

Keep Pace

Freddy Dezeure
DCISO for Europe



Agenda

1

How Microsoft protects Microsoft
Active defense - at world scale

2

AI Agents at work
Train and contain your agents

3

Frontier AI models
Insights for patching, and more

4

Prepare for resilience
Minimal viable service

How Microsoft protects Microsoft

Active defense - at world scale



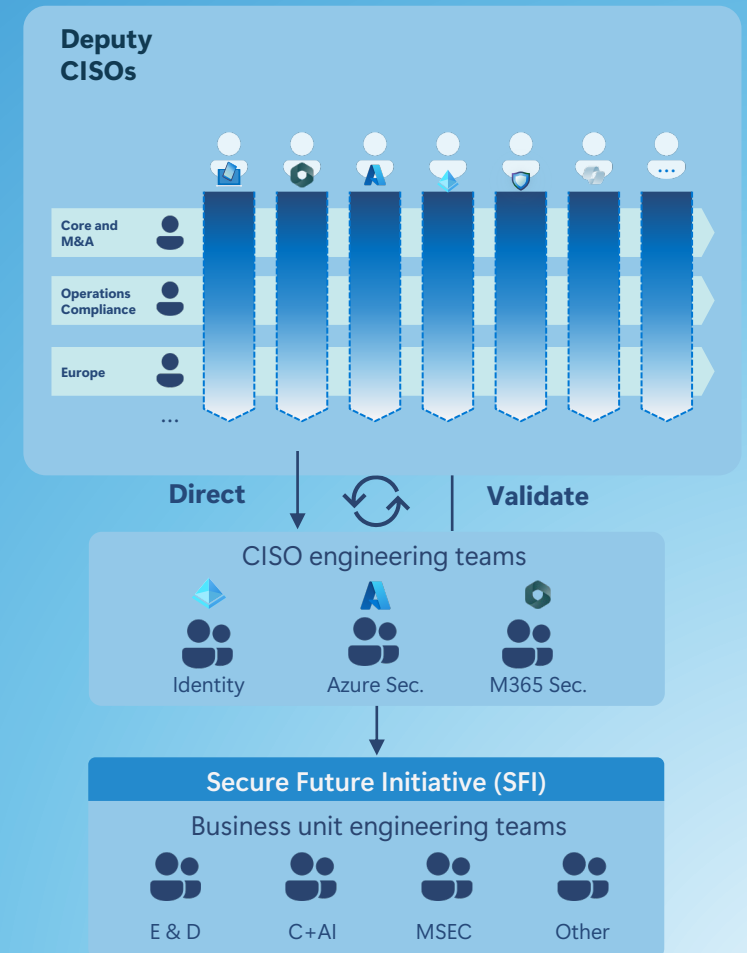
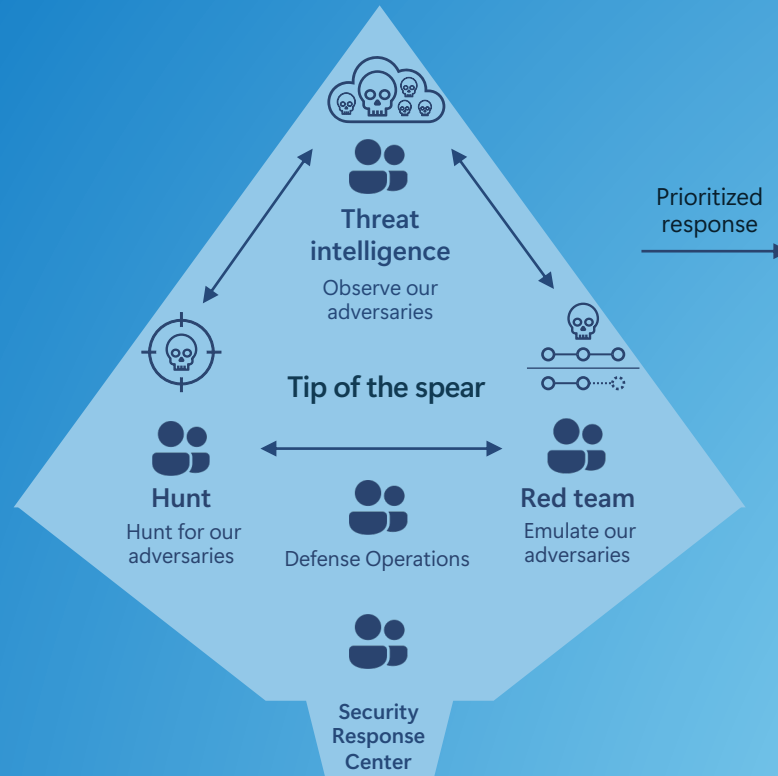
CISO Org - Impactful structure and operation

Cross-function expertise
and decision making

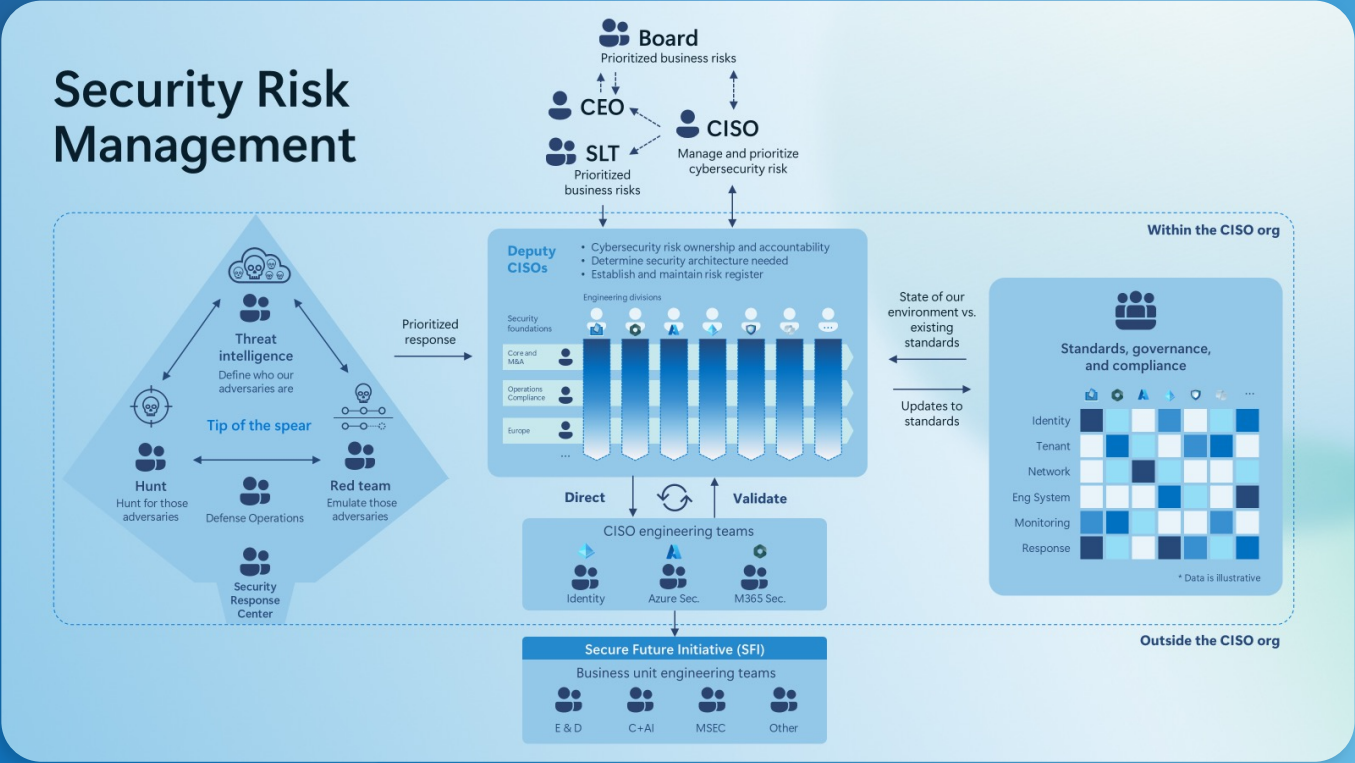
Quasi real-time
threat-informed defense

Visibility and impact at scale

Durable improvements in
infrastructure and services



Active defense at scale



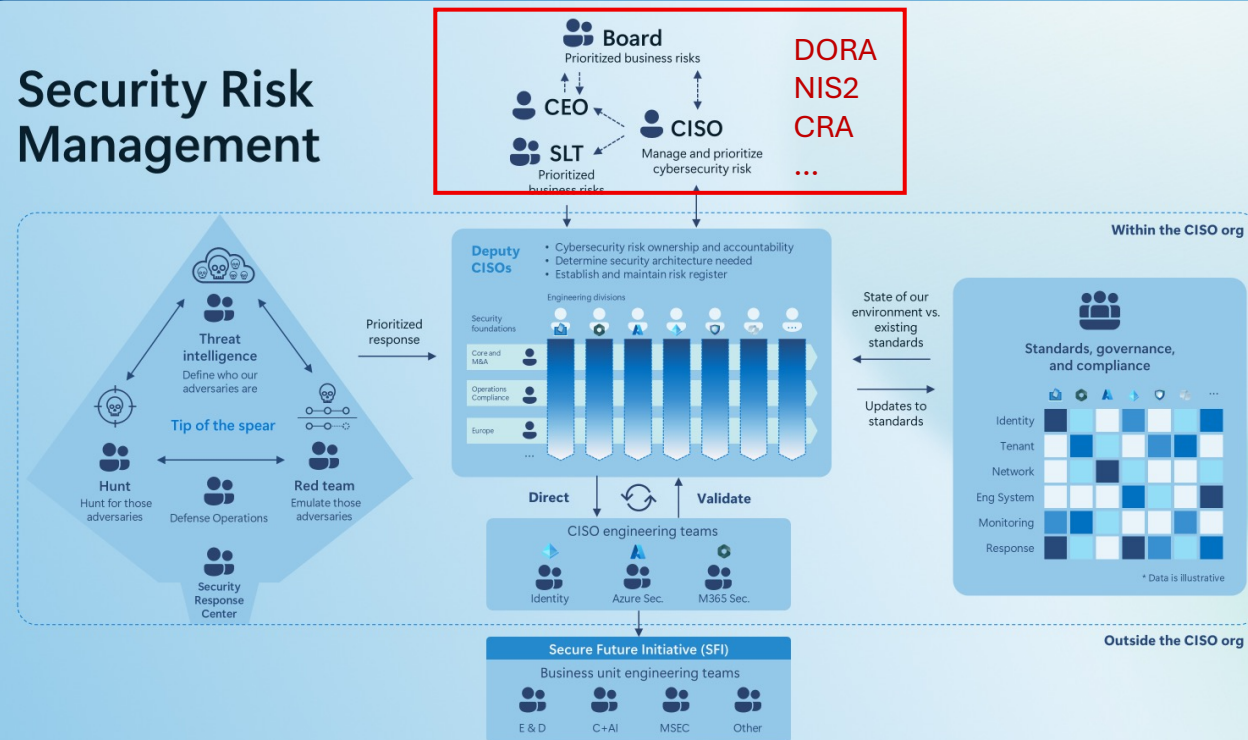
Microsoft
tenants

Customer
tenants

Microsoft infrastructure and
services

Board reporting

Security Risk Management



Microsoft
tenants

Customer
tenants

Microsoft infrastructure and
services

AI Agents at work

Train and contain your agents





AI Agents

AI agents

- 🛡️ Democratization of development – fast adoption
- 🛡️ Gaps in our understanding of Agent behaviour
 - Non-deterministic
 - Autonomous
 - Agent-to-agent cooperation
 - Pace of execution
- 🛡️ Lack of “social systems”
- 🛡️ Agents may become our adversaries



PRODUCT

CONFIGURATION

Traditional control frameworks



Product

- Safety and security controls that customers cannot override
- Prompt controls, model drift, training and avoidance of bias, predictability, explainability and transparency.
- OWASP AI, NIST AI RMF, AIUC-1



Configuration

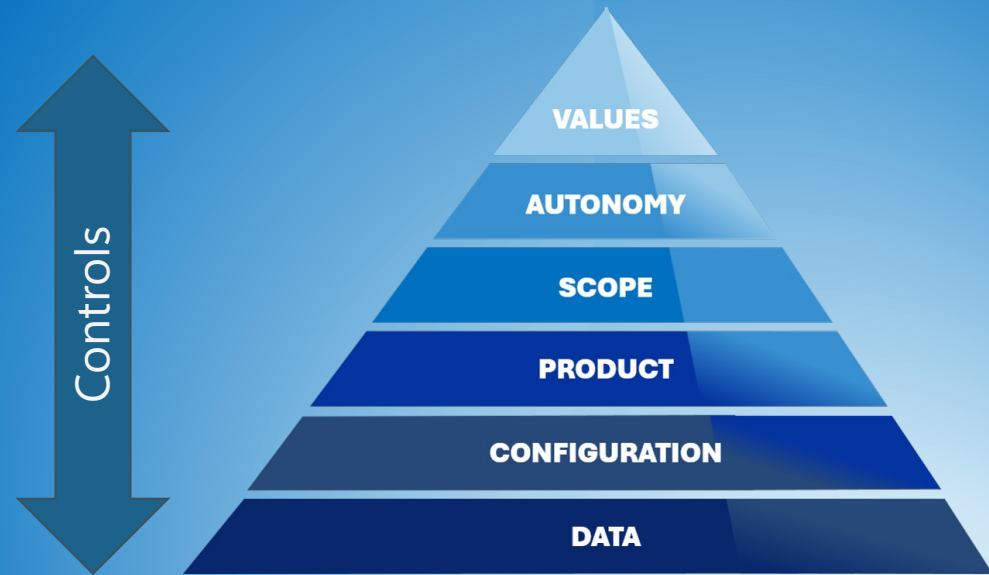
- Customer determines specific implementation
- Asset management, identity management, minimum privilege, network segmentation, access controls, supply chain risk, monitoring.
- NIST CSF, NIST 800-53, ISO 27001, ISO 42001
- CIS Baselines



Update frequency not at pace



Coverage not sufficient



Extending our coverage

🛡️ Values

- 🛡️ AI should respect corporate values, ethical and regulatory requirements

🛡️ Autonomy

- 🛡️ Can AI modify, delete data? Can it carry out financial transactions and to which threshold? Can it launch physical action?
- 🛡️ Is AI allowed to take initiatives?
- 🛡️ Is a human-in-the-loop required for critical actions?
- 🛡️ Do we have an "off switch"? Can we activate it automatically?
- 🛡️ Is AI backing up state before executing, can we roll back its actions?
- 🛡️ Can AI resist human oversight?

🛡️ Scope

- 🛡️ To what data, services, systems AI has access?
- 🛡️ Does AI have access to the internet and to other AI tools?
- 🛡️ What is its primary role and success factors?
- 🛡️ Do we have an AI insider risk program?

🛡️ Data layer is the foundation

- 🛡️ Data and services provenance, lineage, classification, integrity

Humanist AI

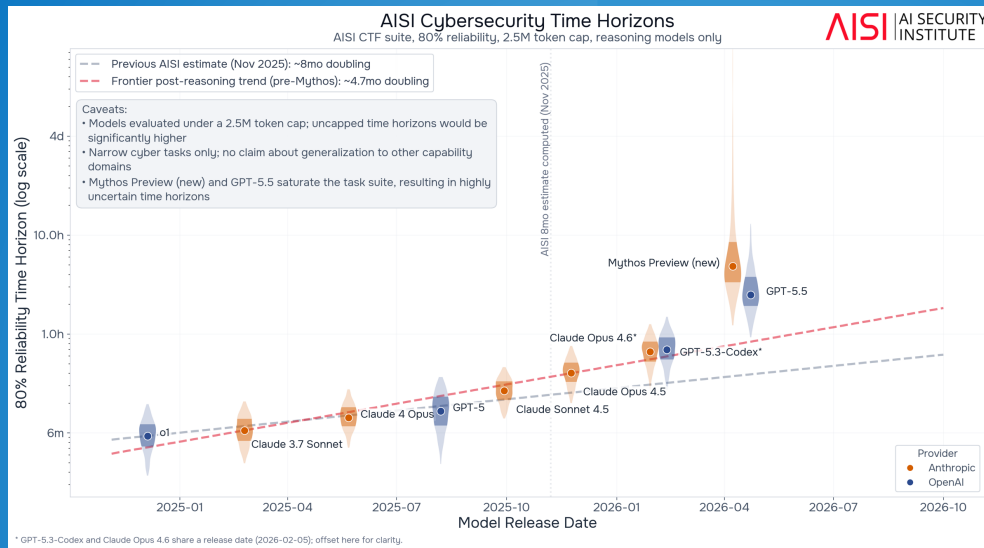
Code of Conduct



Frontier AI models Insights for patching, and more



Frontier Models

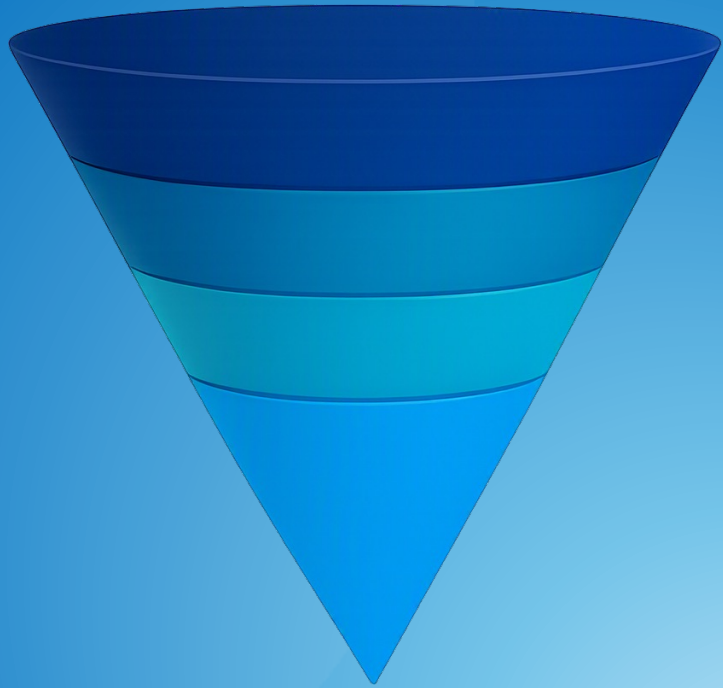


- 🛡 Finding vulnerabilities in code, faster*
- 🛡 Building exploits, faster (even based on binaries)
- 🛡 Allowing autonomous attacks**
- 🛡 Continuously improving
- 🛡 Accessible to our adversaries

* [How fast is autonomous AI cyber capability advancing? | AISI Work](#)

** [jadepuffer-agentic-ransomware-for-automated-database-extortion](#)

Glasswing insights



- 🛡️ Non-deterministic, multiple runs required
- 🛡️ "Harnesses" matter, a lot
- 🛡️ Large number of findings
- 🛡️ Triage, prioritization, remediation process
- 🛡️ Large impact on resources (FTEs, tokens)
- 🛡️ Continuous scanning of old and new code



Keep Pace

What can you do?

🛡️ Scan your own software

- Don't wait, use a harness + available models
- Prepare for a continuous process

🛡️ Patch overnight

- Allocate resources, change your policies, measure, report*
- Prioritize identity management, edge devices
- Can we break production to patch our systems?

🛡️ Limit exposure

- Replace legacy software if you can, isolate if you can't
- Respond to incidents at pace
- Defend in depth**

* BOD 26-04: Prioritizing Security Updates Based on Risk | CISA

** <https://sip.security.microsoft.com/securenow>

Microsoft Baseline Security Mode*

Hardening our digital defenses with Microsoft Baseline Security Mode

November 18, 2025 | Jason Kellington



- 🛡️ Benefit from how Microsoft protects Microsoft
- 🛡️ Staged rollout with built-in impact analysis, exclusions
- 🛡️ New tenants will come with BSM controls by default
- 🛡️ V1: 18 secure settings
- 🛡️ V2: 25 additional settings across Microsoft 365, Entra, Intune, Purview, Dynamics 365, and Azure

* [Baseline security mode](#)





[Best practices](#) • October 5 • 6 min read

CISO perspectives on managing vulnerability risks in the age of AI

By [Freddy Dezeure](#) and [Sesha Mani](#)

[Listen to this post](#)

0:00 / 0:00

1X



Prepare for resilience

Minimal viable service



MITRE ATT&CK

Initial Access 11 techniques	Execution 20 techniques	Persistence 22 techniques	Privilege Escalation 13 techniques	Stealth 30 techniques	Defense Impairment 18 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Content Injection	BITS Jobs	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Access Token Manipulation (0/5)	Disable or Modify System Firewall (0/3)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/5)	Automated Exfiltration (0/1)	Account Access Removal
Drive-by Compromise	Cloud Administration Command	BITS Jobs	Access Token Manipulation (0/5)	BITS Jobs	Disable or Modify Tools (0/6)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (0/1)
Exploit Public-Facing Application	Command and Scripting Interpreter (0/13)	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/7)	Build Image on Host	Domain or Tenant Policy Modification (0/2)	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Debugger Evasion	Downgrade Attack	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing (0/4)	ESXi Administration Command	Compromise Host Software Binary	Create Account (0/3)	Direct Volume Access	File and Directory Permissions Modification (0/2)	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Replication Through Removable Media	Exploitation for Client Execution	Event Triggered Execution (0/18)	Create or Modify System Process (0/5)	Execution Guardrails (0/2)	Modify Authentication Process (0/9)	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Scheduled Transfer	Email Bombing
Supply Chain Compromise (0/3)	Hijack Execution Flow (0/12)	Exclusive Control	Domain or Tenant Policy Modification (0/2)	Exploitation for Stealth	Modify Cloud Compute Infrastructure (0/5)	Multi-Factor Authentication Interception	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Transfer Data to Cloud Account	Endpoint Denial of Service (0/4)
Trusted Relationship	Input Injection	External Remote Services	Escape to Host	Hide Artifacts (0/14)	Modify Registry	Multi-Factor Authentication Request Generation	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/6)	Hide Infrastructure		Financial Theft
Valid Accounts (0/4)	Inter-Process Communication (0/3)	Implant Internal Image	Event Triggered Execution (0/18)	Hijack Execution Flow (0/12)	Modify System Image (0/2)	Network Sniffing	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Firmware Corruption
Wi-Fi Networks	Native API	Modify Authentication Process (0/9)	Exploitation for Privilege Escalation	Indicator Removal (0/8)	Network Boundary Bridging (0/1)	OS Credential Dumping (0/8)	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
	Poisoned Pipeline Execution	Modify Registry	Process Injection (0/12)	Indirect Command Execution	Plist File Modification	Steal Application Access Token	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
	Scheduled Task/Job (0/5)	Power Settings	Scheduled Task/Job (0/5)	Masquerading (0/12)	Prevent Command History Logging	Steal or Forge Authentication Certificates	Group Policy Discovery		Email Collection (0/3)	Non-Standard Port		Resource Hijacking (0/4)
	Serverless Execution	Pre-OS Boot (0/5)	Valid Accounts (0/4)	Obfuscated Files or Information (0/18)	Rogue Domain Controller	Steal or Forge Kerberos Tickets (0/5)	Local Storage Discovery		Input Capture (0/4)	Protocol Tunneling		Service Stop
	Shared Modules	Scheduled Task/Job (0/5)		Pre-OS Boot (0/5)	Safe Mode Boot	Steal Web Session Cookie	Log Enumeration		Screen Capture	Proxy (0/4)		System Shutdown/Reboot
	Software Deployment Tools	Office Application Startup (0/6)		Process Injection (0/12)	Subvert Trust Controls (0/6)	Unsecured Credentials (0/8)	Network Service Discovery		Video Capture	Remote Access Tools (0/3)		
	System Services (0/3)	Power Settings		Reflective Code Loading	Weaken Encryption (0/2)		Network Share Discovery			Traffic Signaling (0/2)		
	Trusted Developer Utilities Proxy Execution (0/3)	Pre-OS Boot (0/5)		Rootkit			Password Policy Discovery			Web Service (0/3)		
	User Execution (0/5)	Scheduled Task/Job (0/5)		Selective Exclusion			Peripheral Device Discovery					
	Windows Management Instrumentation		IIS Components	Social Engineering (0/2)			Permission Groups Discovery (0/3)					
			SQL Stored Procedures	System Binary Proxy Execution (0/14)			Process Discovery					
			Terminal Services DLL	System Script Proxy Execution (0/2)			Query Registry					
			Transport Agent	Template Injection			Remote System Discovery					
			vSphere Installation Bundles	Traffic Signaling (0/2)			Software Discovery (0/2)					
			Web Shell	Trusted Developer Utilities Proxy Execution (0/3)			System Information Discovery					
				Unused/Unsupported Cloud Regions			System Location Discovery (0/1)					
				Valid Accounts (0/4)			System Network Configuration Discovery (0/2)					

MITRE ATT&CK – attack flow

Initial Access 11 techniques	Execution 20 techniques	Persistence 22 techniques	Privilege Escalation 13 techniques	Stealth 30 techniques	Defense Impairment 18 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Content Injection	BITS Jobs	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Access Token Manipulation (0/5)	Disable or Modify System Firewall (0/5)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/5)	Automated Exfiltration (0/1)	Account Access Removal
Drive-by Compromise	Cloud Administration Command	BITS Jobs		BITS Jobs	Disable or Modify Tools (0/6)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (0/1)
Exploit Public-Facing Application	Command and Scripting Interpreter (0/13)	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	Build Image on Host	Domain or Tenant Policy Modification (0/2)	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Debugger Evasion	Downgrade Attack (0/2)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel (0/3)	Data Manipulation (0/3)
Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Delay Execution	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing (0/4)	ESXi Administration Command	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	File and Directory Permissions Modification (0/2)	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Replication Through Removable Media	Exploitation for Client Execution	Create Account (0/3)	Create or Modify System Process (0/5)	Direct Volume Access	Modify Authentication Process (0/9)	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Email Bombing
Supply Chain Compromise (0/3)	Hijack Execution Flow (0/12)	Event Triggered Execution (0/18)	Domain or Tenant Policy Modification (0/2)	Execution Guardrails (0/2)	Modify Cloud Compute Infrastructure (0/5)	Modify Authentication Process (0/9)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Trusted Relationship	Input Injection	Exclusive Control	Escape to Host	Exploitation for Stealth	Indicator Removal (0/8)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/6)	Hide Infrastructure	Scheduled Transfer	Financial Theft
Valid Accounts (0/4)	Inter-Process Communication (0/3)	External Remote Services	Event Triggered Execution (0/18)	Hide Artifacts (0/14)	Indirect Command Execution	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Wi-Fi Networks	Native API	Implant Internal Image	Event Triggered Execution (0/18)	Hijack Execution Flow (0/12)	Masquerading (0/12)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
	Poisoned Pipeline Execution	Modify Authentication Process (0/9)	Exploitation for Privilege Escalation	Indicator Removal (0/8)	Modify Cloud Resource Hierarchy	OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
	Scheduled Task/Job (0/5)	Modify Registry	Process Injection (0/12)	Indirect Command Execution	Modify Registry	Steal Application Access Token	Local Storage Discovery		Email Collection (0/3)	Non-Standard Port		Resource Hijacking (0/4)
	Serverless Execution	Office Application Startup (0/6)	Scheduled Task/Job (0/5)	Masquerading (0/12)	Modify System Image (0/2)	Steal or Forge Kerberos Tickets (0/5)	Log Enumeration		Input Capture (0/4)	Protocol Tunneling		Service Stop
	Shared Modules	Power Settings	Valid Accounts (0/4)	Masquerading (0/12)	Network Boundary Bridging (0/1)	Steal Web Session Cookie	Network Service Discovery		Screen Capture	Proxy (0/4)		System Shutdown/Reboot
	Software Deployment Tools	Pre-OS Boot (0/5)		Obfuscated Files or Information (0/18)	Plist File Modification	Unsecured Credentials (0/8)	Network Share Discovery		Video Capture	Remote Access Tools (0/3)		
	System Services (0/3)	Scheduled Task/Job (0/5)		Pre-OS Boot (0/5)	Prevent Command History Logging		Network Sniffing			Traffic Signaling (0/2)		
	Trusted Developer Utilities Proxy Execution (0/3)			Process Injection (0/12)	Rogue Domain Controller		Password Policy Discovery			Web Service (0/3)		
	User Execution (0/5)			Reflective Code Loading	Safe Mode Boot		Peripheral Device Discovery					
	Windows Management Instrumentation		IIS Components	Rootkit	Subvert Trust Controls (0/6)		Permission Groups Discovery (0/3)					
			SQL Stored Procedures	Selective Exclusion	Weaken Encryption (0/2)		Process Discovery					
			Terminal Services DLL	Social Engineering (0/2)			Query Registry					
			Transport Agent	System Binary Proxy Execution (0/14)			Remote System Discovery					
			vSphere Installation Bundles	System Script Proxy Execution (0/2)			Software Discovery (0/2)					
			Web Shell	Template Injection			System Information Discovery					
				Traffic Signaling (0/2)			System Location Discovery (0/1)					
				Trusted Developer Utilities Proxy Execution (0/3)			System Network Configuration Discovery (0/2)					
				Unused/Unsupported Cloud Regions								
				Valid Accounts (0/4)								

Incident response process



Identify

- When did the event happen?
- Has the source (point of entry) of the event been discovered?
- What is the scope of the compromise?
- Is it spreading?
- Does it affect operations?
- ...

Contain

- Limit spread and impact

MITRE ATT&CK – in fast forward

Initial Access 11 techniques	Execution 20 techniques	Persistence 22 techniques	Privilege Escalation 13 techniques	Stealth 30 techniques	Defense Impairment 18 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Content Injection	BITS Jobs	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Access Token Manipulation (0/5)	Disable or Modify System Firewall (0/5)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/5)	Automated Exfiltration (0/1)	Account Access Removal
Drive-by Compromise	Cloud Administration Command	BITS Jobs		BITS Jobs	Disable or Modify Tools (0/6)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (0/1)
Exploit Public-Facing Application	Command and Scripting Interpreter (0/1)	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	Build Image on Host	Domain or Tenant Policy Modification (0/2)	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Debugger Evasion	Downgrade Attack	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Defacement (0/2)
Hardware Additions			Boot or Logon Autostart Execution (0/14)	Deobfuscate/Decode Files or Information	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe
Phishing (0/4)	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	File and Directory Permissions Modification (0/2)	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Email Bombing
Replication Through Removable Media	ESXi Administration Command	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Execution Guardrails (0/2)	Hide Artifacts (0/14)	Input Capture (0/4)	Cloud Storage Object Discovery	Taint Shared Content	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Supply Chain Compromise (0/3)	Exploitation for Client Execution	Create Account (0/3)	Create or Modify System Process (0/5)	Exploitation for Stealth	Modify Authentication Process (0/9)	Modify Authentication Process (0/9)	Container and Resource Discovery	Use Alternate Authentication Material (0/4)	Data from Configuration Repository (0/2)	Fallback Channels	Scheduled Transfer	Financial Theft
Trusted Relationship	Hijack Execution Flow (0/12)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Hide Artifacts (0/14)	Modify Cloud Compute Infrastructure (0/5)	Multi-Factor Authentication Interception	Debugger Evasion		Data from Information Repositories (0/6)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Valid Accounts (0/4)	Input Injection	Event Triggered Execution (0/18)	Escape to Host	Indicator Removal (0/8)	Masquerading (0/12)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
Wi-Fi Networks	Inter-Process Communication (0/3)	Exclusive Control		Indirect Command Execution	Obfuscated Files or Information (0/18)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (0/2)
	Native API	External Remote Services		Masquerading (0/12)	Pre-OS Boot (0/5)	OS Credential Dumping (0/8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking (0/4)
	Poisoned Pipeline Execution	Implant Internal Image		Pre-OS Boot (0/5)	Process Injection (0/12)	Steal Application Access Token	Group Policy Discovery		Data Staged (0/2)	Non-Standard Port		Service Stop
	Scheduled Task/Job (0/5)	Modify Authentication Process (0/9)		Process Injection (0/12)	Reflective Code Loading	Steal or Forge Authentication Certificates	Local Storage Discovery		Email Collection (0/3)	Protocol Tunneling		System Shutdown/Reboot
	Serverless Execution	Modify Registry		Rootkit	Selective Exclusion	Steal or Forge Kerberos Tickets (0/5)	Log Enumeration		Input Capture (0/4)	Proxy (0/4)		
	Shared Modules	Office Application Startup (0/6)		Selective Exclusion	Social Engineering (0/2)	Unsecured Credentials (0/8)	Network Service Discovery		Screen Capture	Remote Access Tools (0/3)		
	Software Deployment Tools	Power Settings		Social Engineering (0/2)	System Binary Proxy Execution (0/14)		Network Share Discovery		Video Capture	Traffic Signaling (0/2)		
	System Services (0/3)	Pre-OS Boot (0/5)		System Binary Proxy Execution (0/14)	System Script Proxy Execution (0/2)		Network Sniffing			Web Service (0/3)		
	Trusted Developer Utilities Proxy Execution (0/3)	Scheduled Task/Job (0/5)		Template Injection	Traffic Signaling (0/2)		Password Policy Discovery					
	User Execution (0/5)	IIS Components		Traffic Signaling (0/2)	Trusted Developer Utilities Proxy Execution (0/3)		Peripheral Device Discovery					
	Windows Management Instrumentation	SQL Stored Procedures		Unused/Unsupported Cloud Regions	Valid Accounts (0/4)		Permission Groups Discovery (0/3)					
		Terminal Services DLL		Valid Accounts (0/4)			Process Discovery					
		Transport Agent					Query Registry					
		vSphere Installation Bundles					Remote System Discovery					
		Web Shell					Software Discovery (0/2)					
							System Information Discovery					
							System Location Discovery (0/1)					
							System Network Configuration Discovery (0/2)					

Incident response process



Identify

- When did the event happen?
- Has the source (point of entry) of the event been discovered?
- What is the scope of the compromise?
- Is it spreading?
- Does it affect operations?
- ...

Contain

- Limit spread and impact

Incident response process – in fast forward



Identify

- When did the event happen?
- Has the source (point of entry) of the event been discovered?
- What is the scope of the compromise?
- Is it spreading?
- Does it affect operations?
- **Limit spread and impact**
- ...

Identify

Contain

Minimal viable service

- 🛡️ Preserve resilience for your critical service
- 🛡️ Identify your most (and least) critical assets
- 🛡️ Obtain agreement to burn down least critical
- 🛡️ Identify trigger points in attack flow and infra
- 🛡️ Contain without perfect knowledge



Keep Pace

Wrapping up

- 🛡 The basics still matter, a lot
- 🛡 Update your risk assessments and playbooks
- 🛡 Expand your controls to agents
- 🛡 Prepare for resilience
- 🛡 Keep pace

Thank you!

Freddy Dezeure
DCISO for Europe

