

Identity Threats and Where to Find Them

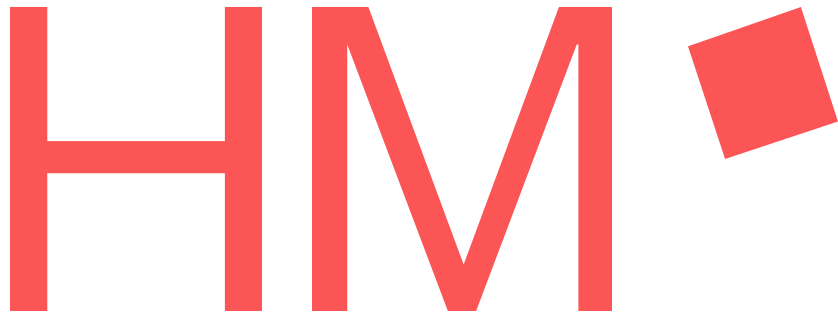
Mapping ITDR and MITRE ATT&CK

Vitali Serzantov, Erwin Kupris, Thomas Schreck

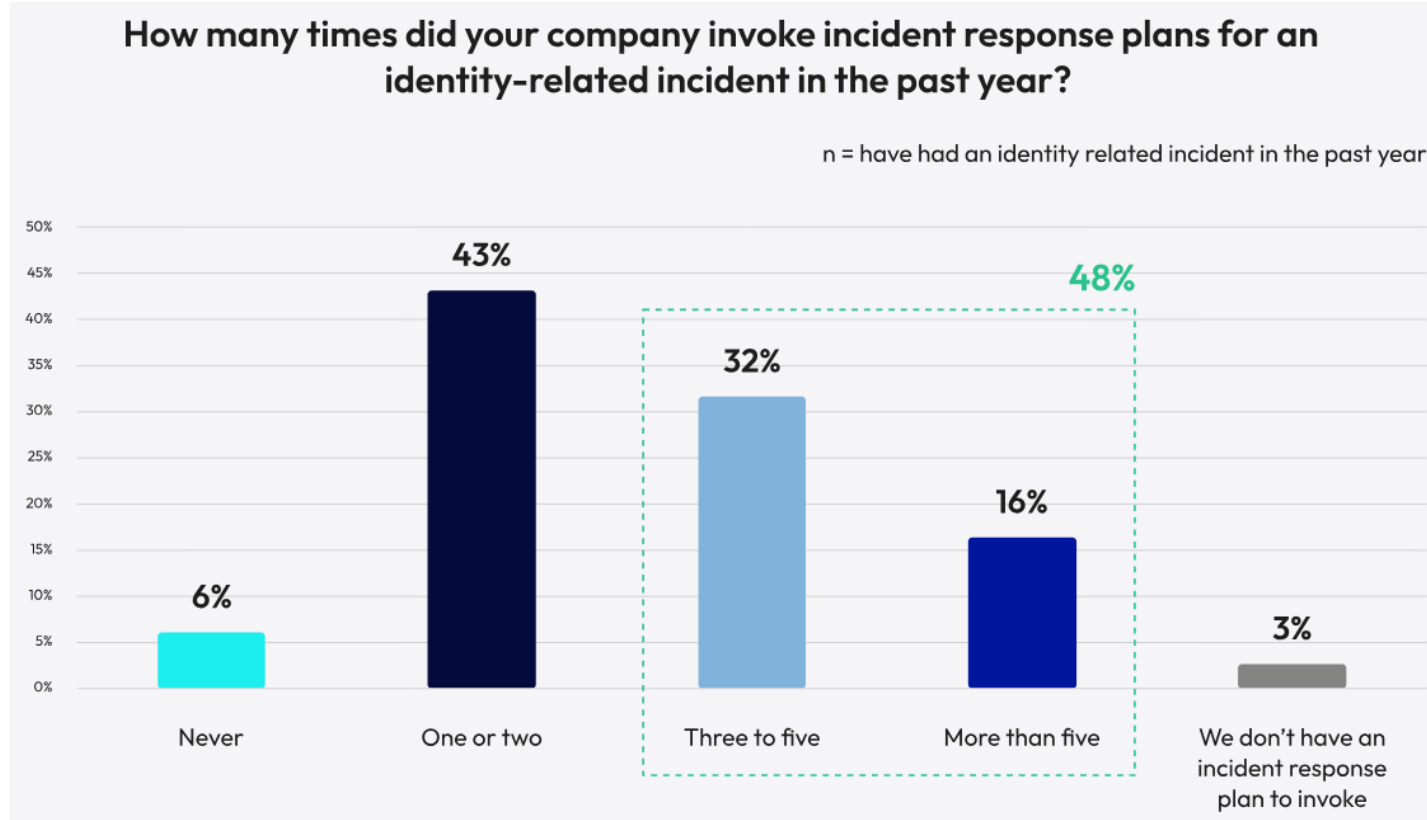
Munich University of Applied Sciences

1st International Workshop on Security and Risk in Identity Management (SeRIM 2025)

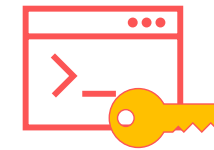
04.07.2025



Motivation



Example



Snowflake data breach

Research Questions

RQ1 - Which potential identity threats can be identified for workforce identities, and which stages of the digital identity lifecycle do they affect?

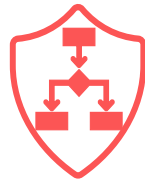
RQ2 - Which detection methods can be used to discover these potential identity threats?

RQ3 - Which preventive and reactive measures can be applied to respond to such threats?

Background

Identity Threat Detection and Response

“Combination of security tools and processes to defend identity-based systems” [2]



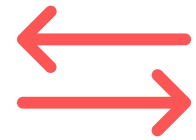
Integration with *IAM*, *PAM*, *EDR*, *XDR*, *SIEM*, *SOAR*, etc.



Monitoring of *IoCs*, *TTPs*, *Roles*, *Privileges*, *Behaviour*



Reactive capabilities
Based on preceding insights



Background

MITRE ATT&CK Enterprise Matrix

Tactics

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 16 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 45 techniques	Credential Access 17 techniques	Discovery 33 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	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
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/12)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	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)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/7)	BITS Jobs	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
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Debugger Evasion	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)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution		Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation	Defacement (0/2)	
Phishing for		Phishing (0/4)							Replication	Clipboard			

Techniques and Sub-techniques

Methodology



- **C1:** Actions that *might* aim to compromise an identity OR
- **C2:** Actions that *might* exploit a compromised digital identity as a starting point for malicious activities OR
- **C3:** Actions that *might* target identity-related infrastructure, such as IdPs, user directories, or policies OR

- MITRE ATT&CK Enterprise techniques
- Independent classification by two researchers
- Agreement rate of 96.74%

Methodology

Evaluation Schema

Identity Threat	MITRE Framework Classification			Lifecycle Stages	Affected Assets	Workforce Identity Type	ITDR Relevance		Data Sources
	Technique	Detection	Mitigation / Response				Pre-Compromise	Post-Compromise	
\mathcal{IT}_{32}	T1199	DS0015, DS0028, DS0029*	M1018**, M1030*, M1032**	Provision Account, Provision Access, Authenticate, Manage Access, Deprovision Access	Organizational Information, Identity-related infrastructure	Privileged	✓	✓	Application Log, Logon Session, IAM, PAM, EDR/XDR

* Detection and Response Methods which are addressed by capabilities of other security systems like EDR, Intrusion Prevention Systems (IPS), etc. Information may still be forwarded to ITDR systems.

** Measures that typically need to be taken before a compromise and fall under the responsibility of other systems such as IAM. The implementation may still be evaluated by ITDR.

Identification of 366 Identity Threats – RQ1

Legend

- C1: Compromises a digital identity
- C2: Exploits a compromised digital identity
- C3: Targets identity-related infrastructure
- C1 + C2
- C1 + C3
- C2 + C3
- C1 + C2 + C3

Results

Evaluation – RQ1

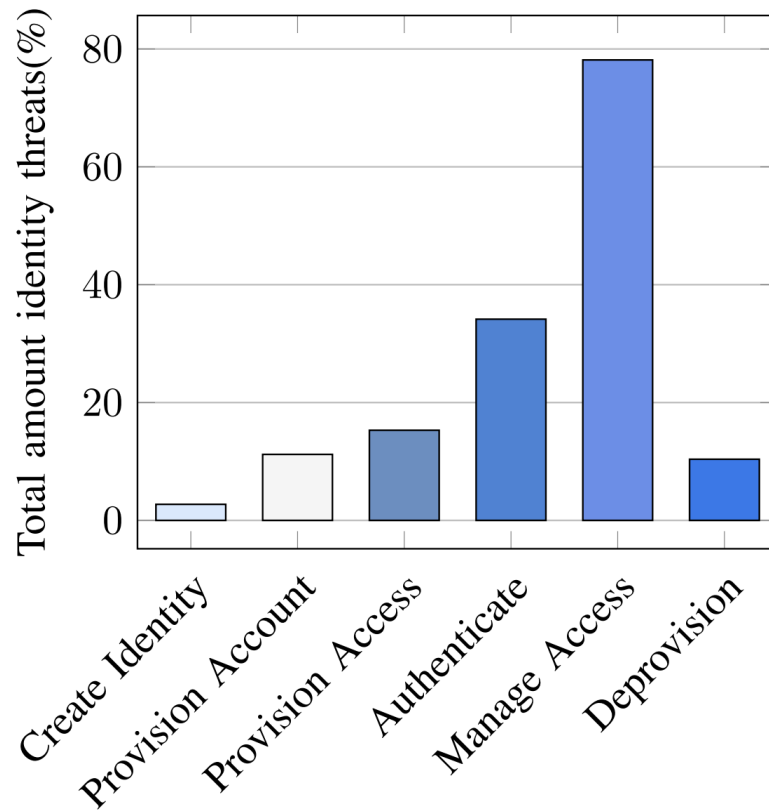


Figure 2. Affected identity lifecycle stages.

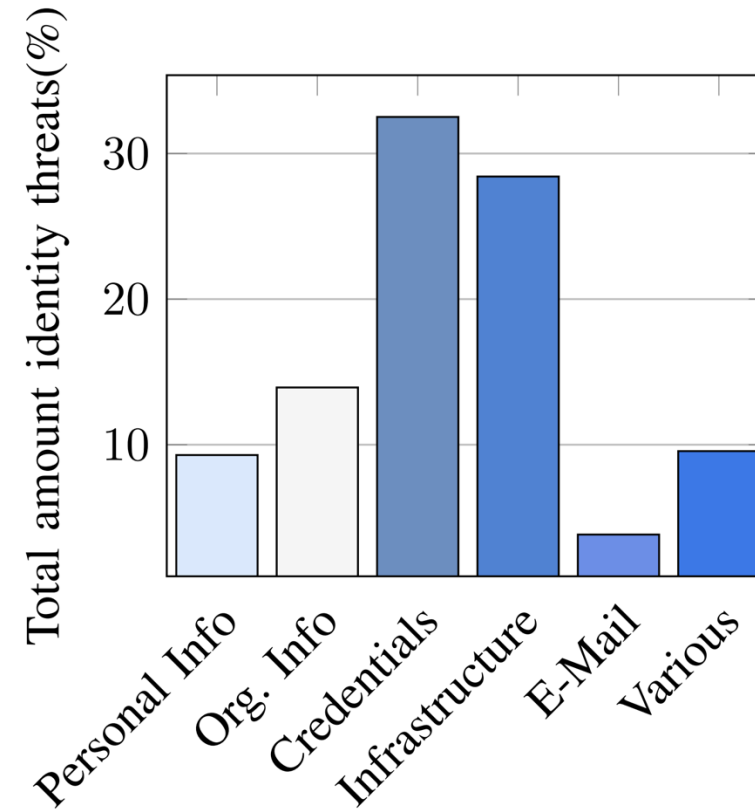


Figure 4. Affected assets.

Results

Detection and Response Methods – RQ2 and RQ3

Primary ITDR Detection Data Sources

MITRE ID	Data Source
DS0002	User Account
DS0006	Web Credential
DS0021	Persona
DS0026	Active Directory
DS0028	Logon Session
DS0036	Group






ITDR-relevant Mitigation Techniques

MITRE ID	Technique
M1018	User Account Management
M1022	Restrict File and Directory Permissions
M1026	Privileged Account Management
M1027	Password Policies
M1032	Multi-Factor Authentication
M1043	Credential Access Protection





Results

Threat-independent Detection and Response Methods

Detection

-  Proactive monitoring of dark web
-  Active detection of stale and inactive accounts
-  Active detection of unnecessary privileges and entitlements
-  User and Entity Behavior Analytics (UEBA)
-  Anomaly Detection to address insider identity threats






Response

-  Locking and disablement of accounts
-  Step-up authentication
-  Cancelling session of suspicious accounts
-  Enforcing conditional access based on risk scores





Discussion

Challenges and Limitations of ITDR

Challenges

-  Legacy Systems
-  Technology Iterations
-  Insider Threats
-  Integration with other tools and disciplines
-  No generally accepted definition

Limitations

-  (Identity-) product-specific vulnerabilities and attack surfaces
-  Social Engineering attacks
-  New identity-related technologies
-  Search of open websites and domains

Conclusion and Future Work

Identification of 366 identity threats based on the MITRE ATT&CK Enterprise Framework

First step into systemization of identity threats and foundation for further development of ITDR capabilities

Classification and Evaluation based on

- Affected lifecycle stage of digital identities
- Affected assets
- Identity types (Privileged and Non-privileged)
- Applicable detection and mitigation techniques

Need for close integration between security tools

Further research needed:

- System identities
- Consumer identities
- Communication standards, etc.

References

[1] IDENTITY DEFINED SECURITY ALLIANCE, dimensional research. 2024 Trends in Securing Digital Identities. 2024. URL: <https://www.idsalliance.org/white-paper/2024-trends-in-securing-digital-identities/>

[2] Morey J. Haber and Darran Rolls. Identity Attack Vectors: Strategically Designing and Implementing Identity Security, Second Edition. Berkeley, CA: Apress, 2024. ISBN: 9798868802324 9798868802331. DOI: 10.1007/979-8-8688-0233-1. URL: <https://link.springer.com/10.1007/979-8-8688-0233-1>

[3] MITRE Corporation, “MITRE ATT&CK Matrix for Enterprise,” 2024. [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>