How a hacker goes from zero to hero and causes a cyber crisis

Etienne Verhasselt, Team lead Application Security & Ethical hacking
Koen Vanderloock, Senior Application Security Consultant & Threat Modeler

In the heat of the crisis

orange™ Cyberdefense


Claim
Anger
???
Disappointed
Crisis
Stress
Sadness
Fear
PII
Lost business
Fired
IP

Your expectations mirror the challenges you encounter!

- Do you have a checklist for better preparedness?
- What is the ultimate solution to prevent all cyberattacks?
- How to anticipate a crisis effectively?
- Identifying the most likely crisis scenarios for your organization.
- Strategies for preventing a cyber crisis.
- The criteria for classifying an incident as a risk.
- Efficient methods to detect all potential hacker entry points.
- Calculating risk efficiently for specific threats or crises.
- Addressing concerns and nervousness within top management.
- Key elements to include in cyber crisis test scenarios.
- Sensitizing customers to the importance of crisis preparedness.
- Predictions for the cybersecurity industry in the next two years.
- Mitigating the lack of anticipation.
- Promoting responsibility among key stakeholders before a crisis and avoiding decision overlaps during a crisis.
- Etc.


It becomes crucial to comprehend potential threats, attack vectors, and their (possible) business impact.

How a hacker goes from zero to hero and causes a cyber crisis

Let’s not wait for a crisis but learn to be the hero ourselves and avoid one.

In this breakout session, we’ll delve into the thrilling realm of attack scenario modeling where red (offensive) and blue (defensive) teams unite to form a powerful purple force.

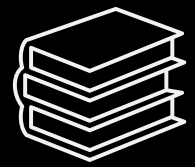
A real-life case will be our guide as we share battle-tested techniques to fortify your defenses.

Real-life attack scenario

Steal confidential data

Red teaming process

Attack scenario modeling



Threat scenario library

Determine objectives / flags

Develop potential threat scenarios

Select threat scenario(s)

Measure / Evaluate

Governance level

Operational level

Refine threat scenario

Validate threat scenario

Execute offensive activities

Reporting

Offensive report

Ongoing defensive activities

Reporting

Defensive report

Analyze, evaluate and triangulate

Lessons learned

Threat scenario playbook

Debriefing report

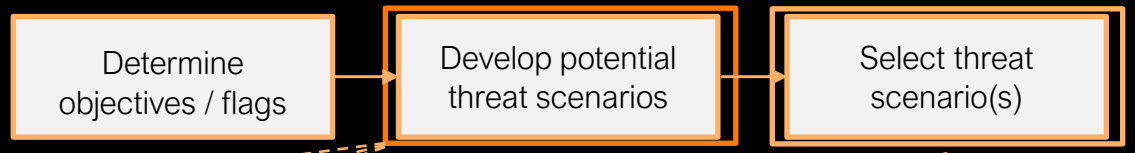
Improvement Lessons learned report

The objective / flag

An attacker will try to steal the confidential data of your organization.

Perceptual positions
- Orange Cyberdefense
- The customer = you
- Neutral observer

Potential threat scenario



#3

#2

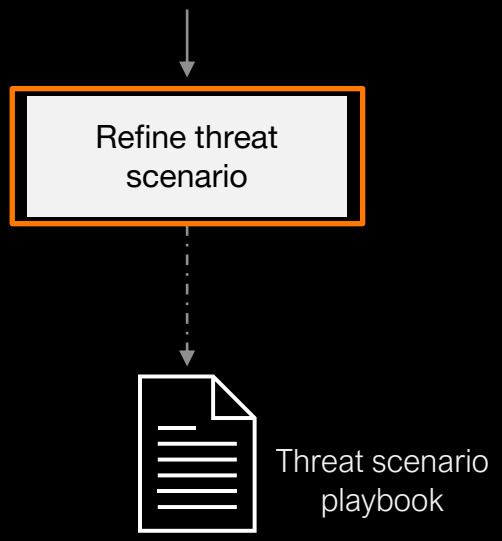
#1

An attacker will look for (zero-day) vulnerabilities in an application and exploit those vulnerabilities.

The objective is to reach and gain control of the internal system located at the deepest level of the network and obtain confidential data (= crown jewels).

Perceptual positions
- Orange Cyberdefense
  - Threat Intelligence
  - Ethical hacker
  - Criminal mindset = adversary, hacker
- The customer = you
- Neutral observer

Refine the threat scenario - (1) Attack scenario



An attacker will look for (zero-day) vulnerabilities in an application and exploit those vulnerabilities.

The objective is to reach and gain control of the internal system located at the deepest level of the network and obtain confidential data (= crown jewels).

Once the internal systems are reached, the attacker can try to trigger the following actions:

1. Execute code on one or more servers in the internal system.
2. Exfiltrate confidential information.

Perceptual positions

- Orange Cyberdefense
  - Threat Intelligence
  - Ethical hacker
  - Criminal mindset = adversary, hacker
- The customer = you
- Neutral observer

Selected threat groups

Threat groups who are active in the financial sector:

Attack group name	Associated groups
admin@338	
Andariel	Silent Chollima
APT-C-36	Blind Eagle
APT18	TG-0416, Dynamite Panda, Threat Group-0416
APT19	Codoso, C0d0so0, Codoso Team, Sunshop Group
APT38	NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima
APT41	WICKED PANDA
BlackTech	Palmerworm
Blue Mockingbird	

MITRE ATT&CK filters

Filters applied to the MITRE ATT&CK navigator.

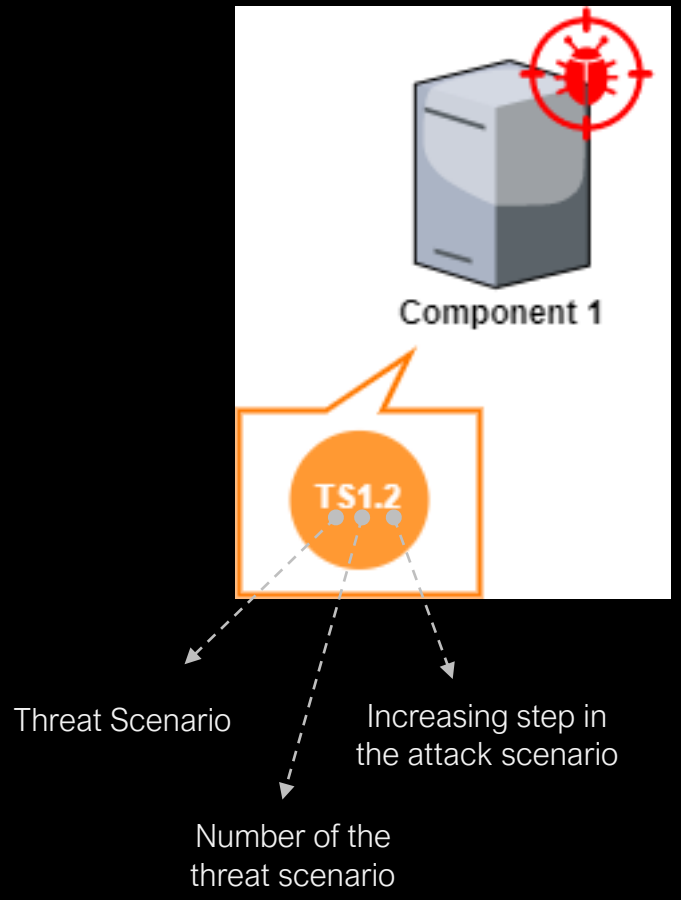
Platforms:

- Linux
- Network
- PRE (Preparatory techniques)
- Containers
- SaaS

Data sources currently collected

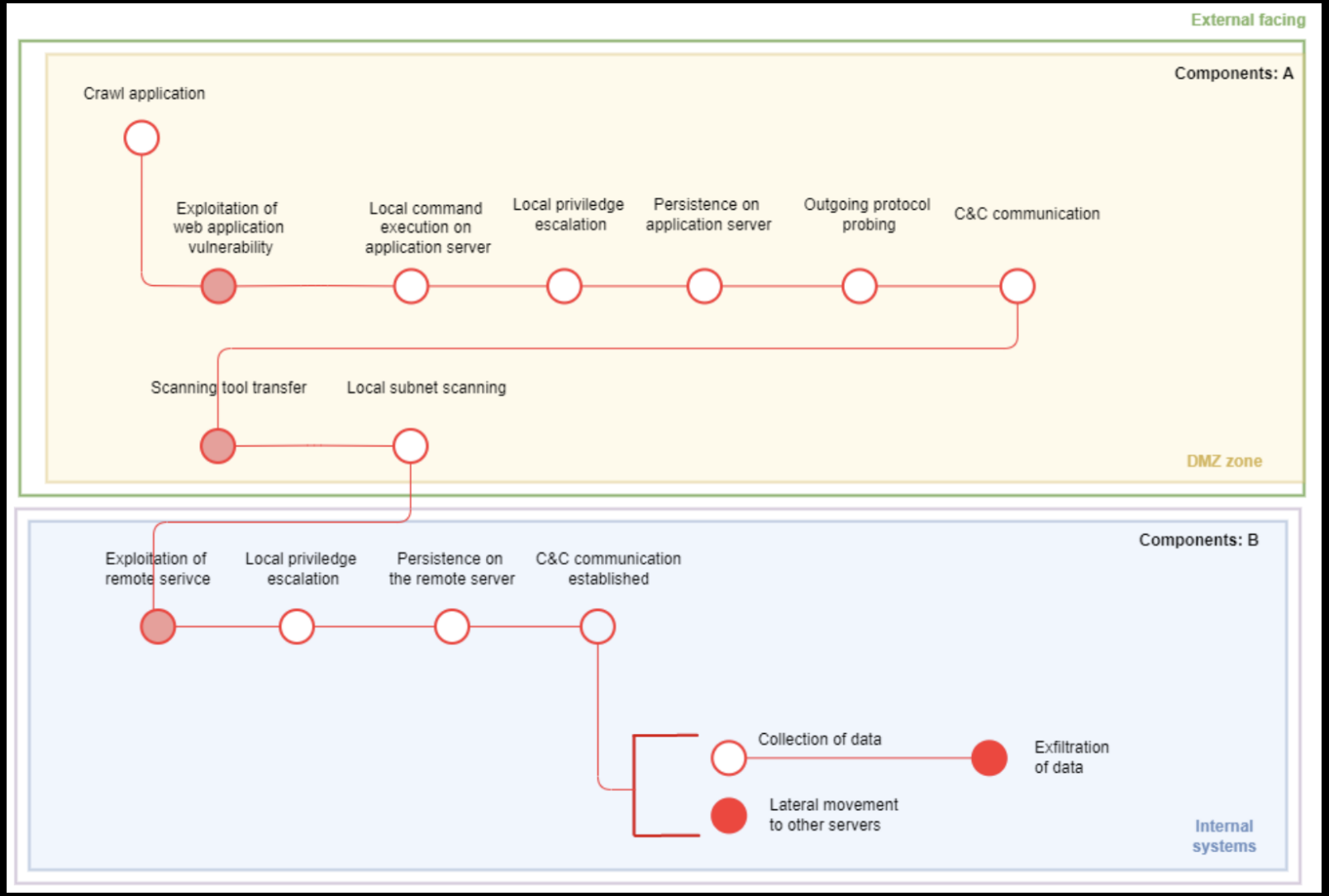
1. Syslog of the Operating systems
2. Access logs of the Load balancers
3. Events of the Intrusion Detection System
4. Events of the Firewall.

Refine the threat scenario - (2) Architectural system overview

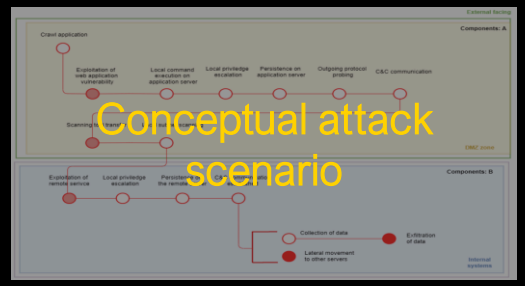


Refine the threat scenario - (3) Offensive part

Conceptual attack scenario



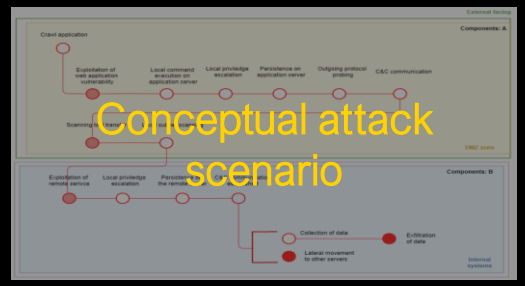
Refine the threat scenario - (3) Offensive part



High-level steps of the attack scenario →

Unified kill chain stage	Component A	Component B
Reconnaissance	TS1.1: Crawl application	TS1.9: Local subnet scanning
Weaponization		
Defense Evasion	TS1.3: Local command execution on application server	
Delivery		
Exploitation	TS1.2: Exploitation of web application vulnerability	TS1.10: Exploitation of remote service
Persistence	TS1.5 : Persistance on application server	TS1.12: Persistence on the remote server
Command & Control	TS1.6: Outgoing protocol probing TS1.7: C&C communication	TS1.13: C&C communication
Pivoting		
Privilege Escalation	TS1.4: Local privilege escalation	TS1.11: Local privilege escalation
Discovery		
Lateral Movement		TS1.14B: Lateral movement to other C-SOC core systems
Execution		
Credential Access		
Target Manipulation / Impact		
Collection		TS1.14A: Collection of data
Exfiltration		TS1.15: Exfiltration of data
Impact		

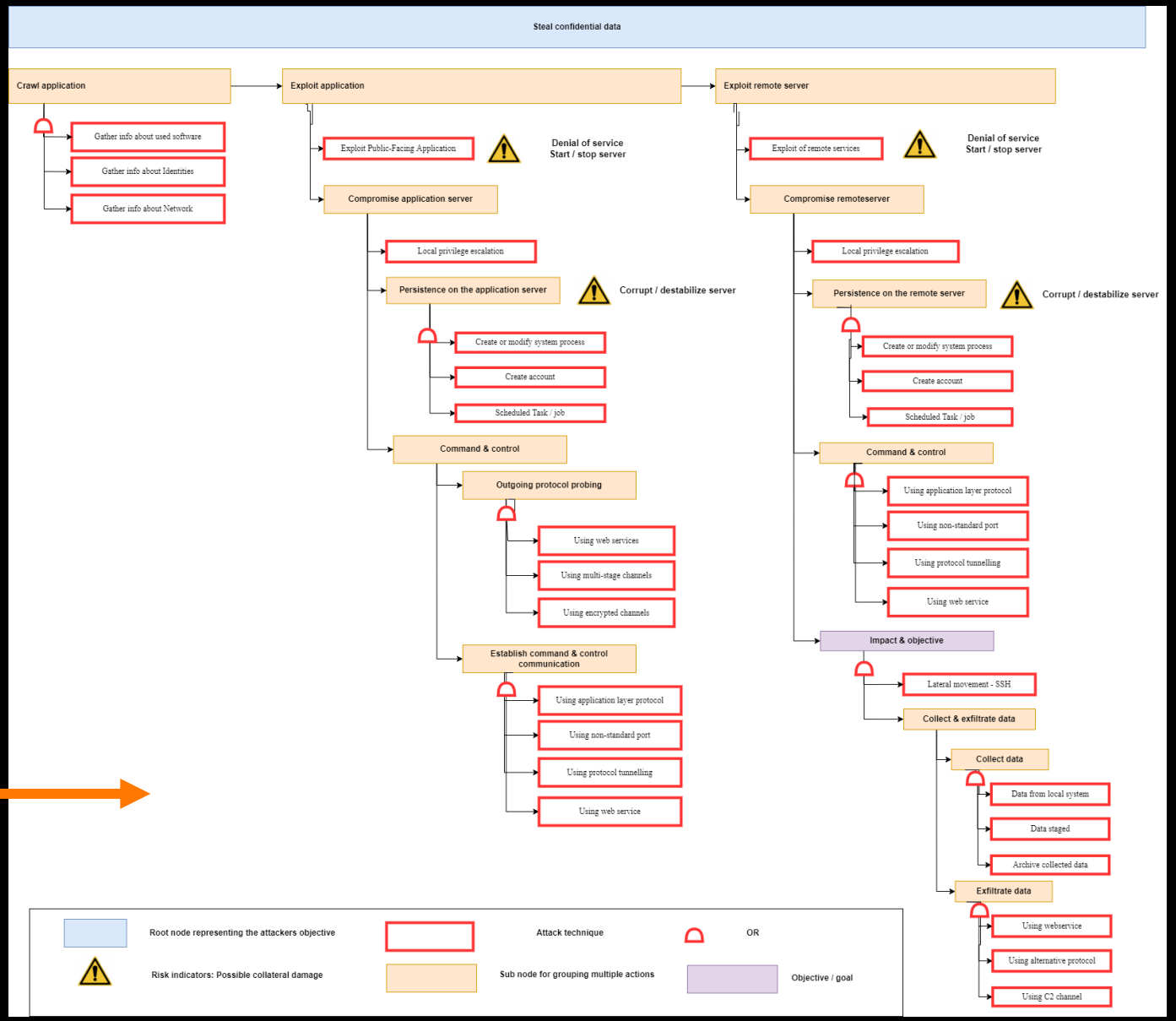
Refine the threat scenario - (3) Offensive part



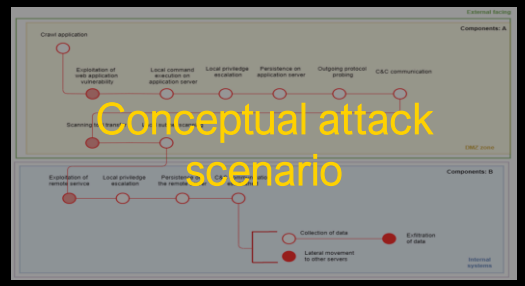
Unified kill chain stage	Component A	Component B
Reconnaissance	TS1.1: Crawl application	TS1.9: Local subnet scanning
Weaponization		
Defense Evasion	TS1.3: Local command execution on application server	
Delivery		
Exploitation	TS1.2: Exploitation of web application vulnerability	TS1.10: Exploitation of remote service
Persistence	TS1.5 : Persistance on application server	TS1.12: Persistence on the remote server
Command & Control	TS1.6: Outgoing protocol probing TS1.7: C&C communication	
Pivoting		
Privilege Escalation	[illegible]	[illegible]
Discovery		
Lateral Movement		TS1.14B: Lateral movement to other C-SOC core systems
Execution		
Credential Access		
Target Manipulation / Impact		
Collection		TS1.14A: Collection of data
Exfiltration		TS1.15: Exfiltration of data
Impact		

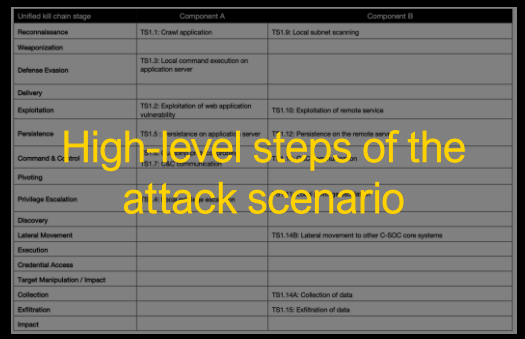
High-level steps of the attack scenario

Scenario attack tree



Refine the threat scenario - (3) Offensive part





Id	Action	MITRE ATT&CK mapping		Stage	Description	Component
TS1.9	Local subnet scanning	T1046	Network Service Discovery	Reconnaissance	Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.	A: Application server
TS1.10	The exploitation of a remote service	T1210	The exploitation of Remote Services	Exploitation	Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.	B: Database server
TS1.11	Local privilege escalation	T1068	Exploitation for Privilege Escalation	Privilege Escalation	Adversaries may exploit software vulnerabilities to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.	B: Database server

Details of the attack scenario

Refine the threat scenario - (4) Defensive part

Implemented detection points

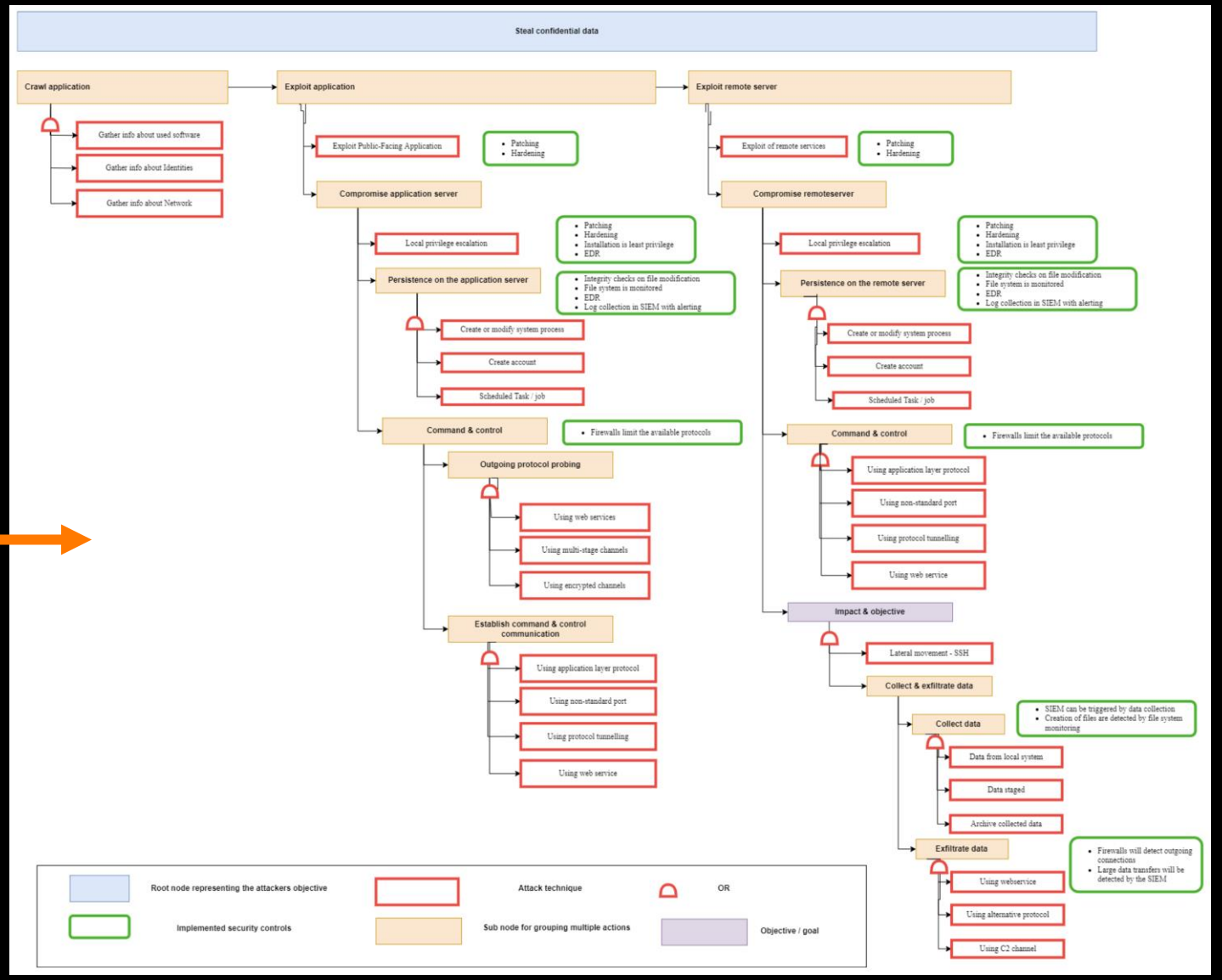
- Network security devices
- Vulnerability assessment and penetration testing
- Anti-Advanced Persistent Threats (AAPT)
- Endpoint detection and response (EDR) security technology
- Security Information and Event Management (SIEM) systems
- Flow collectors (network traffic analysis)
- Cyber Threat Intelligence (CTI/TI)

Refine the threat scenario - (4) Defensive part

- Network security devices
- Vulnerability assessment and penetration testing
- Anti-Advanced Persistent Threats (AAPT)
- Endpoint [illegible] technology
- Security Information and Event Management (SIEM) systems
- Flow collectors (network traffic analysis)
- Cyber Threat Intelligence (CTI/TI)

Implemented detection points

Attack defense tree



Refine the threat scenario - (4) Defensive part

- Network security devices
- Vulnerability assessment and penetration testing
- Anti-Advanced Persistent Threats (AAPT)
- Endpoint [illegible] technology
- Security Information and Event Management (SIEM) systems
- Flow collectors (network traffic analysis)
- Cyber Threat Intelligence (CTI/TI)

Implemented detection points

Attack defense tree

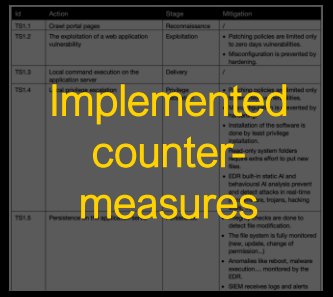
Implemented countermeasures

Id	Action	Stage	Mitigation
TS1.1	Crawl portal pages	Reconnaissance	/
TS1.2	The exploitation of a web application vulnerability	Exploitation	• Patching policies are limited only to zero days vulnerabilities. • Misconfiguration is prevented by hardening.
TS1.3	Local command execution on the application server	Delivery	/
TS1.4	Local privilege escalation	Privilege Escalation	• Patching policies are limited only to zero days vulnerabilities. • Misconfiguration is prevented by hardening. • Installation of the software is done by least privilege installation. • Read-only system folders require extra effort to put new files. • EDR built-in static AI and behavioural AI analysis prevent and detect attacks in real-time (ransomware, trojans, hacking tools, ...)
TS1.5	Persistence on the application server	Persistence	• Integrity checks are done to detect file modification. • The file system is fully monitored (new, update, change of permission...) • Anomalies like reboot, malware execution.... monitored by the EDR. • SIEM receives logs and alerts

Refine the threat scenario - (4) Defensive part

- Network security devices
- Vulnerability assessment and penetration testing
- Anti-Advanced Persistent Threats (AAPT)
- Endpoint [illegible] (EDR) [illegible] technology
- Security Information and Event Management (SIEM) systems
- Flow collectors (network traffic analysis)
- Cyber Threat Intelligence (CTI/TI)

Implemented detection points



		T1005	T1021.004	T1041	T1046	T1048	T1053	T1068	T1071	T1074	T1102	T1104	T1136	T1190	T1210	T1505.003	T1543	T1560	T1567	T1570	T1573	T1589.001	T1590.003	T1592.002
DS0017	**Command**	●		●	●	●	●			●			●				●	●		●				
DS0029	**Network Traffic**		●	●	●	●			●		●	●		●	●	●				●	●			
DS0015	Application Log													●	●	●								
DS0027	Driver							●									●							
DS0022	**File**	●		●		●	●			●						●	●	●		●				
DS0009	**Process**	●	●				●						●			●	●	●		●				
DS0019	Service																●							
DS0003	Scheduled Job						●																	
DS0002	User account												●											
DS0023	Named pipe																			●				
DS0033	Network share																			●				
DS0012	Script																	●	●					
DS0028	Logon Session		●																					
DS0035	Internet scan																							●

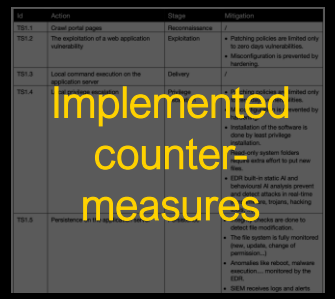
Data source mapping

Refine the threat scenario - (4) Defensive part

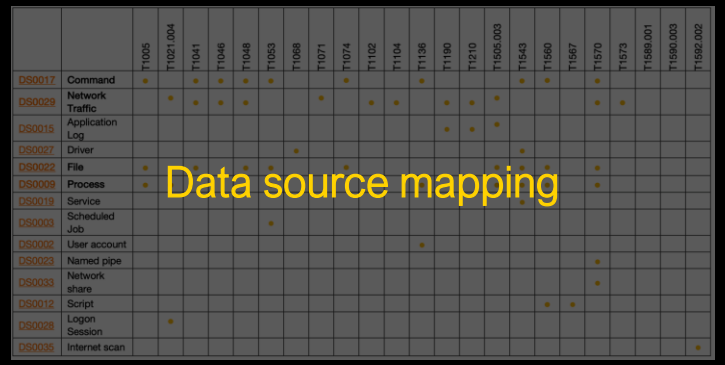
- Network security devices
- Vulnerability assessment and penetration testing
- Anti-Advanced Persistent Threats (AAPT)
- Endpoint [illegible] technology
- Security Information and Event Management (SIEM) systems
- Flow collectors (network traffic analysis)
- Cyber Threat Intelligence (CTI/TI)

Implemented detection points

Attack defense tree



Implemented counter measures



Data source mapping

Detection capability scoring

Id	Action	Detection capability		Stage
TS1.1	Crawl application	T1592.002 T1589.001 T1590.003	?	Reconnaissance
TS1.2	The exploitation of a web application vulnerability	T1190	?	Exploitation
TS1.3	Local command execution on the application server			Delivery
TS1.4	Local privilege escalation	T1068	?	Privilege Escalation
TS1.5	Persistence on the application server	T1543 T1136 T1053	?	Persistence
TS1.6	Outgoing protocol probing	T1102 T1104 T1573	?	Command & Control
TS1.7	C&C communication	T1071 T1571 T1572 T1102	?	Command & Control
TS1.8	Scanning tool transfer	T1570	?	Delivery
TS1.9	Local subnet scanning	T1046	?	Reconnaissance
TS1.10	The exploitation of a remote service	T1210	⊖	Exploitation
TS1.11	Local privilege escalation	T1068	⊖	Privilege Escalation
TS1.12	Persistence on the remote server	T1505.003	⊖	Persistence
TS1.13	C&C communication	T1071	?	Command &

✓ This attack will most probably be detected

? It is uncertain whether this attack is detected

⊖ This attack will most probably remain undetected

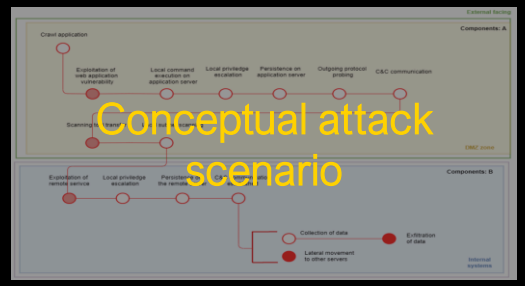
Comprehending potential threats, attack vectors, risks, and their business impact is a critical factor that sets apart cybersecurity excellence from cybersecurity in the mainstream.

Cyberdefense

Thank you!

Etienne Verhasselt, Team lead Application Security & Ethical hacking
Koen Vanderloock, Senior Application Security Consultant & Threat Modeler

Refine the threat scenario - (3) Offensive part



Scenario attack tree