Tempest

[ACADEMY]

Conference

2023

A glitch in the Matrix: Attack as Déjà vu

Manoelito Filho

28 de novembro de 2023

Classificação da Informação: PÚBLICA
Autor da apresentação: <Manoelito Filho | Blue Consulting>

Tempest

:ACADEMY:

Conference

00 Introduction

01 Security Operations Center (SOC)

02 Frameworks

03 Threat Scenarios

04 Conclusion

05 References

Introduction

Who am I, motivation and scope

$ whoami

BLUE CONSULTING

Tempest
[ACADEMY]
Conference

Raul HackerClub

instituto
AARON SWARTZ

>_FARPA

Motivation

Motivation

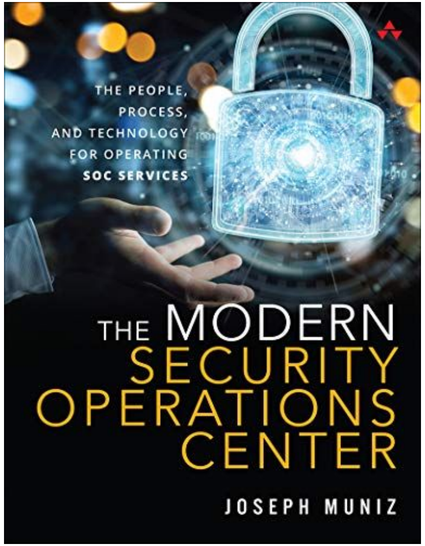
Scope

MITRE ATT&CK™

NIST
National Institute of Standards and Technology

CSA cloud security alliance℠

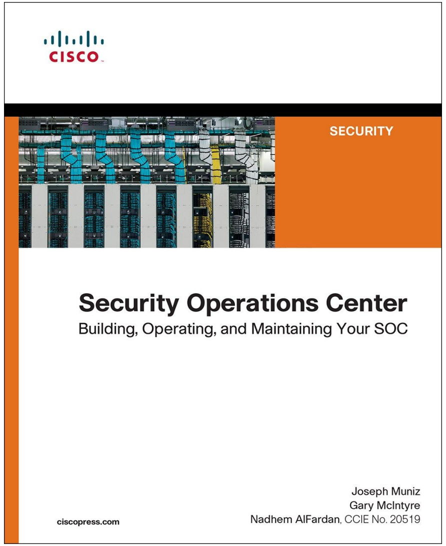
CISA CYBER+INFRASTRUCTURE



THE PEOPLE, PROCESS, AND TECHNOLOGY FOR OPERATING SOC SERVICES

THE MODERN SECURITY OPERATIONS CENTER

JOSEPH MUNIZ



cisco

SECURITY

Security Operations Center

Building, Operating, and Maintaining Your SOC

Joseph Muniz
Gary McIntyre
Nadhem AlFardan, CCIE No. 20519

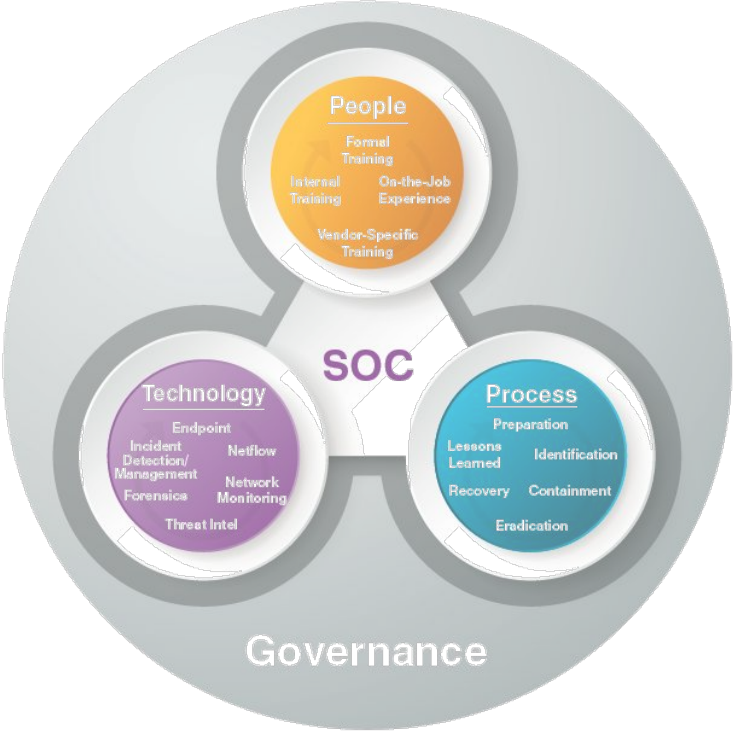
ciscopress.com

Security Operations Center (SOC)

What is a SOC?

SOC, what is it?

Tempest
[ACADEMY]
Conference



SOC, what is it?

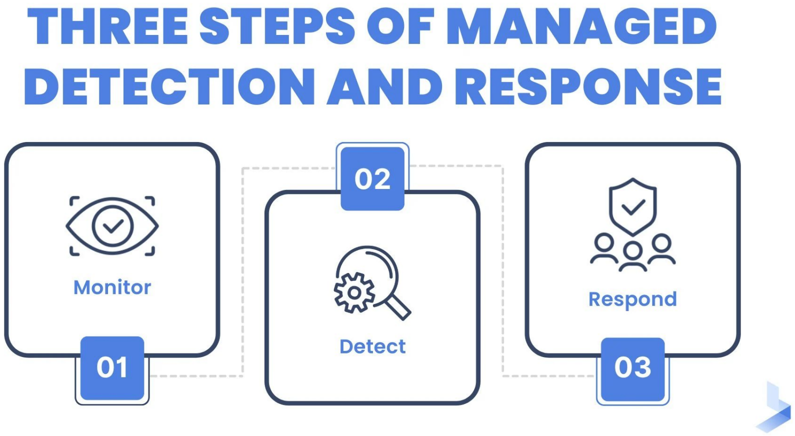
“SOC is not SIEM”

by someone smart

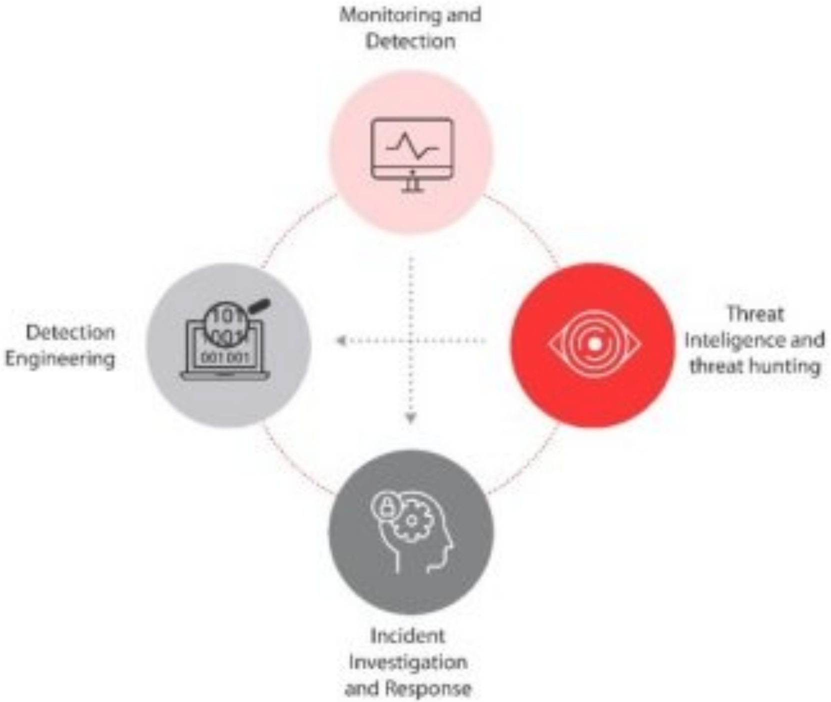
SIEM: Security Information and Event Management

SOC, more than MDR

Tempest
[ACADEMY]
Conference



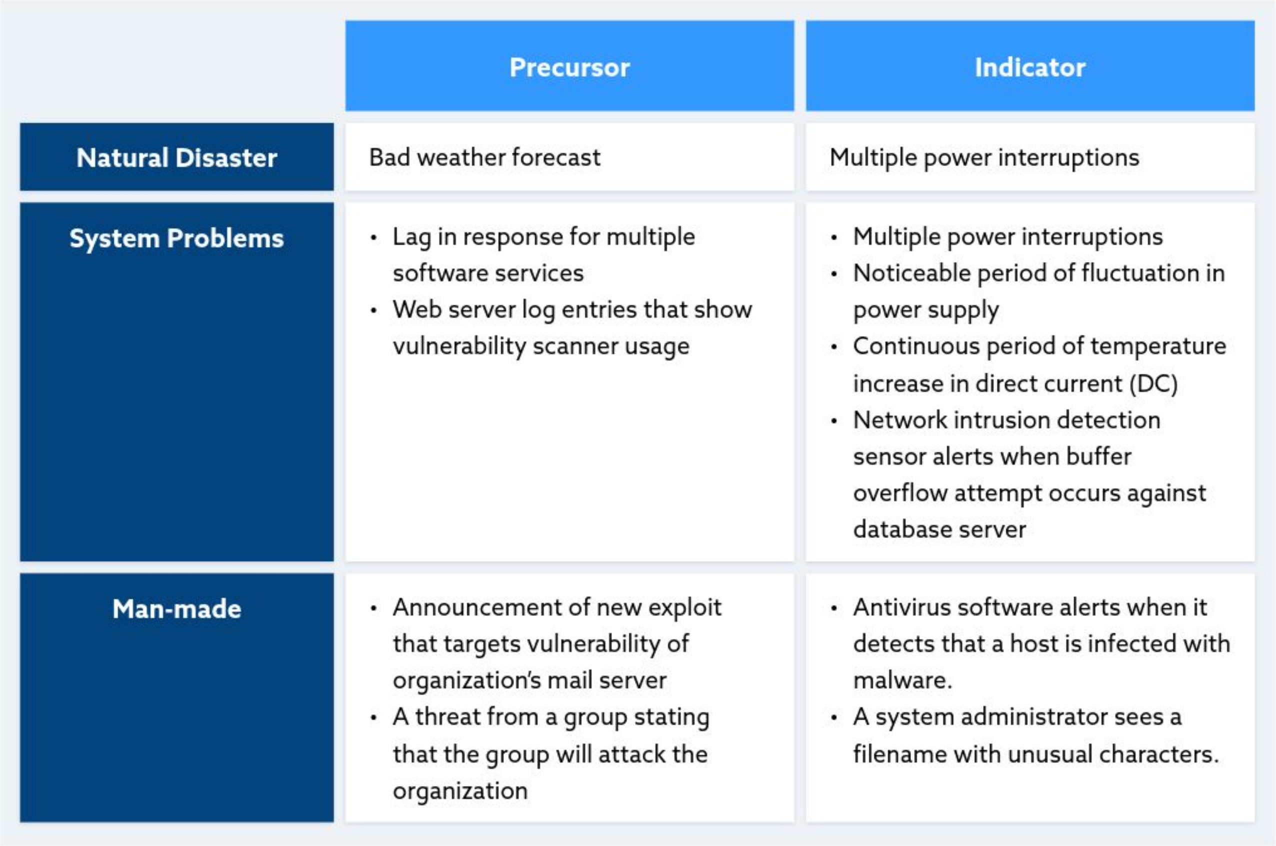
THREE STEPS OF MANAGED DETECTION AND RESPONSE



Monitoring and Detection
Detection Engineering
Threat Inteligence and threat hunting
Incident Investigation and Response

SOC, incident types

Tempest
[ACADEMY]
Conference

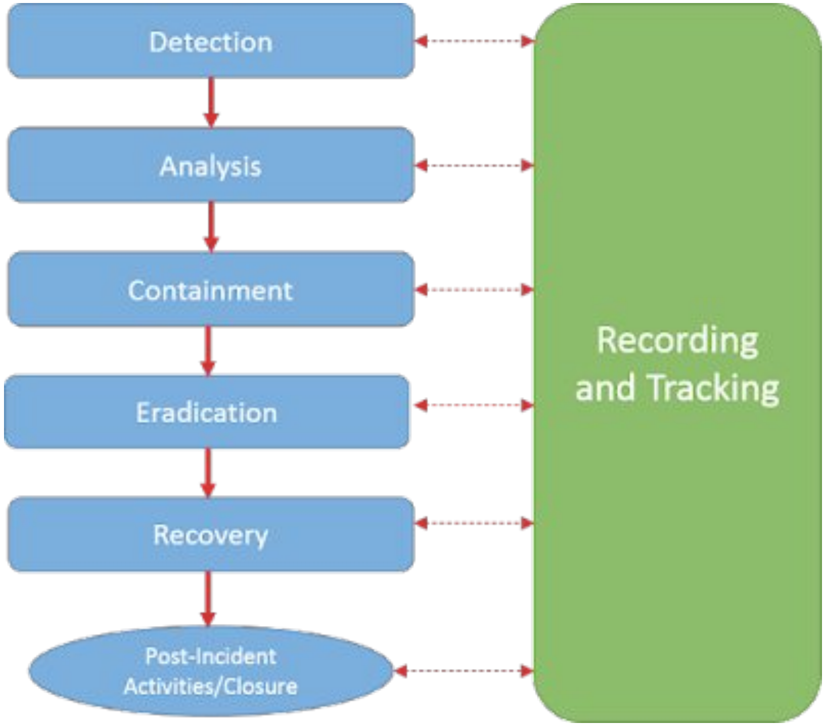


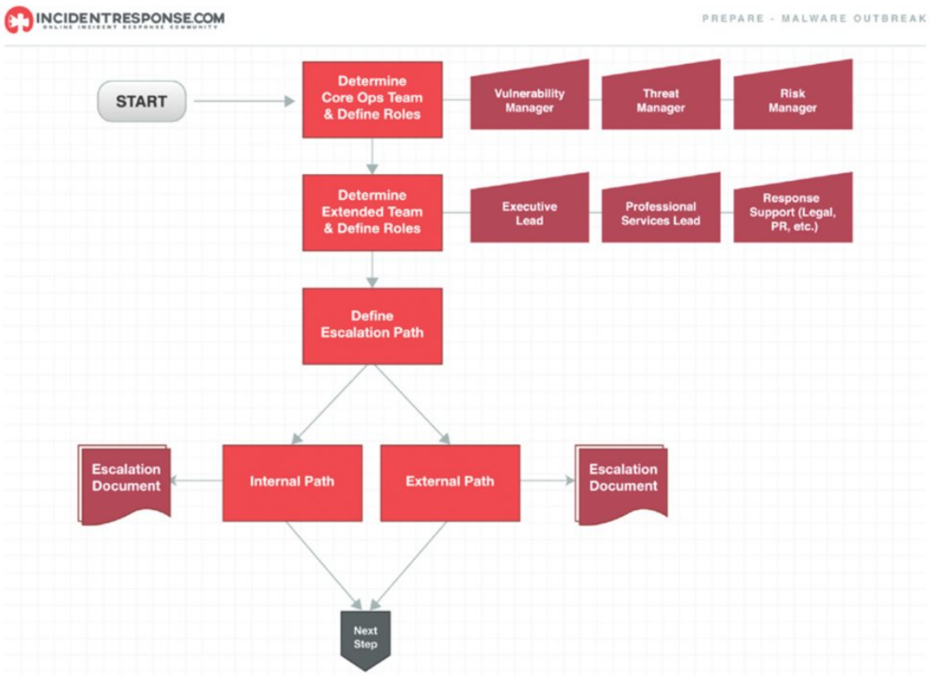
	Precursor	Indicator
Natural Disaster	Bad weather forecast	Multiple power interruptions
System Problems	• Lag in response for multiple software services • Web server log entries that show vulnerability scanner usage	• Multiple power interruptions • Noticeable period of fluctuation in power supply • Continuous period of temperature increase in direct current (DC) • Network intrusion detection sensor alerts when buffer overflow attempt occurs against database server
Man-made	• 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	• Antivirus software alerts when it detects that a host is infected with malware. • A system administrator sees a filename with unusual characters.

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

SOC, incident response and run/playbooks

Tempest
ACADEMY
Conference

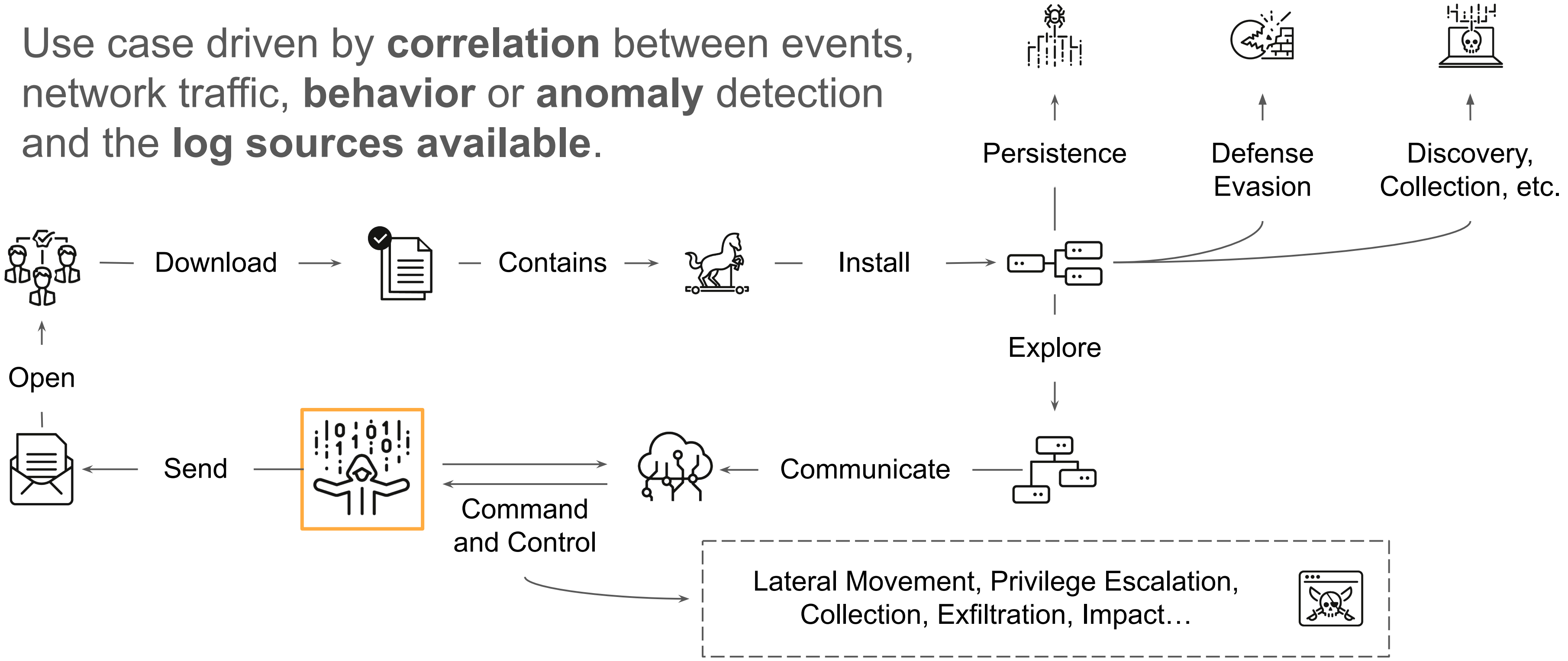




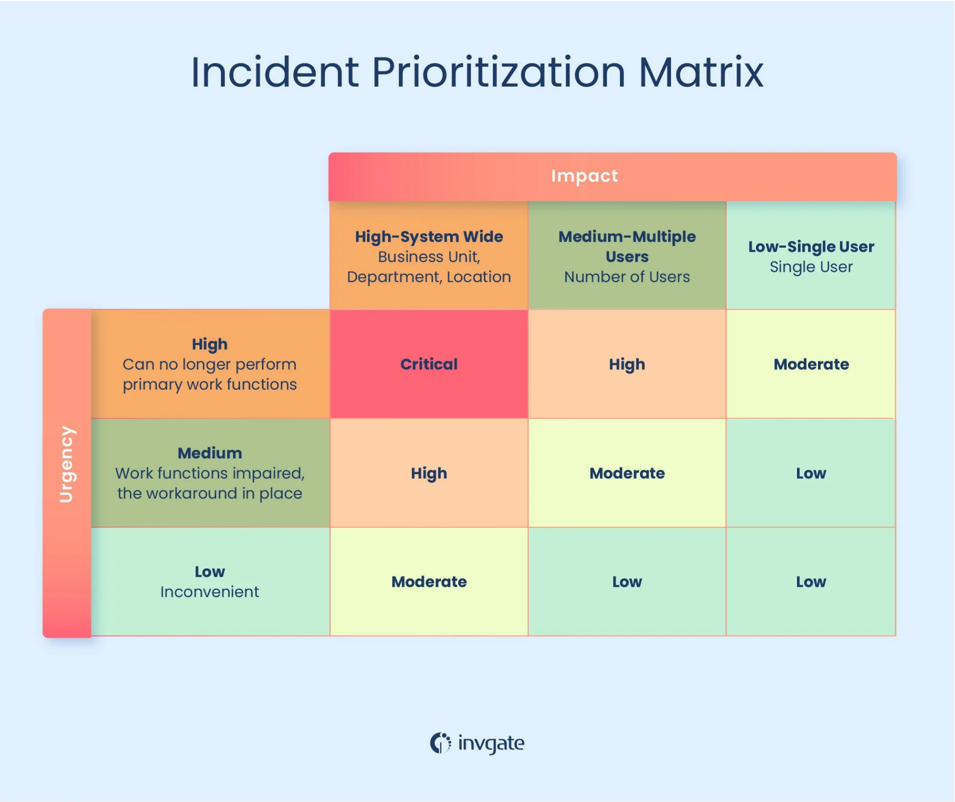
INCIDENTRESPONSE.COM
ONLINE INCIDENT RESPONSE COMMUNITY
PREPARE - MALWARE OUTBREAK
START
Determine Core Ops Team & Define Roles
Vulnerability Manager
Threat Manager
Risk Manager
Determine Extended Team & Define Roles
Executive Lead
Professional Services Lead
Response Support (Legal, PR, etc.)
Define Escalation Path
Escalation Document
Internal Path
External Path
Escalation Document
Next Step

SOC, attack path + intelligence

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


Persistence
Defense Evasion
Discovery, Collection, etc.
Download
Contains
Install
Open
Explore
Send
Communicate
Command and Control
Lateral Movement, Privilege Escalation, Collection, Exfiltration, Impact…

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**

invgate

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

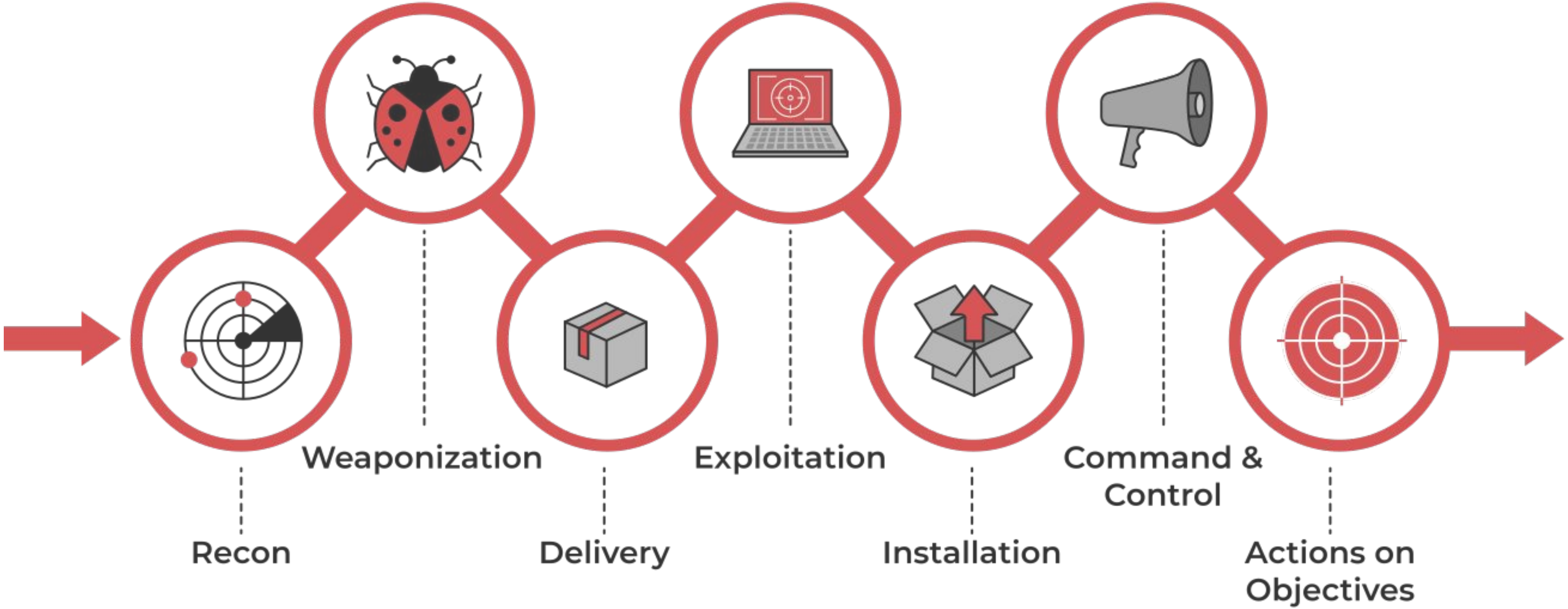
Frameworks

Attacker thinking and some frameworks:

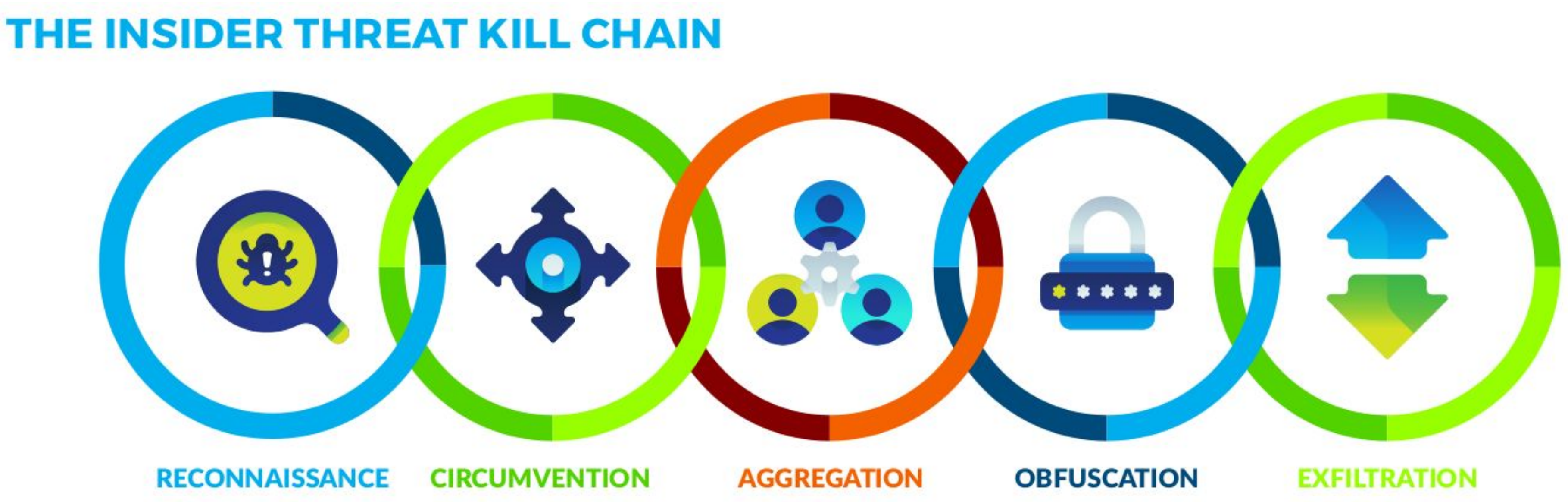
Cyber Kill Chain, Insider Threat Kill Chain and Mitre Att&ck.

Cyber Kill Chain, **by stage**

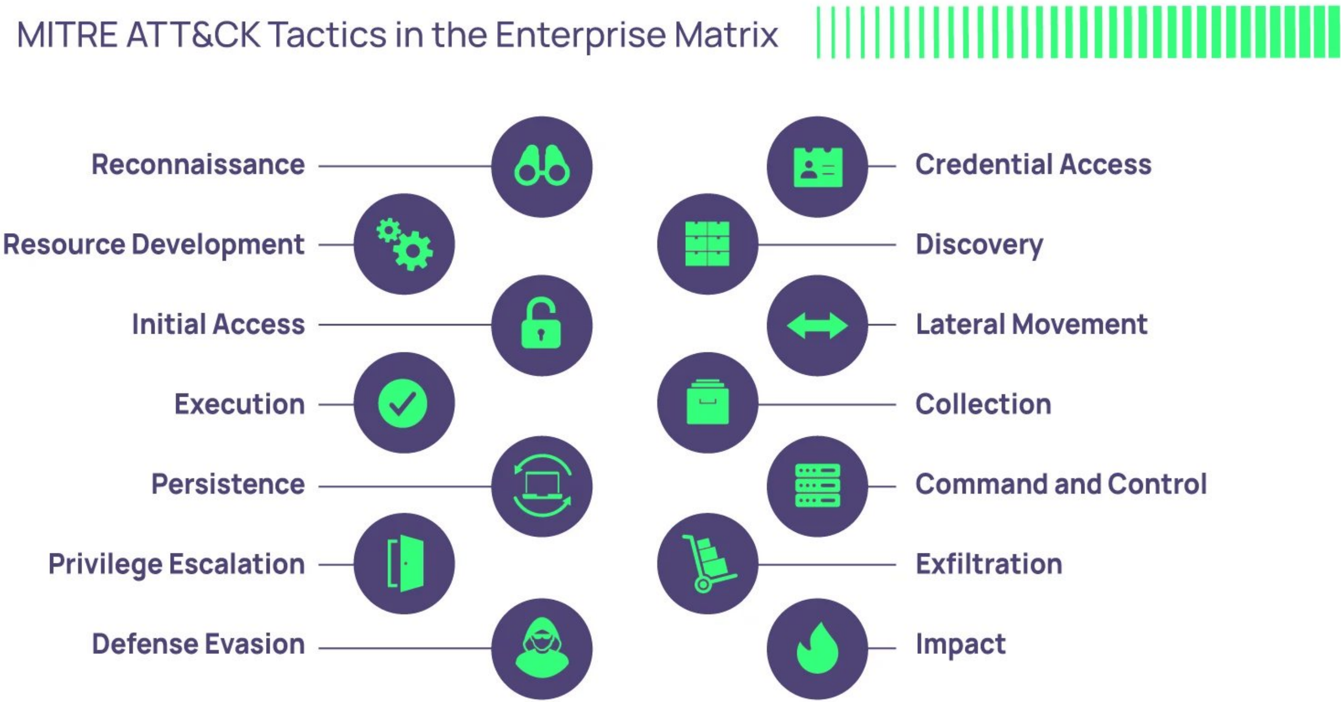
Tempest
[ACADEMY]
Conference



Insider Threat Kill Chain, by stage

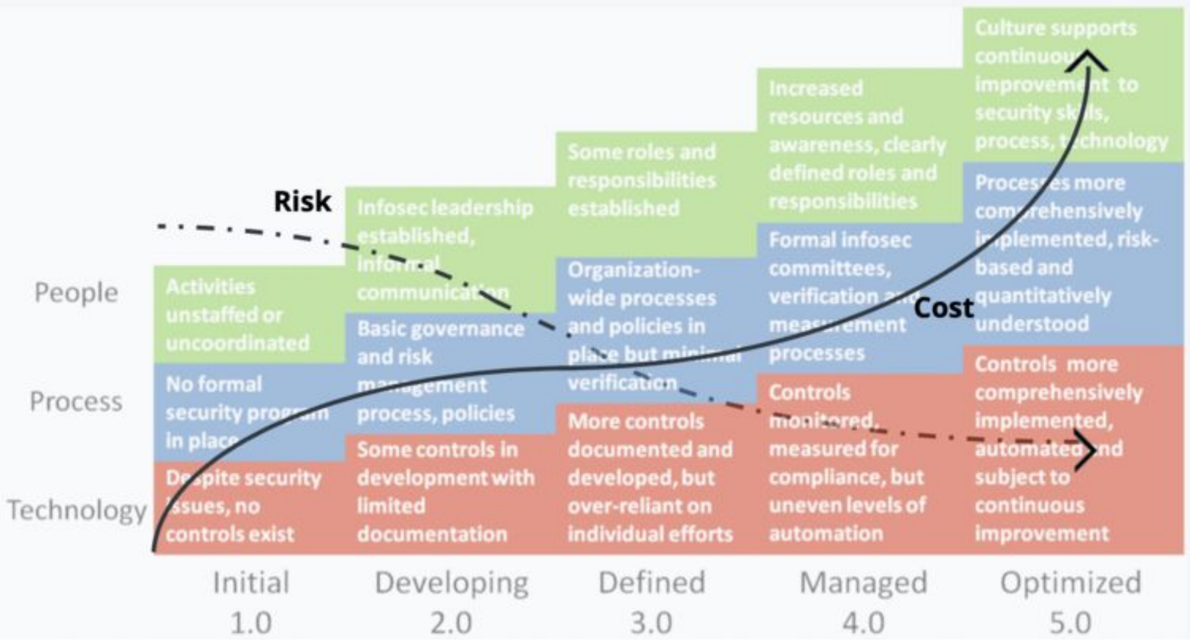


Mitre Att&ck, by tactics



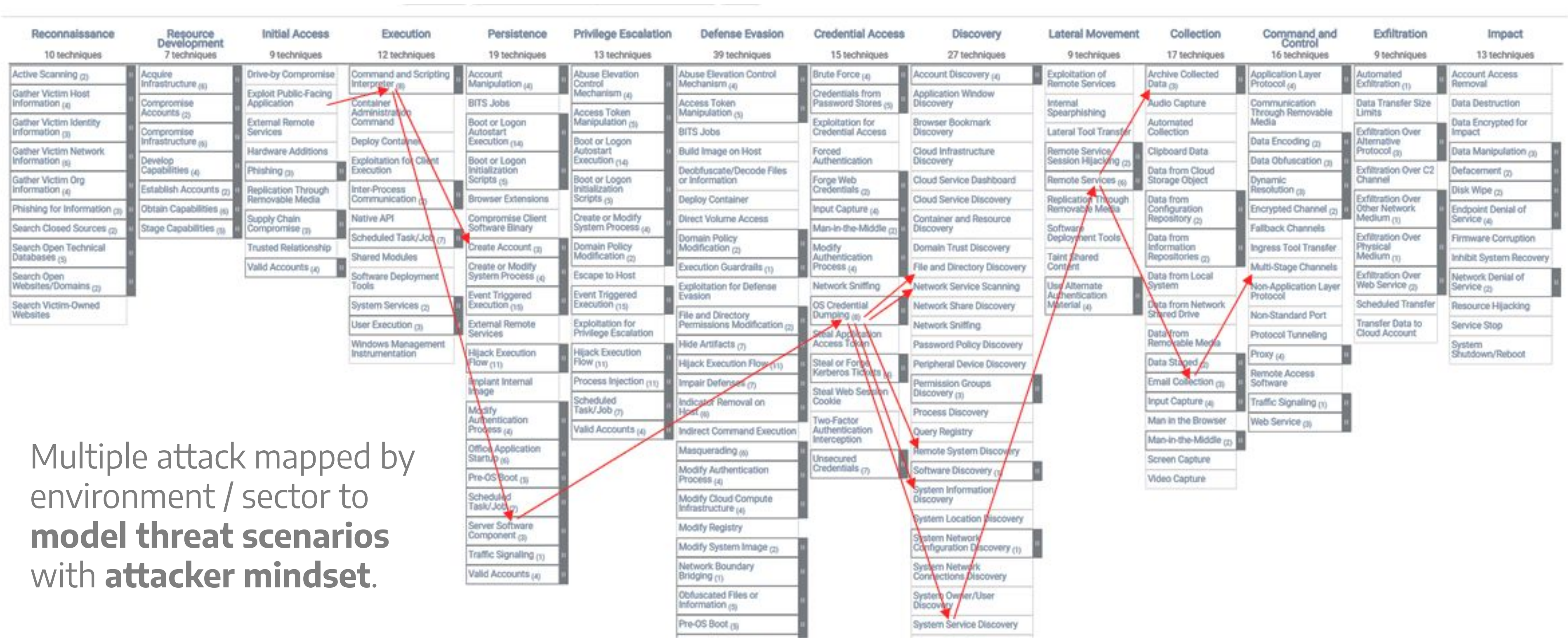
MITRE ATT&CK Tactics in the Enterprise Matrix

Mitre Att&ck, disclaimer



	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
People	Activities unstaffed or uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
Process	No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
Technology	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

Mitre Att&ck, **the matrix**



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Share Discovery		Data Staged (2)	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (7)	Hide Artifacts (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Email Collection (3)	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Password Policy Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Impair Defenses (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (7)		Indirect Command Execution		Process Discovery		Screen Capture	Web Service (3)		
				Server Software Component (3)		Masquerading (6)		Query Registry		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Remote System Discovery					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
						Modify Registry		System Information Discovery					
						Modify System Image (2)		System Location Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery (1)					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
								System Service Discovery					

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

Tempest

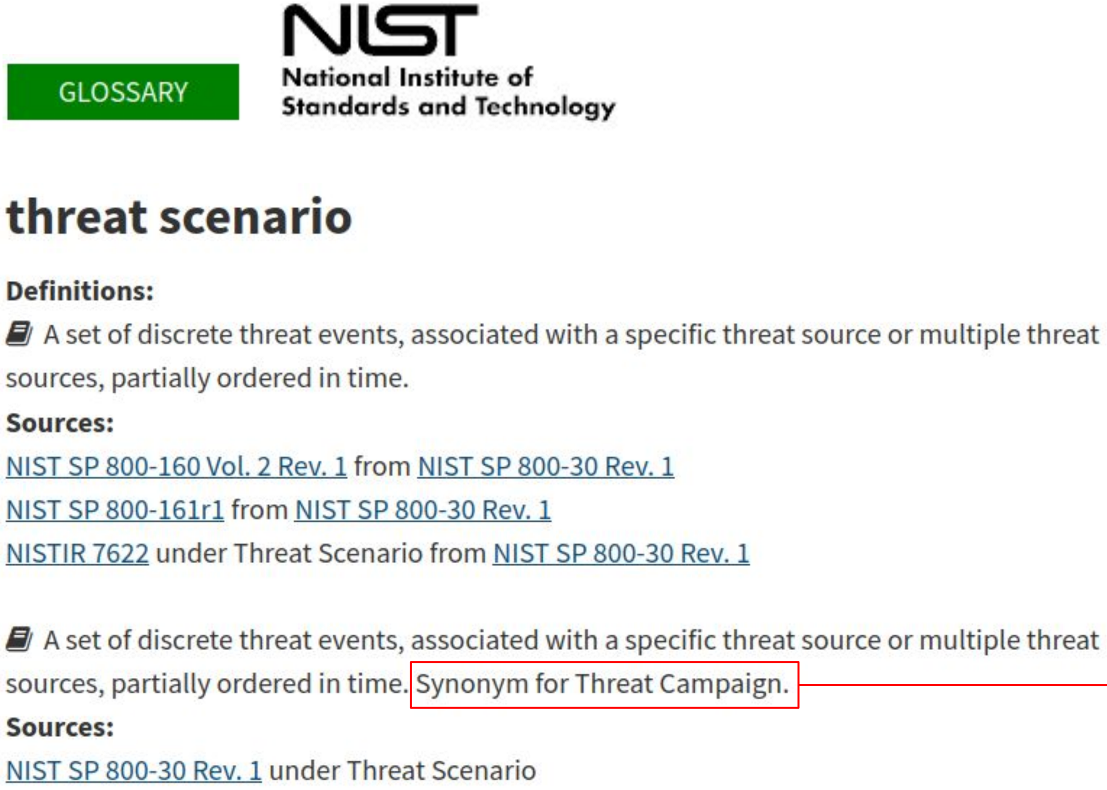
:ACADEMY:

Conference

Threat Scenarios

Modeling with knowledge of business

Threat scenarios, **what are they?**



GLOSSARY

NIST
National Institute of Standards and Technology

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.

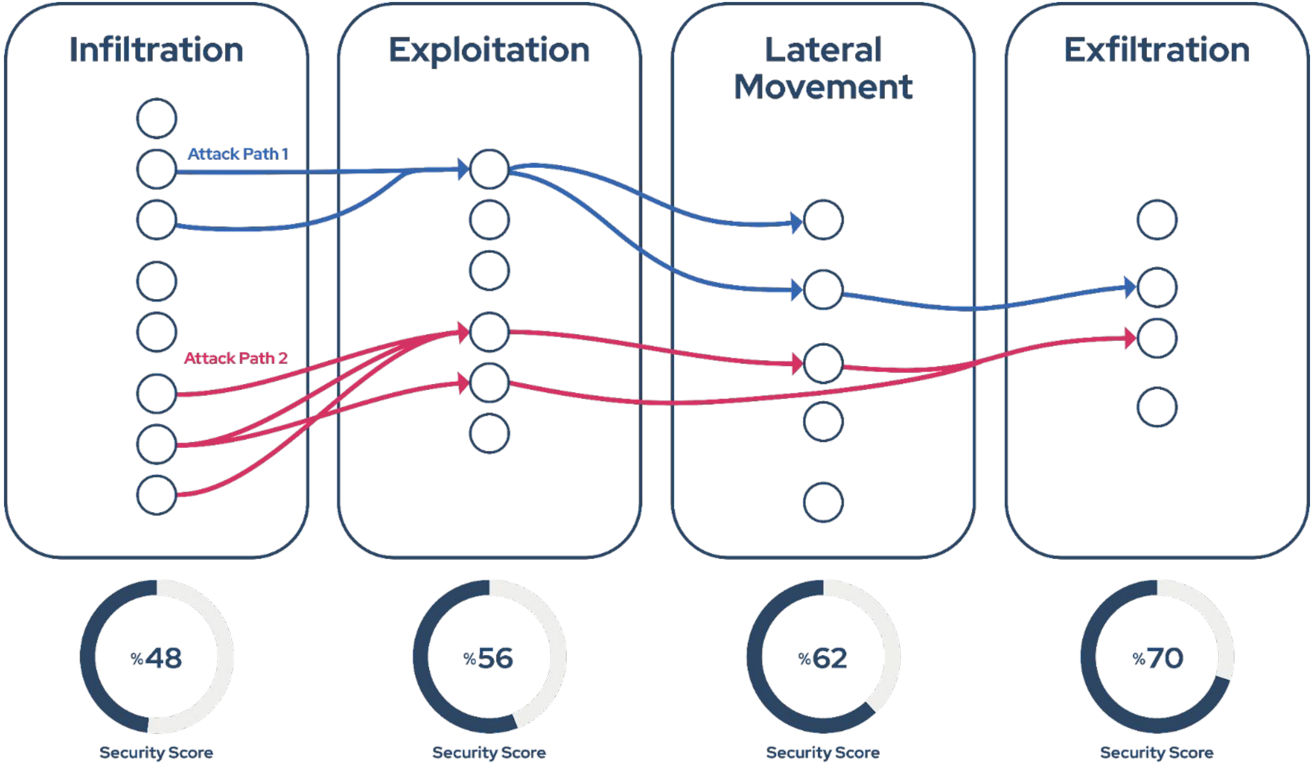
Sources:

NIST SP 800-30 Rev. 1 under Threat Scenario

Campaign may imply insistence

Threat scenarios, attack path and mindset

Tempest [ACADEMY] Conference



Threat scenarios, ex: phishing

Tempest [ACADEMY] Conference

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**

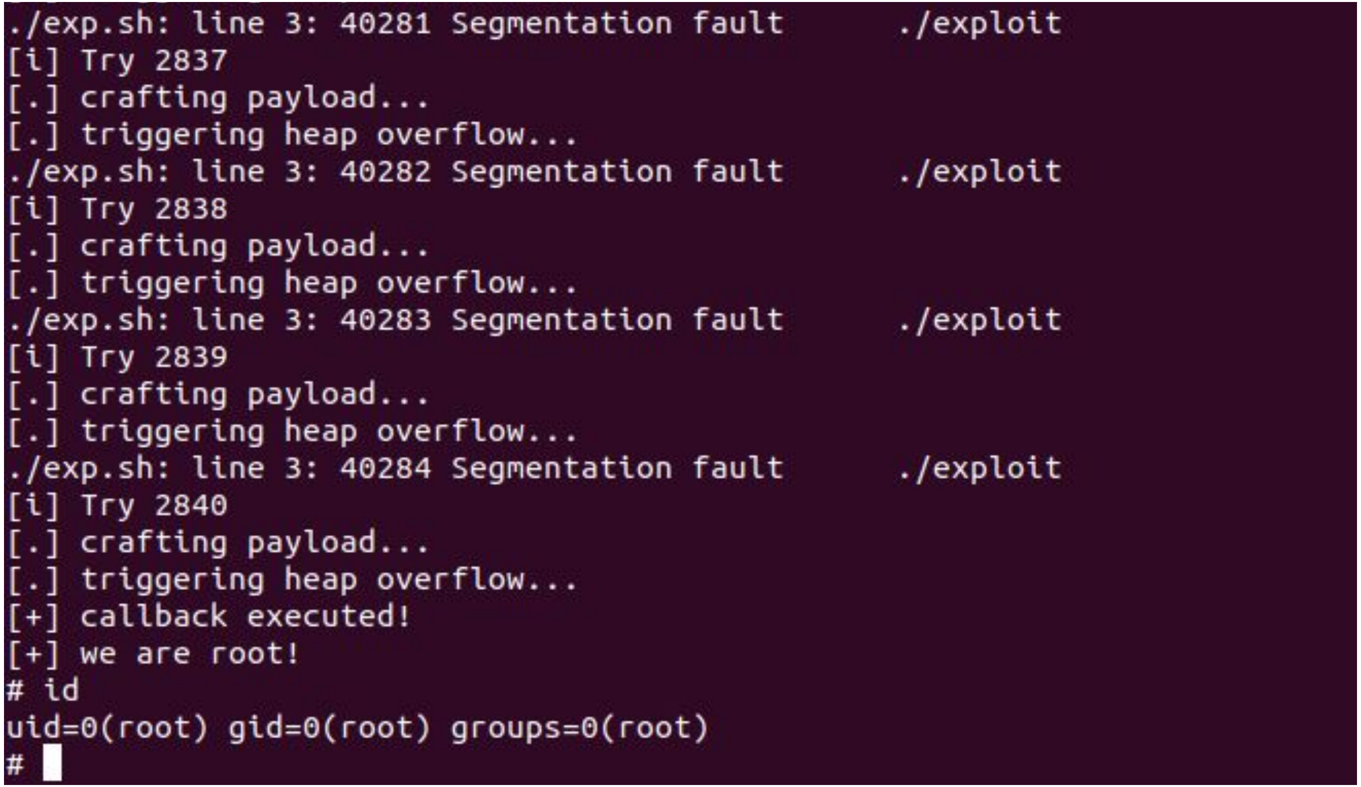
Sub-techniques:
T1598.001,
T1598.002,
T1598.003,
T1598.004

(T1534)
Internal Spearphishing
Tactic: **Lateral Movement**

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

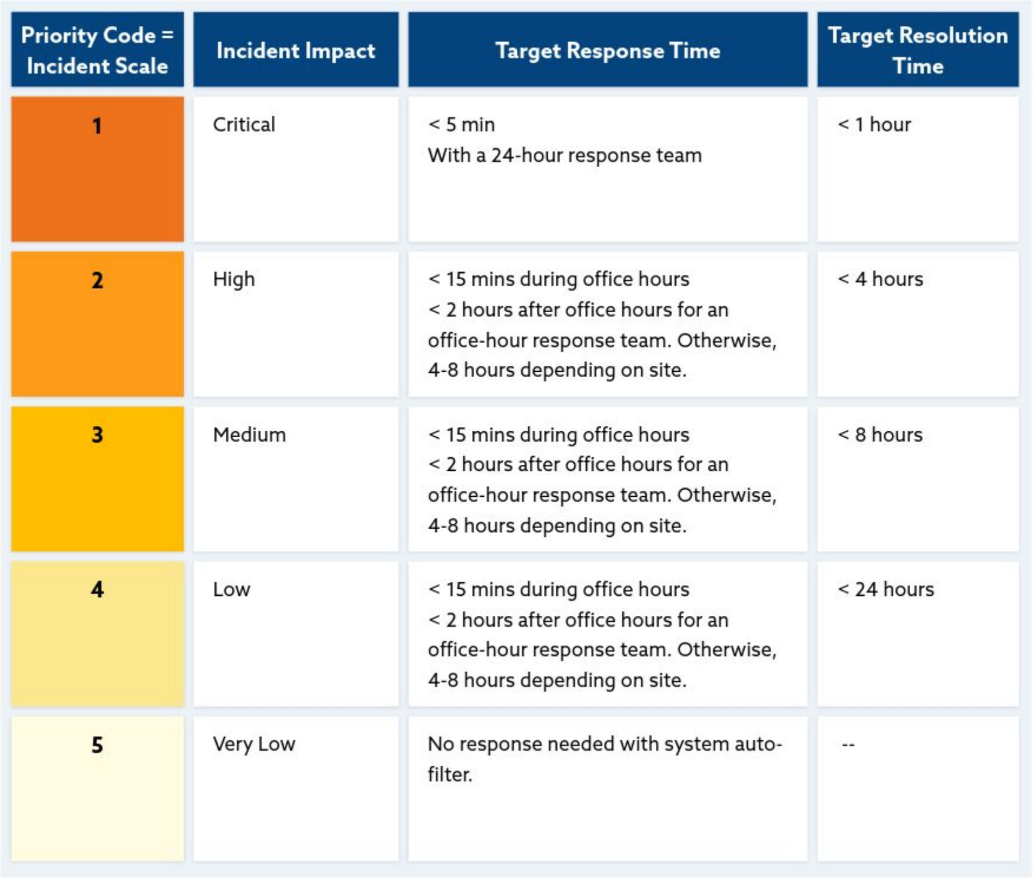
Threat scenarios, other scenarios

Tempest [ACADEMY] Conference



```
./exp.sh: line 3: 40281 Segmentation fault      ./exploit
[i] Try 2837
[.] crafting payload...
[.] triggering heap overflow...
./exp.sh: line 3: 40282 Segmentation fault      ./exploit
[i] Try 2838
[.] crafting payload...
[.] triggering heap overflow...
./exp.sh: line 3: 40283 Segmentation fault      ./exploit
[i] Try 2839
[.] crafting payload...
[.] triggering heap overflow...
./exp.sh: line 3: 40284 Segmentation fault      ./exploit
[i] Try 2840
[.] crafting payload...
[.] triggering heap overflow...
[+] callback executed!
[+] we are root!
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

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.	--

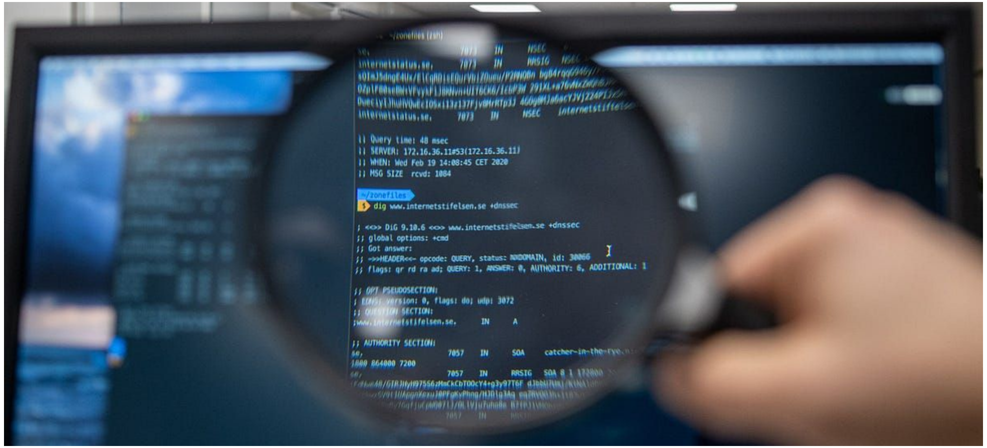
Considering:

- 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.



```
~/zonefiles (zsh)
se.                     7073    IN      NSEC
internetstatus.se.      7073    IN      RRSIG   NSEC
[illegible]
internetstatus.se.      7073    IN      NSEC    internetstifelsen
;; Query time: 48 msec
;; SERVER: 172.16.36.11#53(172.16.36.11)
;; WHEN: Wed Feb 19 14:08:45 CET 2020
;; MSG SIZE  rcvd: 1084

~/zonefiles
$ dig www.internetstifelsen.se +dnssec

; <<>> DiG 9.10.6 <<>> www.internetstifelsen.se +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 30066
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 3072
;; QUESTION SECTION:
;www.internetstifelsen.se.      IN      A

;; AUTHORITY SECTION:
se.                     7057    IN      SOA     catcher-in-the-rye.
1800 864000 7200
se.                     7057    IN      RRSIG   SOA 8 1 172800
[illegible]
```

Conclusion

Because conclusion is also important

Conclusion, complex and abstract

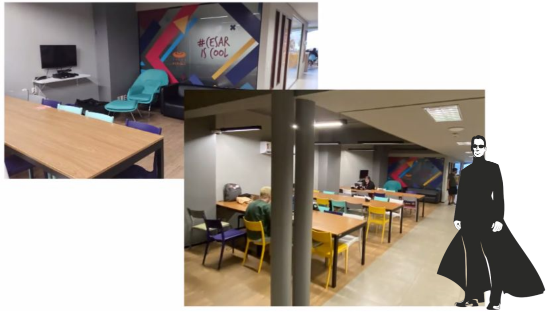
Conclusion, what have we learned?

- 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)
manoelito.filho (a) tempest.com.br
Suggestions and questions, ping me ;)

We are at “Ask the Experts” space!



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.

Tempest

:ACADEMY:

Conference

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.

Tempest

:ACADEMY:

Conference

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.

– 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.

Tempest

[ACADEMY]

Conference

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.