SECURITY SUMMIT
Academy

Atelier

Linee guida per iniziative di Privileged Access Management di successo.

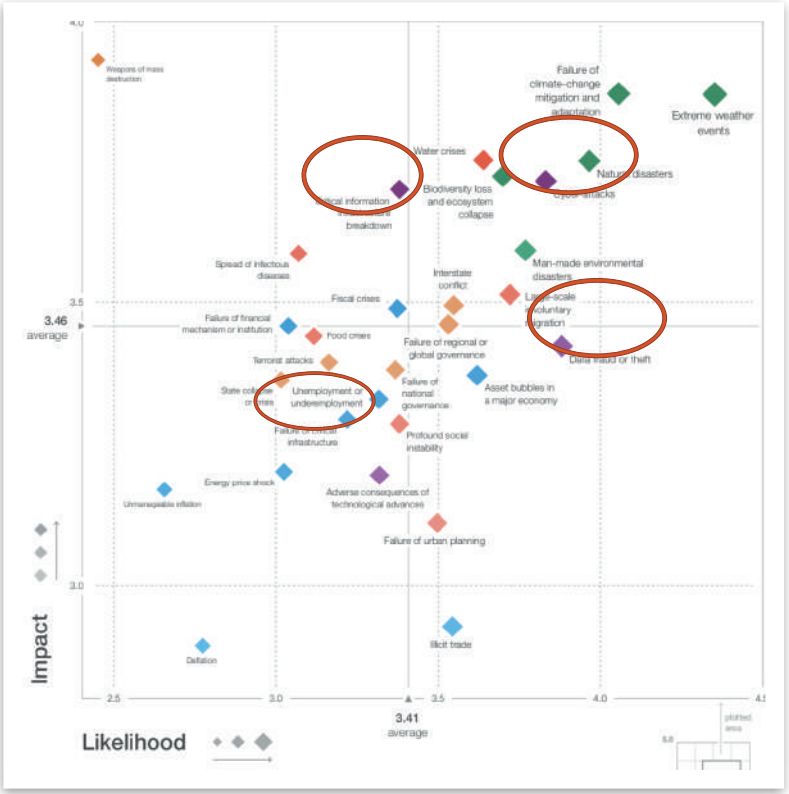
Luca Bechelli, Comitato Scientifico, Clusit
Massimo Carlotti, Sales Engineer - Italy and South EMEA,CyberArk

21 aprile 2020 orario 11-12 - StreamingEdition

#securitysummit #academy #streamingedition

Luca Bechelli

- Practice Leader Information & Cyber Security Advisory Team @ P4I
- Membro del Comitato Scientifico Clusit
- Coordinatore GdL «Security Readiness» presso l'Osservatorio «Cybersecurity & Data Protection» del Politecnico di Milano OSSERVATORI.NET digital innovation
- Direttore Didattico Master in Cybersecurity Experis Academy Experis ManpowerGroup



World Economic Forum:

- i cyber attacks rappresentano una minaccia molto probabile con un elevato impatto

20 anni Clusit

Rapporto Clusit 2020

sulla sicurezza ICT in Italia

Rapporto Clusit:

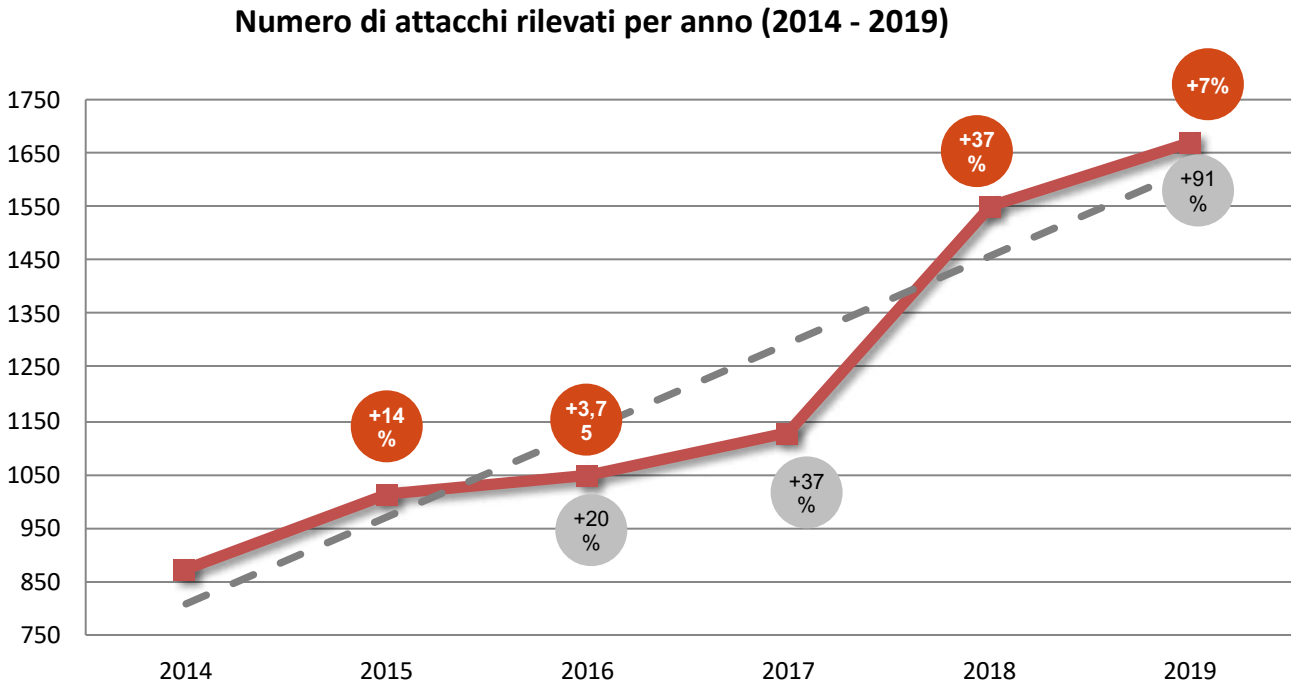
- +37% di attacchi rispetto alla media degli ultimi 6 anni
- Dal 2014 al 2019: +91% attacchi gravi
- Nel triennio 17-19 il numero degli attacchi gravi cresce di circa +50% rispetto al precedente

Il trend degli attacchi

Negli ultimi 9 anni 94 attacchi gravi di dominio pubblico al mese (129 nel 2018, 137 nel 2019)

- 10.087 attacchi gravi analizzati dal gennaio 2011 al dicembre 2019 (di cui 7.284 dal 2014).

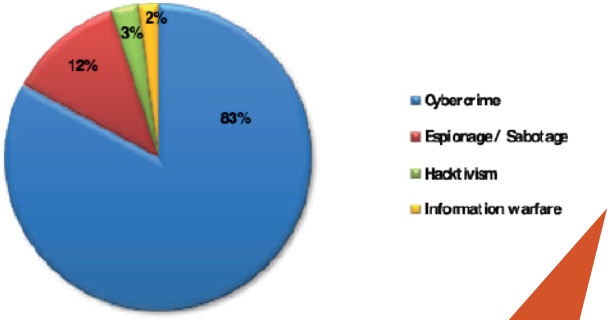
- 873 nel 2014
- 1.012 nel 2015
- 1.050 nel 2016
- 1.127 nel 2017
- 1.552 nel 2018
- 1.670 nel 2019



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

La crescita del cybercrime

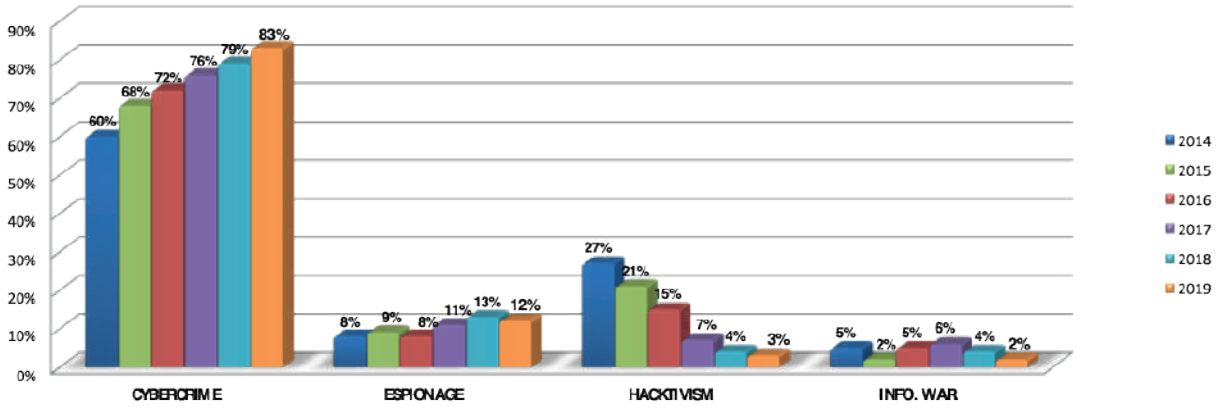
Tipologia e distribuzione degli attaccanti 2019



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

+162% rispetto al 2014

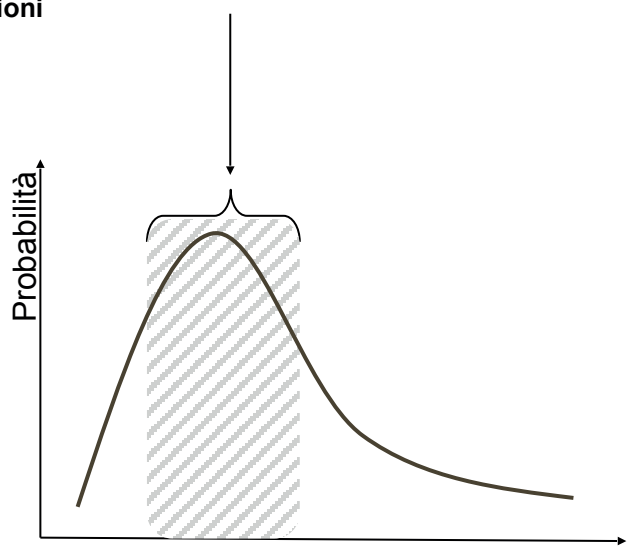
Distribuzione degli attaccanti 2014 - 2019



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Come dobbiamo interpretare questi dati?

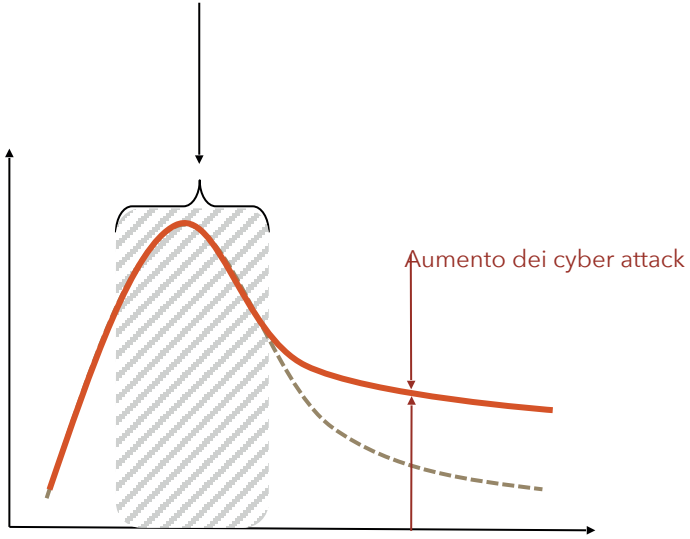
Information Security → Contesto → **Rischio sicurezza delle informazioni** → **“ieri”**



Come dobbiamo interpretare questi dati?

…security attacks in the Cyberspace have evolved from hacking for personal fame to […] Cybercrime. A plethora of tools and processes previously observed in isolated Cybersecurity incidents are now being used together in multi-blended attacks, often with far reaching malicious objectives

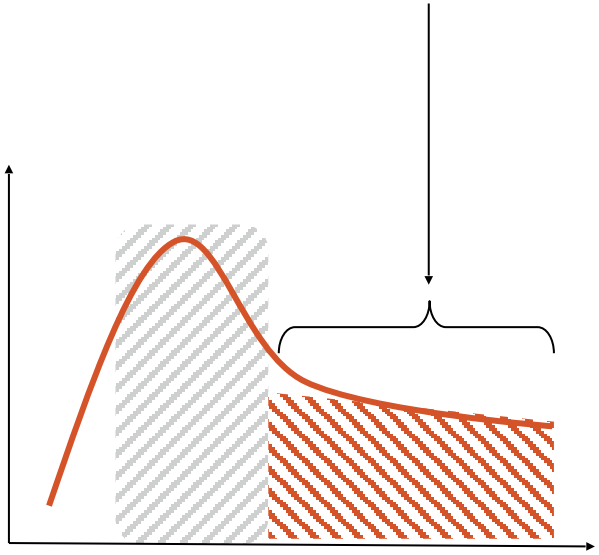
ISO 27032:2012



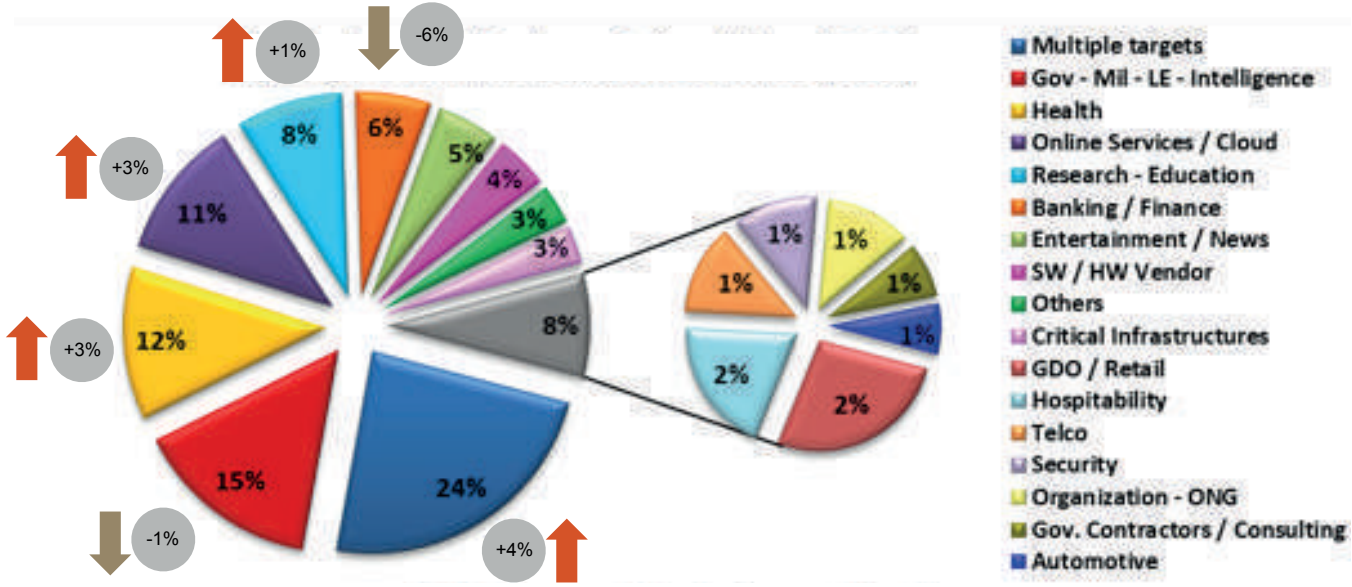
Come dobbiamo interpretare questi dati?

…security attacks in the Cyberspace have evolved from hacking for personal fame to […] Cybercrime. A plethora of tools and processes previously observed in isolated Cybersecurity incidents are now being used together in multi-blended attacks, often with far reaching malicious objectives

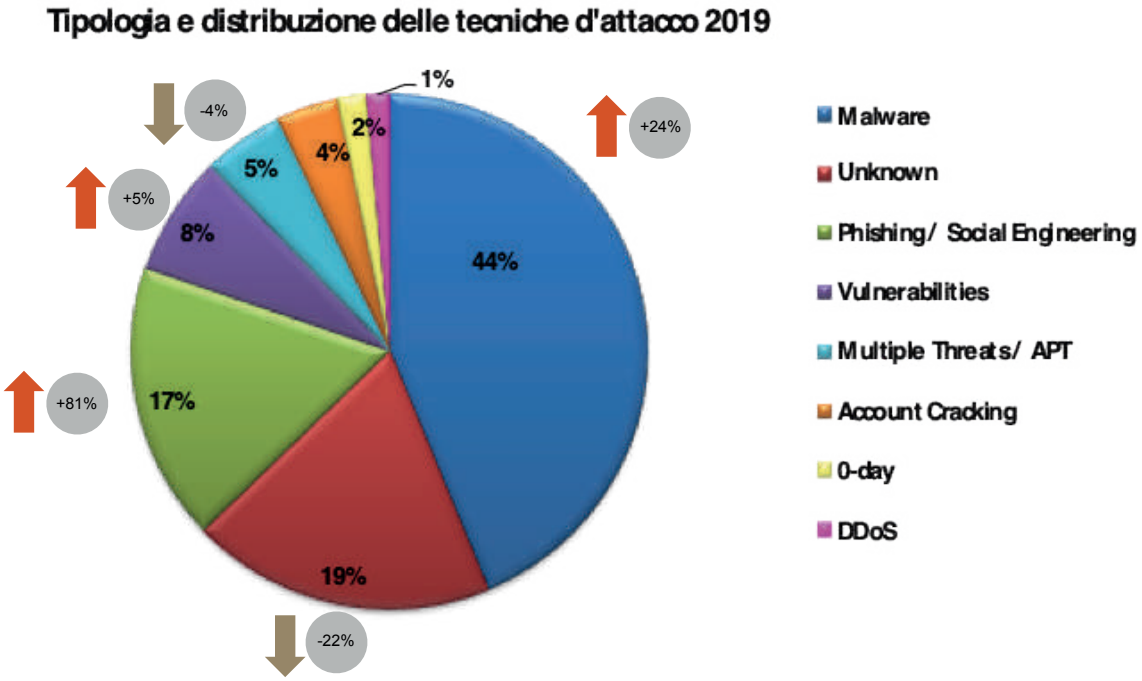
ISO 27032:2012



Una classifica da cui è impossibile essere esclusi



Malware e phishing ANCORA (!?!?) la principale minaccia!



Tecniche di attacco

+81% **Phishing**

+54% **Account Cracking**

€18,8M **Il danno delle frodi BEC denunciate in Italia**

Alcuni elementi della kill chain sono sotto il nostro controllo…

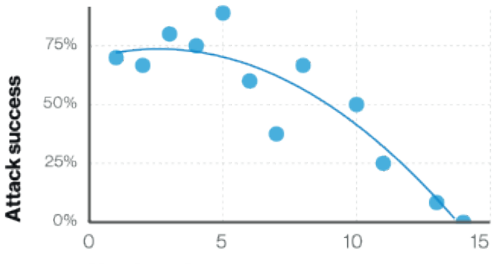


Figure 34. Attack success by chain length in simulated incidents (n=87)

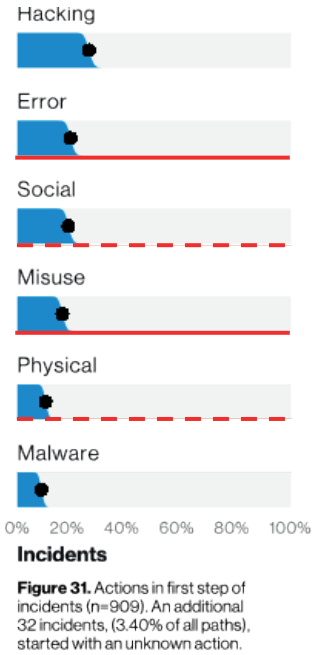


Figure 31. Actions in first step of incidents (n=909). An additional 32 incidents, (3.40% of all paths), started with an unknown action.

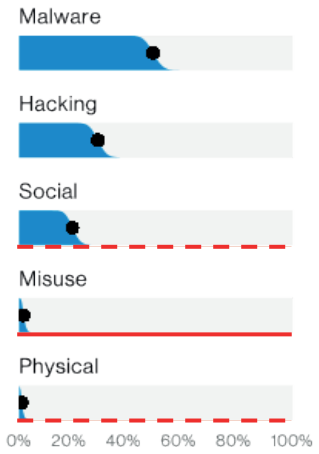


Figure 32. Actions in middle steps of incidents (n=302)

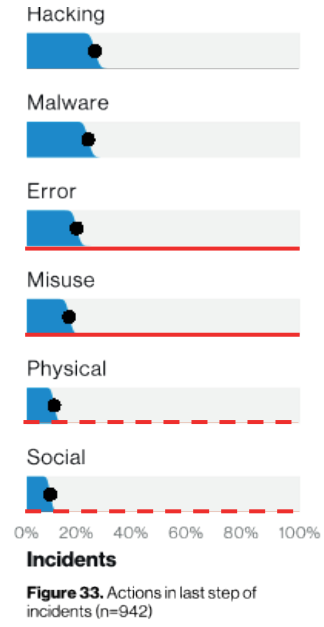
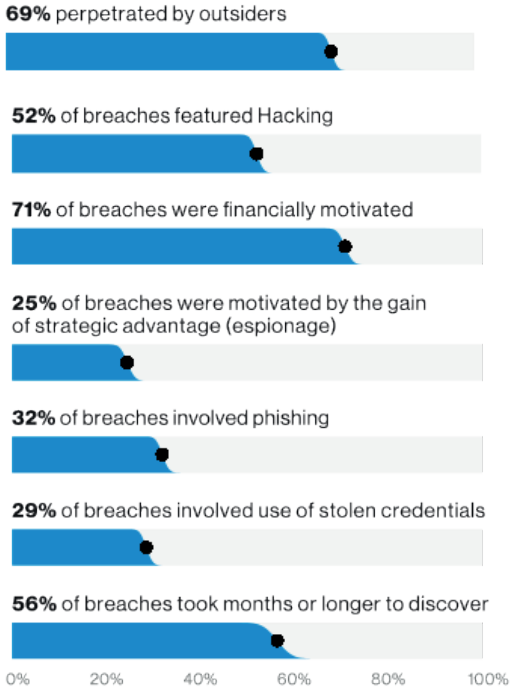


Figure 33. Actions in last step of incidents (n=942)

Verizon 2019 Data Breach Investigation Report

Punti di attenzione



Action	Asset	Count
Hacking - Use of stolen creds	Server - Mail	340
Social - Phishing	Server - Mail	270
Social - Phishing	User Dev - Desktop	251
Malware - Backdoor	User Dev - Desktop	229
Malware - C2	User Dev - Desktop	210
Hacking - Use of backdoor or C2	User Dev - Desktop	208
Malware - Spyware/Keylogger	User Dev - Desktop	103
Malware - Adminware	User Dev - Desktop	91
Misuse - Privilege abuse	Server - Database	90
Malware - Capture app data	Server - Web application	83

Table 1
Top action and asset variety combinations within breaches, (n= 2,013)

Verizon 2019 Data Breach Investigation Report

Punti di attenzione

52% degli incidenti sono dovuti a errori umani

99% «of cloud security failures, through 2025 will be the customer's fault»

0 alternative all'uso degli strumenti tecnologici per mantenere operativo il business nella prima metà del 2020

BLUEPRINT
FOR PRIVILEGED ACCESS MANAGEMENT SUCCESS
CYBERARK
All Rights Reserved.
12/01/2019
www.cyberark.com
www.cyberark.com
CYBERARK – 60 Wells Avenue Newton, MA 02459

WHY CYBERARK BLUEPRINT FOR PAM SUCCESS?

THE FOUNDATION

CYBERARK BLUEPRINT FOR PAM SUCCESS

Enterprise Best Practices

5000+ Global Customers
>50% of Fortune 500

Post Breach, Risk Reduction Expertise

>40% of largest 21st century breaches turned to CyberArk
Red Team attack experts and CyberArk Labs researchers

Leader in PAM

Creator of PAM market
#1 PAM vendor and market share leader
Decades of experience

1 Source: IDG's "Biggest breaches of the 21st Century" Published 1.28.18 + internal CyberArk analysis

WHY CYBERARK BLUEPRINT FOR PAM SUCCESS?

THE FEATURES

CYBERARK BLUEPRINT FOR PAM SUCCESS

Simple and Prescriptive

Future-Proof

Measurable, Risk-Based Advice

CYBERARK BLUEPRINT: 3 GUIDING PRINCIPLES

Risk based program designed to secure privileged access across all environments

CYBERARK BLUEPRINT STAGES OVERVIEW

GOAL	RISK REDUCTION: PREVENT CREDENTIAL THEFT	RISK REDUCTION: STOP LATERAL & VERTICAL MOVEMENT	RISK REDUCTION: LIMIT PRIVILEGE ESCALATION & ABUSE
STAGE 1 — **Rapid Risk Mitigation**: Secure privileged ids that have the potential to control an entire environment	Critical	Major	Moderate
STAGE 2 — **Core Security**: Focus on locking down the most universal technology platforms	Critical	Major	Moderate
STAGE 3 — **Enterprise Program**: Build PAS into the fabric of enterprise security strategy and application pipelines	Critical	Major	Moderate
STAGE 4 — **Mature the Program**: Mature existing controls and expand into advanced privileged access security	Critical	Major	Moderate
STAGE 5 — **Advanced Security**: Look for new opportunities to shore up privileged access across the enterprise	Critical	Major	Moderate

Learn more and sign up for your Blueprint session at https://www.cyberark.com/blueprint/

Critical Major Moderate

SECURITY SUMMIT Academy

20 anni Clusit

CYBERARK BLUEPRINT STAGES OVERVIEW

	GOAL	PAM CONTROLS & TECHNOLOGIES: Foundational Privileged Access Management	PAM CONTROLS & TECHNOLOGIES: Least Privilege	PAM CONTROLS & TECHNOLOGIES: App Secrets Management	RISK REDUCTION: PREVENT CREDENTIAL THEFT	RISK REDUCTION: STOP LATERAL & VERTICAL MOVEMENT	RISK REDUCTION: LIMIT PRIVILEGE ESCALATION & ABUSE
STAGE 1	Secure privileged ids that have the potential to control an entire environment	IaaS Admins, Domain Admins, VM & Hypervisor, Windows Server Local, MFA		3rd Party Security Tools (via C3 Integrations)	Critical	Critical	Moderate
STAGE 2	Focus on locking down the most universal technology platforms	CI/CD Consoles, Workstation Local Admin, Privileged AD Users, *NIX Root		3rd Party Business Tools (via C3 Integrations)	Critical	Critical	Moderate
STAGE 3	Build PAS into the fabric of enterprise security strategy and application pipelines	Cred boundaries, *NIX Root Similar, 3rd Party Vendors, Out of Band access, Database Built-In Admins	IT Admin Workstations	Dynamic Apps	Major	Major	Moderate
STAGE 4	Mature existing controls and expand into advanced privileged access security	Web Apps (Top), Business Apps (Top), Network & Infra Admins, Named DBA	Windows Servers, All Workstations	Static Apps	Moderate	Moderate	Moderate
STAGE 5	Look for new opportunities to shore up privileged access across the enterprise	Web Apps (All), Business Apps (All), Mainframe Admins, Windows Services	Windows Servers, *NIX Servers	Static Apps (Adv)	Moderate	Moderate	Moderate

Learn more and sign up for your Blueprint session at https://www.cyberark.com/blueprint/

Critical Major Moderate

WHAT NEXT?

GET BLUEPRINT TO WORK FOR YOU

CYBERARK BLUEPRINT FOR PAM SUCCESS

https://www.cyberark.com/it/resource/cyberark-blueprint-for-privileged-access-management-success/

https://www.cyberark.com/it/resource/privileged-access-management-program-development-service-package/

https://www.cyberark.com/it/blueprint/#demo

CYBERARK

THANK YOU!

SECURITY SUMMIT
Academy