Tu ch-IA-male se vuoi... Evoluzioni

Luca Bechelli | Comitato Direttivo, *Clusit*
Massimo Carlotti | Sales Engineering Manager -Italy, *CyberArk*

Luca Bechelli



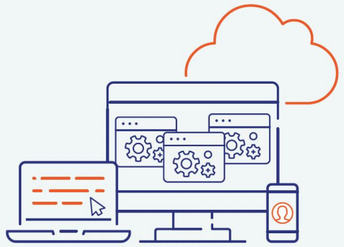
COMITATO DIRETTIVO

PARTNER @P4I – GRUPPO DIGITAL360

Massimo Carlotti
Sales Engineering Manager -Italy, *CyberArk*

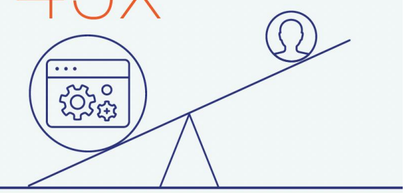


CyberArk Identity Threat Landscape Report 2022



The average staff member accesses more than 30 applications and accounts

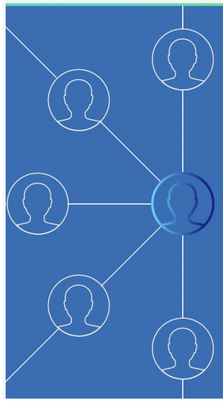
45x



Machine identities outnumber human identities by a factor of 45x



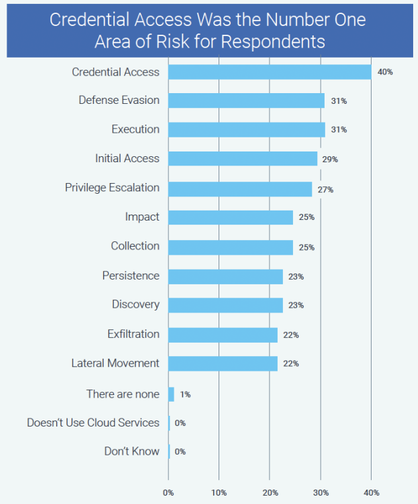
68% of non-humans or bots have access to sensitive data and assets





52% of organizations' workforces have access to sensitive corporate data

Respondents were asked about the cyber attacker tactics and techniques laid out in the MITRE ATT&CK® Matrix for Enterprise: which represented the biggest areas of risk for their organizations?



Q2. Which cyber attacker tactics and techniques (as laid out in the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques) represent the biggest areas of risk for your organization? Combination of responses ranked first, second and third.



Q24. For which of the below environments and devices does your organization have Identity Security controls in place?

CyberArk Identity Threat Landscape Report 2023

Technology adoption continues at pace. In 2023 alone, this will drive:

2.4x
growth in human & machine identities

68%
increase in SaaS tools deployed

Q: Over the next 12 months, we expect the total number of identities (i.e., both human and machine identities) under management to approximately (banded options, 2,300 respondents)

Q: Approximately how many Software as a Service providers does your organization leverage today and in the next 12 months (2,300 respondents)



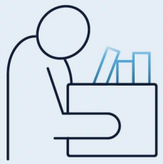
68% expect layoffs and workforce churn to create new security issues, while nearly **one-third say cybersecurity skills gaps hinder security** defences.



63% admit that highest-sensitivity access for employees is **not adequately secured**.

Q: Which of the following is true for your organisation in 2023? (2,300 respondents)

Q: To what extent do you agree or disagree with the following statements? (2,300 respondents)



74% of respondents are **concerned about confidential information loss** stemming from employees, ex-employees and third-party vendors.



No.1
Credential theft remains the number one concern for cybersecurity professionals.



77% of respondents say developers have too many privileges — making these human identities highly attractive targets.



62% of **security teams** operate with **limited visibility** across their environment.



No.1
Business-critical applications top the list of at-risk systems.



89%
indicate their organizations were **targeted by at least one ransomware attack in the last 12 months** (97% for healthcare, the most-targeted sector).



59%
say they **would not be able to protect against an attack stemming from a successful compromise of a software supply chain provider**. The energy and utilities sector — which is often critical infrastructure — is the vertical most "at-risk," with 67% saying they could not stop an attack of this type.

Clusit 25 2000-2025

SECURITY SUMMIT

ASTREA

CyberArk Identity Threat Landscape Report 2024

NEW ATTACK METHODS

99%

93%

72%

What we asked:

What negative impacts, if any, do you expect from tools in the next year?

What we learned:

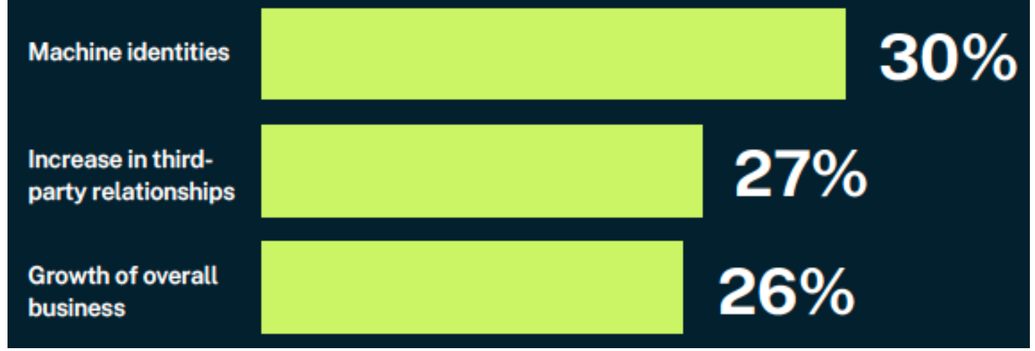
93% of organizations expect AI-related cybersec challenges, with malware and phishing topping th

What we asked:

What is driving the increase in the number of identities under management at your organization?

What we learned:

Machine identities are the #1 driver for overall identity growth.



80% of organizations experienced an identity-related breach due to a software supply chain attack.

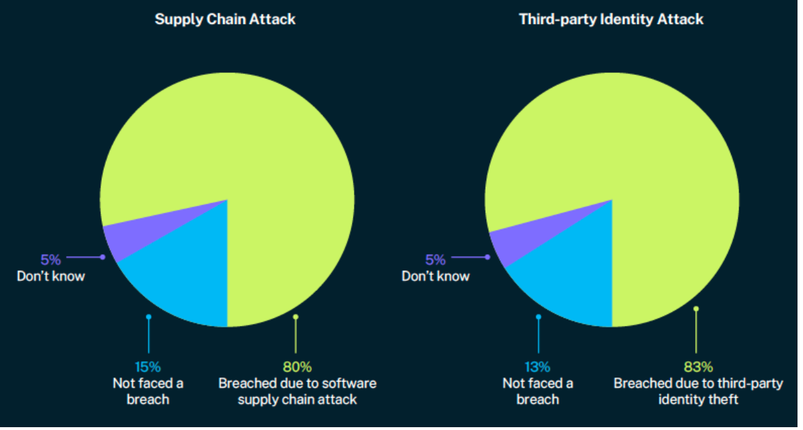
ities.

What we asked:

How often has your organization faced a successful identity-related breach due to a software supply chain attack in the last 12 months?

What we learned:

The majority of organizations have suffered from a supply chain attack and third-party identity theft.

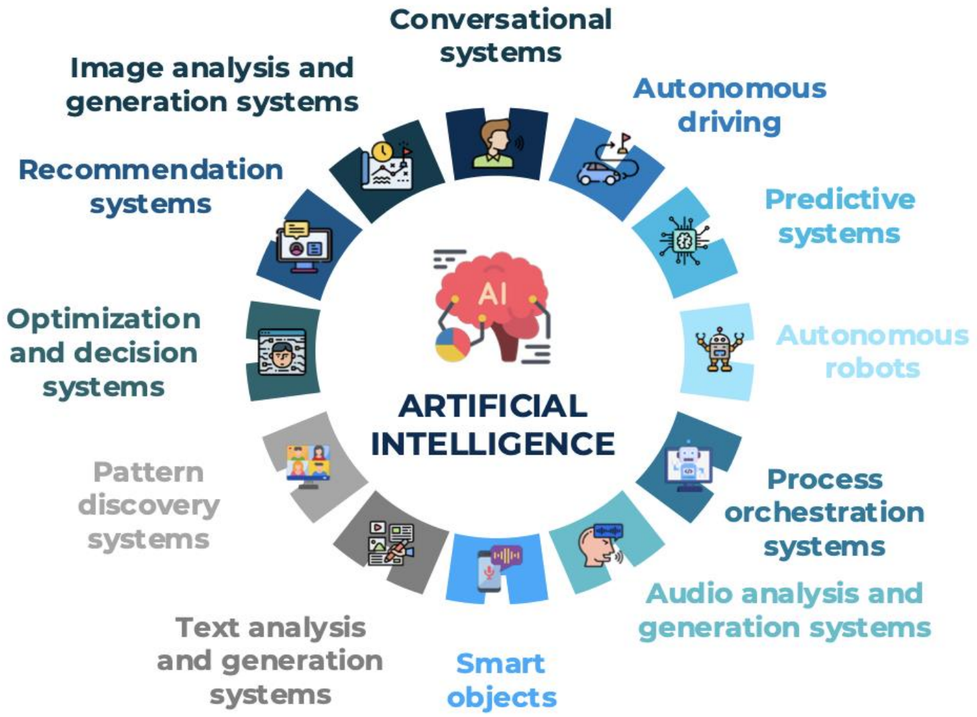


6%

5%

emain flat

Quali sono gli ambiti di maggiore applicazione delle soluzioni di AI?

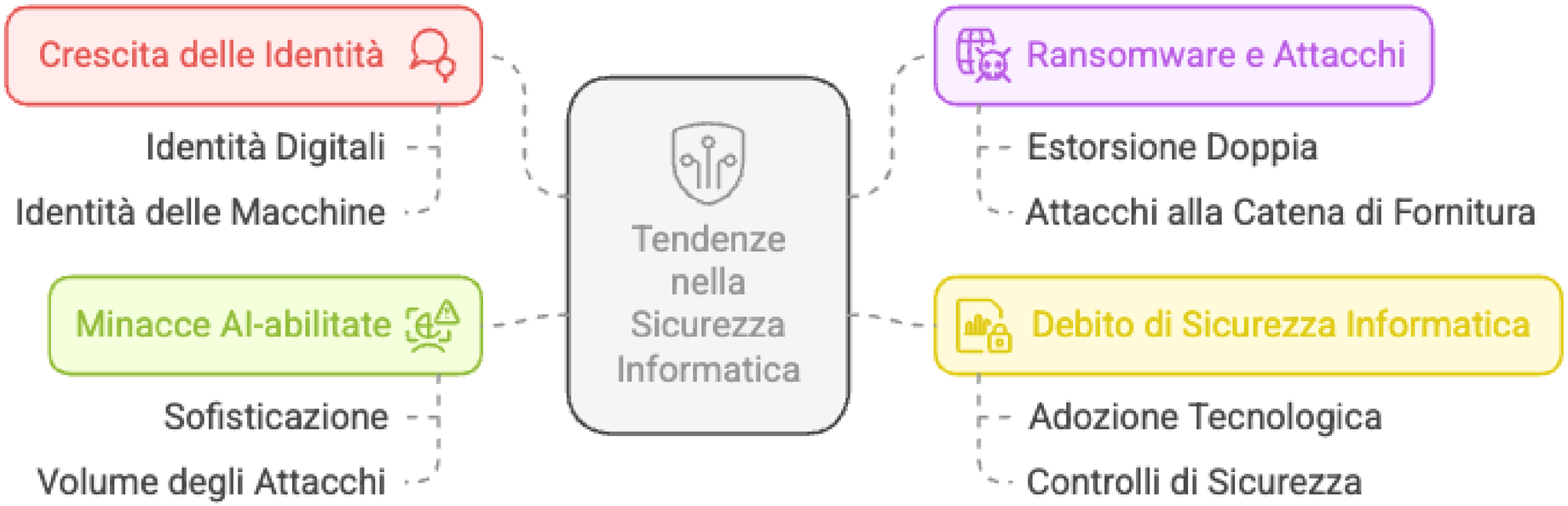


Fonte: Osservatorio Artificial Intelligence - School of Management - Politecnico di Milano

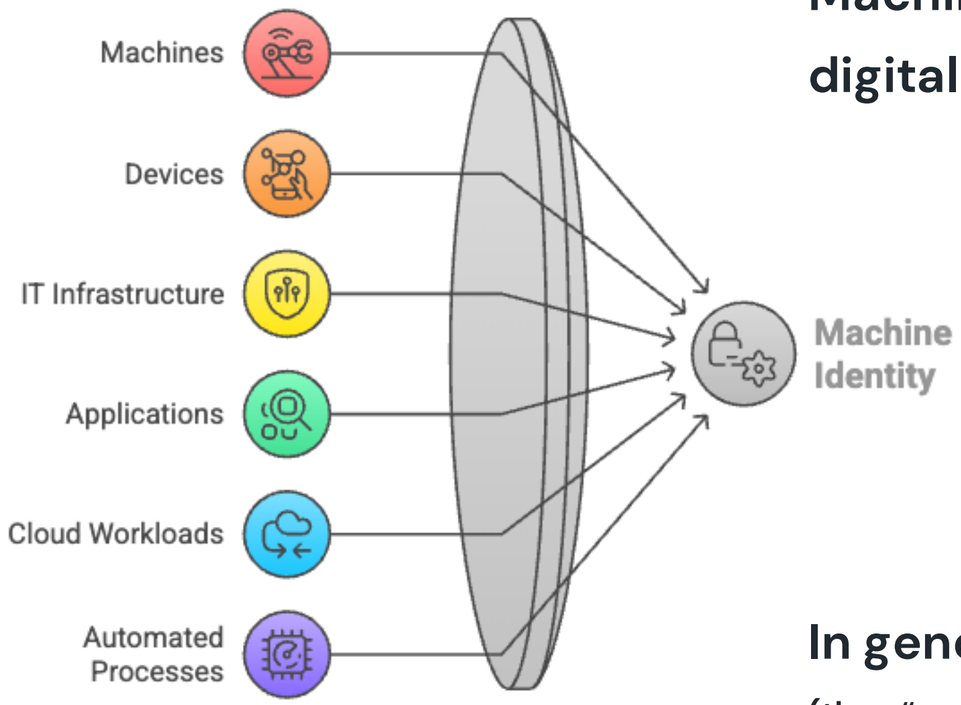
POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation



CyberArk Threat Landscape Report - TRENDS



Machine Identity – WHAT IS IT?



Machine Identity:

digital entities used to identify, authenticate and authorize

In general… Any digital entity not operated by a human

(then “non-human identities”)

Machine Identity Security – WHAT IS IT?

Estabilish, Manage and Protect:

- **Digital certificates**
- **Cryptographic keys**
- **IoT security role**
- **Lifecycle management (LCM)**
- **Compliance and standards**
- **Secrets**

Challenges: if compromised…

- **Unauthorized access**
- **Data Breaches**
- **Security incidents**

… and “human” MFA can’t be used

Solution:

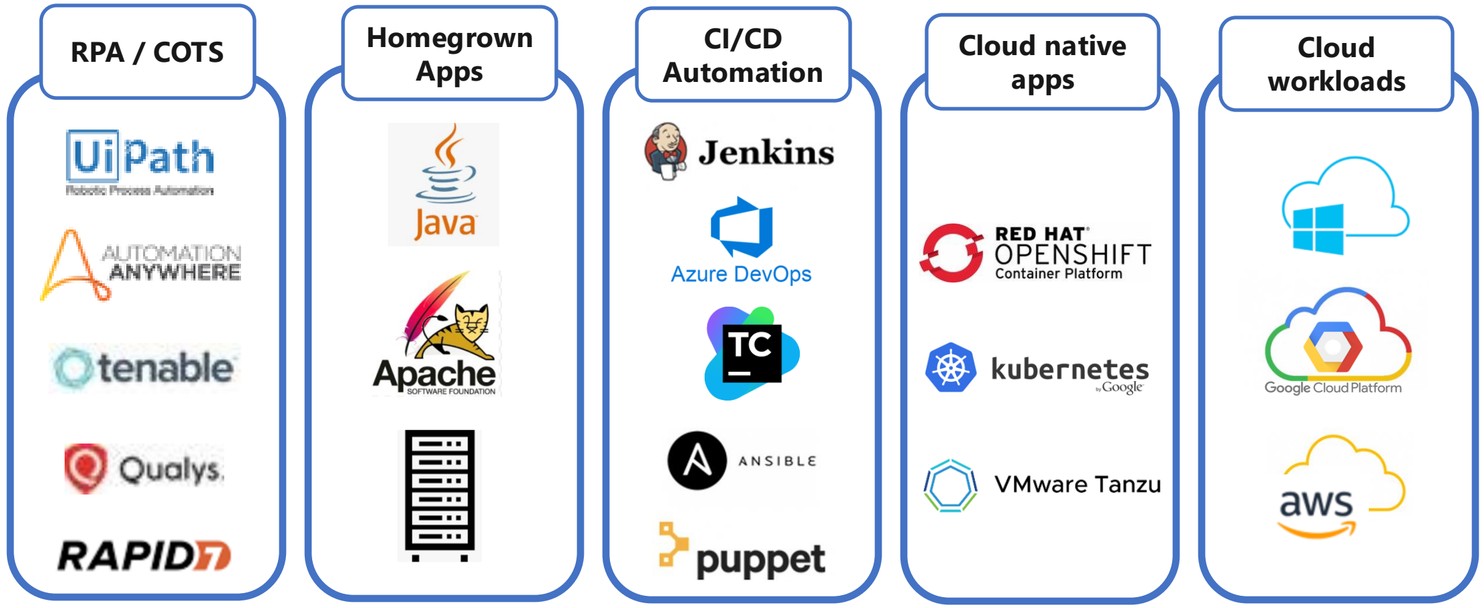
Machine ID Mgmt + Access Mgmt

Machine Identity Security – WHY?

1. **Protection of Resources and Sensitive Data**:
   - Authentication and authorization of resources.
   - Prevention of unauthorized access.
2. **Increase in Attack Surfaces**:
   - More machine identities than human identities.
   - Vulnerabilities without proper policies and automation.
3. **Zero Trust Strategy**:
   - Communication only between trusted machines.
   - Generation, renewal, and revocation of identities.



Machine Identity Security – GENERATIONS

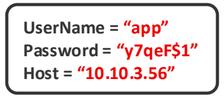


- IT environments are **heterogeneous** and **complicated**
- **Applications rely on Secrets** (passwords, SSH Keys, API Keys,…) to access IT Systems and encrypt transactions
- Each Application uses its **model and tools**
- Often **procedures** in place are **manually intensive**, then **error-prone** and may introduce **security gaps** and **blind spots**
- **Opportunity** windows for Attackers and Malicious users

Machine Identity Security – GENERATIONS



THEY EXIST **EVERYWHERE**
(ON-PREM, CLOUD, HYBRID)



SECRETS ARE **HARD-CODED**
IN CLEAR-TEXT



SECRETS VALUES ARE
STATIC AND **AGING**



SECRETS ARE STORED **LOCALLY.**
ON THE FILESYSTEM



SECRETS **LEAKED** TO **PUBLIC**
REPOSITORIES ACCIDENTALLY



LACK OF **ACCOUNTABILITY** FOR
NON-HUMAN AND HUMANS



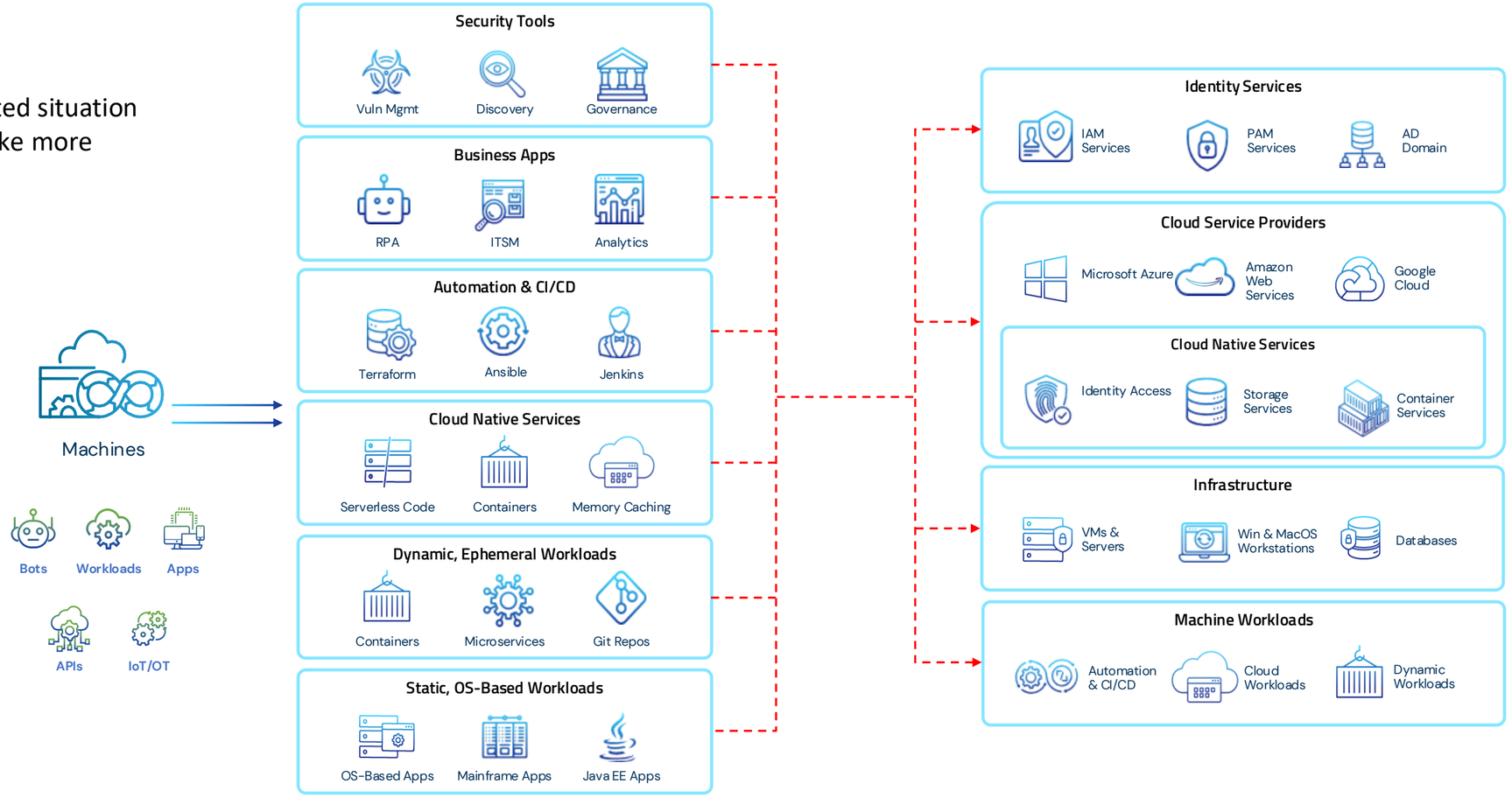
SECURITY ISLANDS CAUSED BY
VAULT & SECRET STORE SPRAWL



PURSUED BY **ATTACKERS**
(INSIDER AND EXTERNAL)

Machine Identity Security - ACCESS

"There is no such complicated situation which people could not make more complicated."
- Eraldo Banovac



Machine Identity Security / AI – WHY?

1. **Sophistication of AI-driven Attacks**:
   - Advanced phishing, AI-driven malware, automated social manipulation.
   - Generation of realistic content and analysis of large data volumes (greater attack effect)
2. **Protection Against Insider Threats**:
   - Web-based agents as emerging insider threats.
   - Prevention of malicious use of AI.
3. **Resilience and Innovation**:
   - Secure innovation and risk reduction.
   - AI-driven security solutions for rapid threat response.

Oltre il rischio «tecnologico»?

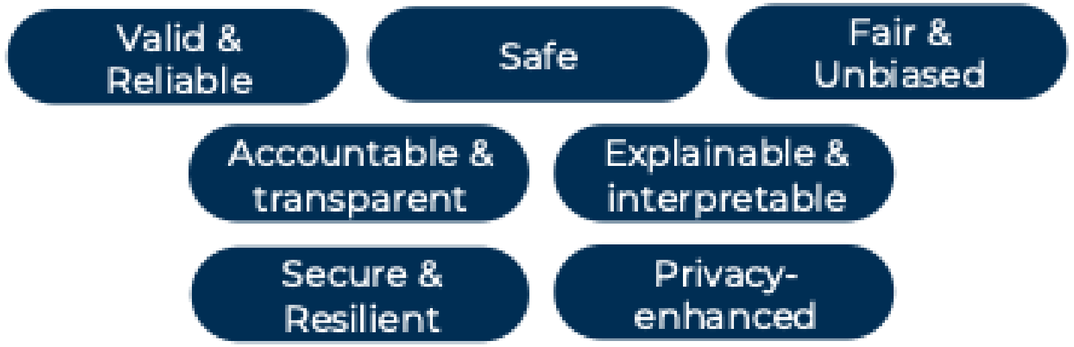
I rischi legati all'AI potrebbero andare **oltre il rischio «tecnologico»:**

- **Modelli non deterministici:**
  Le capacità autonome dell'AI possono generare decisioni o azioni non intenzionali
- **«Contenitori» di informazioni:**
  I modelli di AI sono allenati su miliardi di dati e informazioni aziendali
- **Vulnerabilità umana:**
  Modelli di AI possono interferire nelle attività e nelle scelte degli utenti che li utilizzano

AI security can be defined as the tools, strategies, and processes implemented that identify and prevent threats and attacks that could compromise the confidentiality, integrity, or availability of an AI model or AI-enabled system.

Fonte: Guidelines for secure AI system development – NCSC, CISA, Others

Trustworthy AI



Fonte: AI Risk Management Framework - NIST

Un messaggio di speranza ?





Il Framework AI Risk Management

GOVERN
Creare un sistema di responsabilità e una cultura di gestione del rischio

- Definizione di politiche di sicurezza e di incident management
- Assegnazione di responsabilità
- Policy e formazione sulla sicurezza per i data scientist e gli Sviluppatori AI

MAP
Identificare e comprendere i rischi strutturandoli in categorie

- Inventario dei sistemi AI
- Controllo sull'integrità dei dati
- Threat mapping
- Implicazioni legali e etiche

MEASURE
Valutare l'impatto e la probabilità di accadimento

- Valutazione delle vulnerabilità
- Test di Sicurezza Continuo (PT)
- Valutazione della conformità normativa
- Monitoraggio delle performance

MANAGE
Mitigare i rischi per mantenere il controllo e garantire la sicurezza

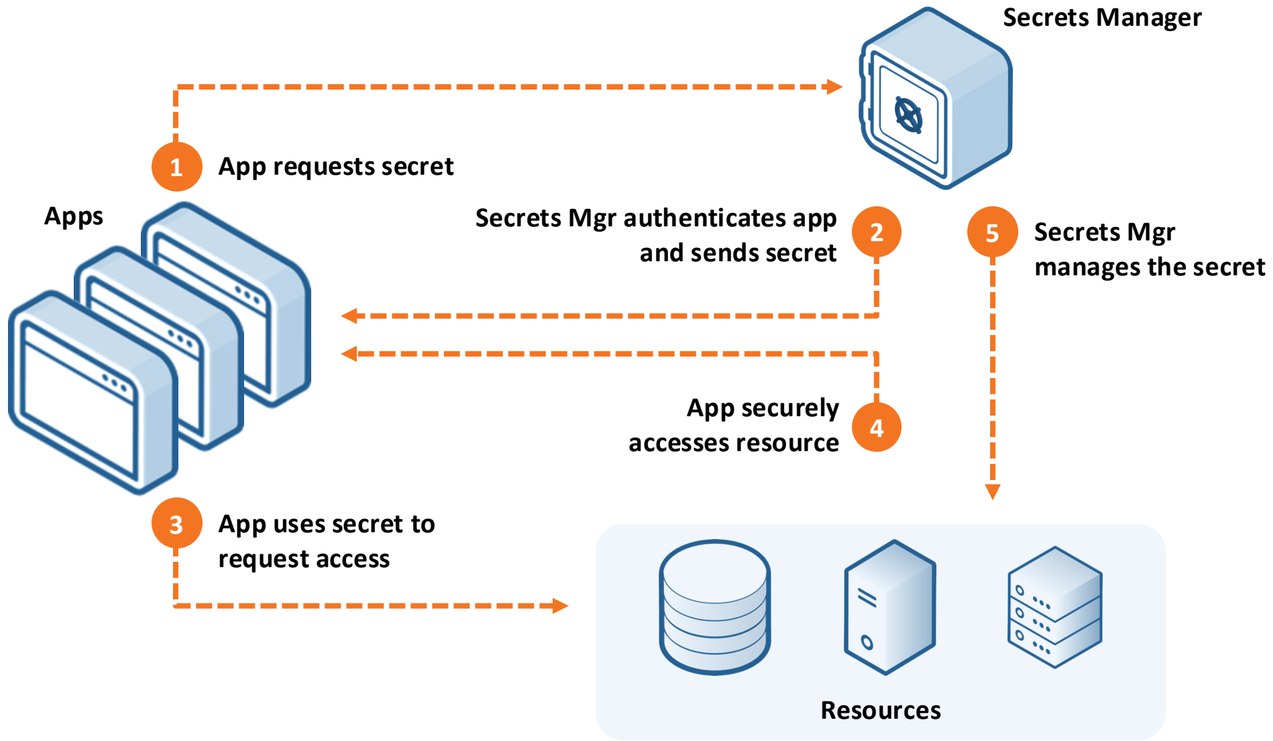
- Privacy/Security-by-design
- Colmare il «debito tecnico»
- Controllo delle soluzioni di terze parti
- Formazione

Fonte: rielaborazione osservatorio da AI Risk Management Framework – NIST

Machine Identity Security – BEST PRACTICES



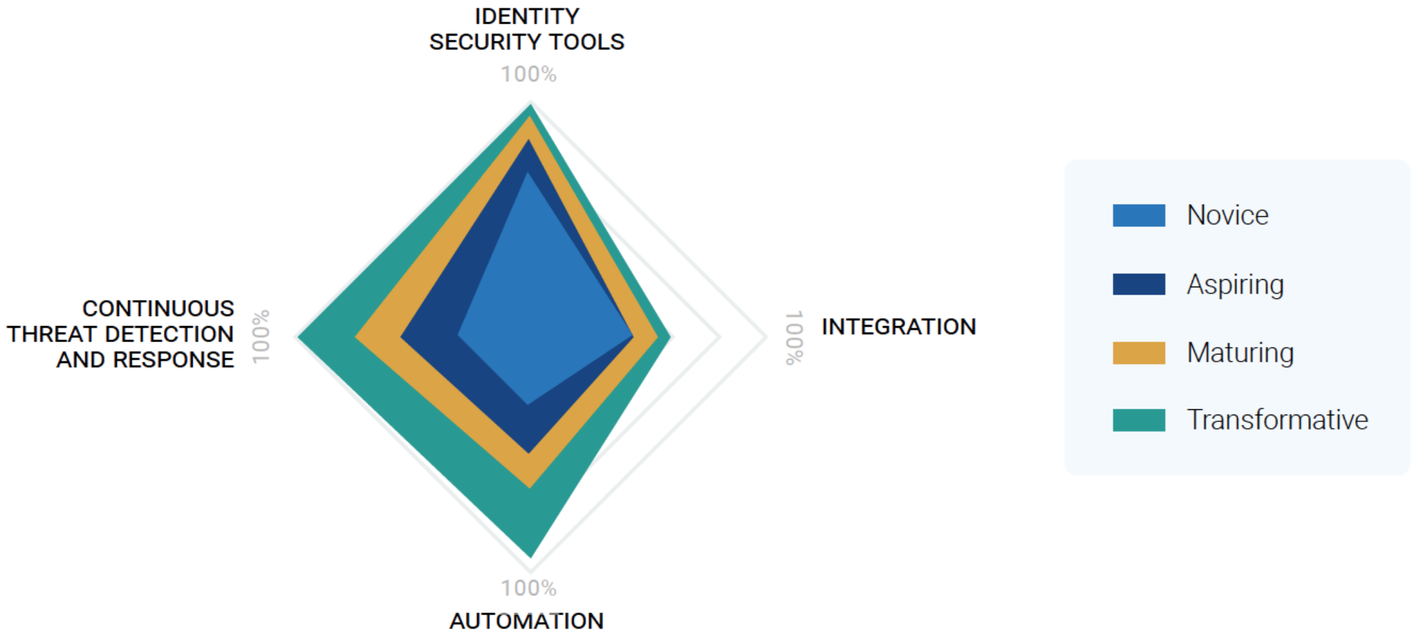
Machine Identity Security – SECRETS MGMT

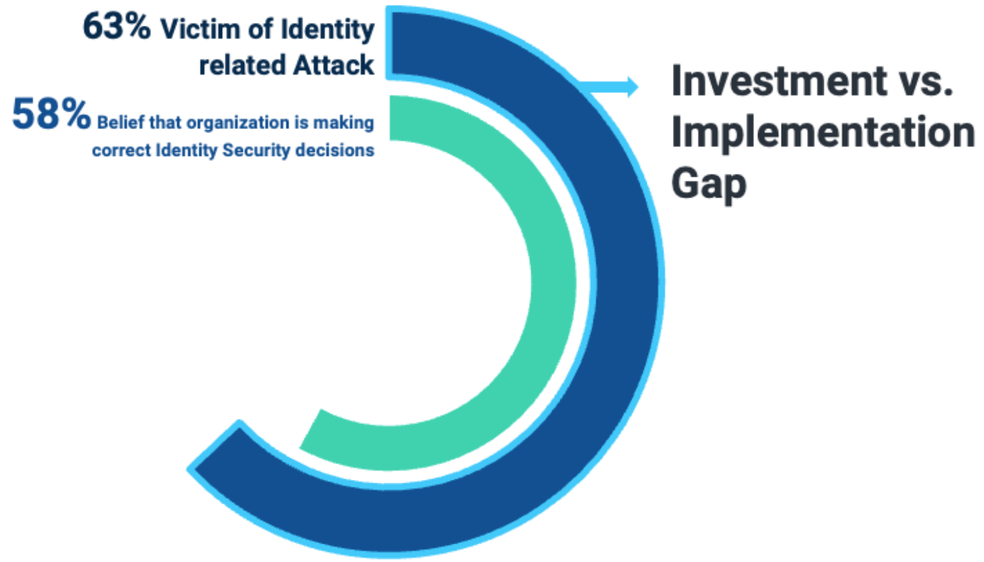


- COTS
- Containerized
- Serverless
- Microservice
- OS-Based
- Mainframe
- Scripts

Machine Identity Security – MATURITY Matters

Machine Identity Security è parte di un Maturity Model più ampio che include tutte le Identità e la Strategia IT

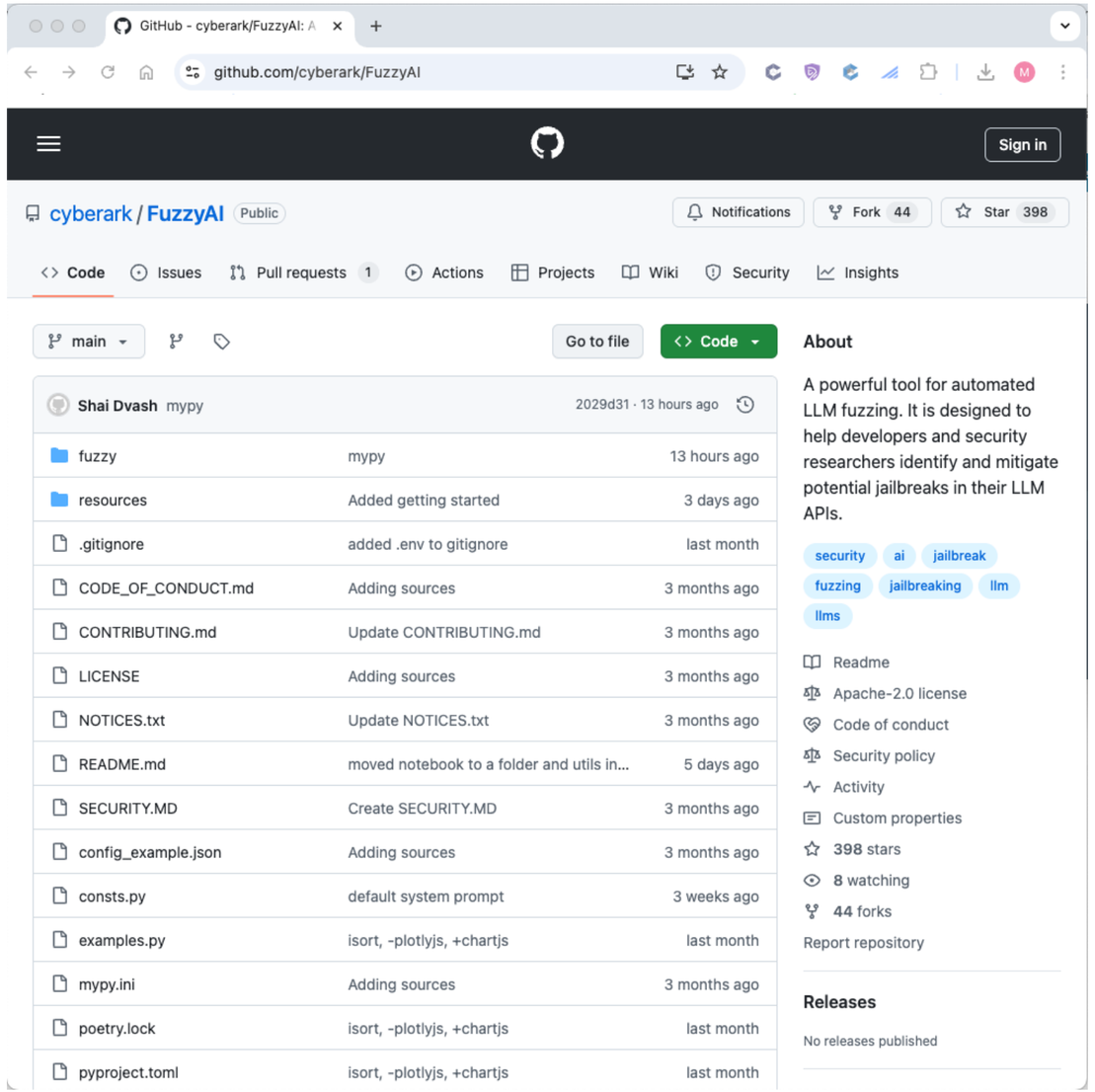




CyberArk FuzzyAI Tool

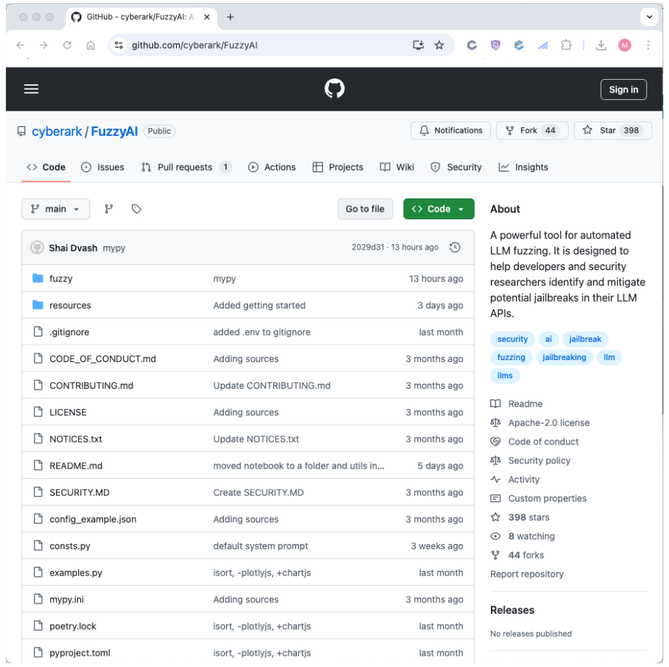
Strumento open-source avanzato progettato per aiutare sviluppatori e ricercatori di sicurezza a identificare e mitigare le vulnerabilità nei modelli di intelligenza artificiale (AI).

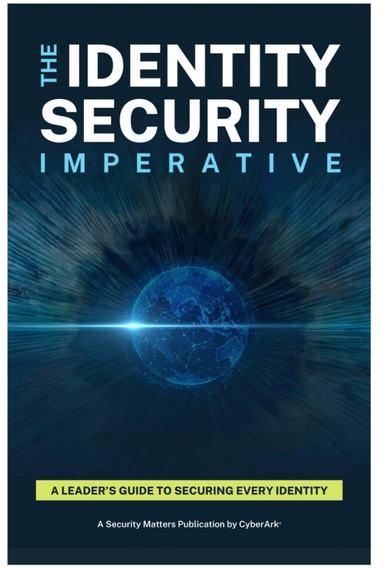
1. **Fuzzing automatizzato**
2. **Identificazione delle vulnerabilità**
3. **Framework estensibile**
4. **Collaborazione della comunità**
5. **Applicazioni pratiche**



Call to Action

- Tool CyberArk (FuzzyAI)
- Report VENAFI (Stay tuned!)
- Identity Security imperative (Book/eBook)
- IDC Report: The Business Value of CyberArk
- Identity Threat Landscape Report
  (Stay Tuned… Expected for May 2025)







Q&A

Vieni a trovarci al nostro stand!