github.io e mais 1



hackbahia

Traga a sua empresa para
o nosso evento!

hackbahia

Call For Papers 2025





Extra, Nullbyte - 08 de Novembro de 2025

Nullbyte Security Conference

📅 08 nov - 2025 • 09:00 > 08 nov - 2025 • 15:00

📍 Evento presencial em **Local a definir, Salvador - BA**





Axé Sec

Somos a instância autônoma de cibersegurança que atua no [Raul Hacker Club](#).

Encontros

- Local: sede do [RHC](#) e no canal/grupo do Telegram
- Reuniões: presenciais (pelo menos 1x/mês) e remotas (sob demanda)
- Eventos: [Oxum Hacker Conf.](#)

Projetos

- [OWASP Salvador](#)
- [Raul Hacker Club](#)
- [Grupos de estudo](#)

Redes Sociais

- Telegram: [@axesec_community](#)
- Gitlab: [@axesec](#)
- InstaLIX0: [@axesec](#)
- InstaLIX0: [@oxumhc](#)

Links rápidos

- [Formulário](#)
- [Preceitos](#)
- [Membros Ativos](#)
- [Eventos de Cyber](#)

Eventos de Cibersegurança 2025

Este é um mapeamento atualizado dos principais eventos de cibersegurança previstos para 2025 no Brasil. As informações foram coletadas ao longo do ano e organizadas em dois formatos:

- Mapa de distribuição, exibindo a quantidade de eventos por estado.
- Calendário de eventos, para consulta rápida das datas e detalhes.

[\[2024\]](#) [\[2025\]](#) [\[2026\]](#)

Mapa de distribuição

Adicionamos cores indicando a distribuição por estado, permitindo visualizar quais são as regiões mais ativas. Dica: interaja com o mapa para ver detalhes ao passar o mouse sobre cada estado.



Calendário de eventos



Extra, Oxum Hacker Conf - 31 de Janeiro de 2026



Thank you!



by Manoelito Filho ([LinkedIn](#))
Suggestions and questions?
ping me ;)

