PERMISO

BUYER'S GUIDE TO

IDENTITY THREAT DETECTION AND RESPONSE

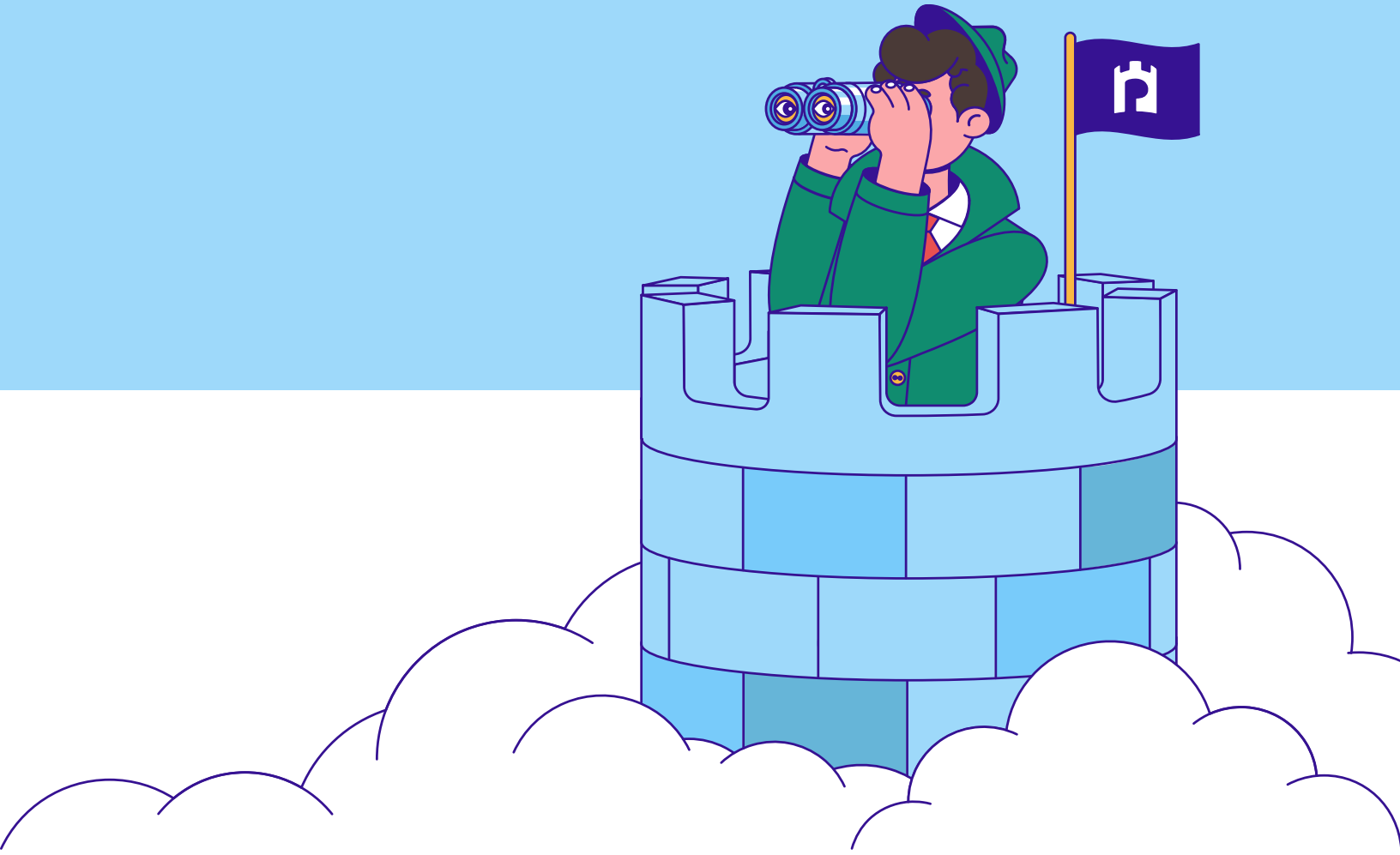


TABLE OF CONTENTS

WHO SHOULD READ THIS

This document should be read by security and risk leaders interested in understanding the relevance of Identity Threat Detection and Response (ITDR) solutions and their growing importance in keeping identities and data secure across the cloud.

“Identities” as referred to in this guide include human and non-human entities. “Access” includes direct access (local and secret users) and in-direct access (role assumption and federation) as it pertains to the following entities:

- Workforce
- Contractor
- Vendor
- Non-Human

SUMMARY

Identity attacks are becoming more frequent and widespread. In the past year, groups like LUCR-3 (Scattered Spider) and Lapsus$ have successfully compromised the identity infrastructure of major enterprises. Their success highlights the ongoing challenges organizations face in managing and monitoring the identity control plane. Centralized authentication and excessive privileges for many identities mean that a single compromised credential can have devastating consequences for any organization.

Many existing Identity Threat Detection and Response (ITDR) solutions focus on monitoring identity providers in the cloud, but this approach is too narrow and leads to a siloed outcome. These solutions lack insight into user activity in the applications and services that identity providers grant access to, such as IaaS/PaaS platforms like AWS, Azure, or GCP, SaaS applications, on-premises applications, and CI/CD systems. They also lack visibility into those environments when access doesn’t occur through the identity provider.

Organizations need a comprehensive ITDR solution because attackers often use compromised credentials to traverse the cloud's attack surface. To effectively monitor and detect threats, an ITDR solution must:

1. Track identity movements across the multi-plane cloud, including identity providers (IdPs), IaaS/PaaS, and SaaS environments.

2. Monitor both federated and non-federated access points.

3. Detect threats from initial sign-in (e.g., Okta) through transitions to other services (e.g., AWS, Salesforce, Jira, GitHub).

4. Directly monitor environments like AWS, Salesforce, Jira, and GitHub for local account usage and secret access to detect unauthorized exploration and modification.

This holistic approach ensures all potential identity threats are comprehensively monitored across the entire cloud environment.

Organizations aiming to deploy effective ITDR solution need capabilities that provide comprehensive visibility into all entity identities in their environments. This includes:

- **Unified Identity Visibility:**
    - Having visibility into all the entities (human and non-human identities, roles, groups, direct and indirect access), the permissions those entities possess, what cloud resources (IdP, IaaS, SaaS, On-Prem applications, CI/CD) they can access.
- **Multi-Plane Cloud Threat Detection, Investigation and Response:**
    - Additionally, ITDR solutions must understand entity activity within one cloud environment for e.g.: SaaS and be able to detect and track anomalous behavior in that environment as well as across the multi-plane cloud environment.
- **Single Pane of Glass for Cloud Identity Threat Detection and Response**
    - This requires having the ability to tie all entity activity conducted through shared credentials back to the performing identity, profiling access and behavior for anomalies across cloud services boundaries.

OVERVIEW

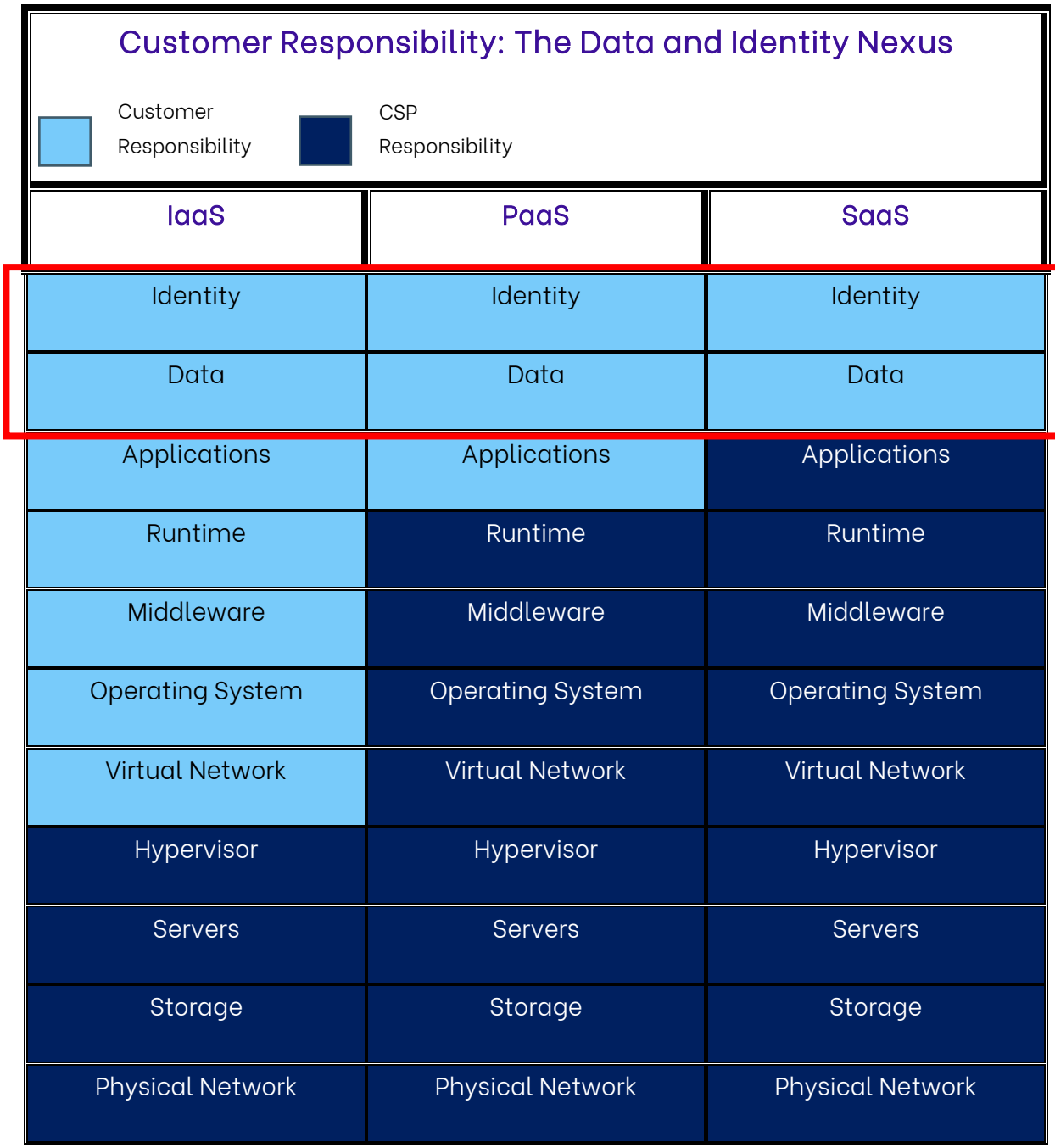
As organizations increasingly leverage the cloud, threat actors are targeting the identity layer to establish initial access into victim's environments. CrowdStrike (2024) reports that 80% of all attacks involve identity and compromised credentials. The Verizon DBIR (2024) states that 68% of breaches involve a non-malicious human element, such as human error related to misconfiguration or having credentials compromised via social engineering. IBM X-Force (2024) observed a 71% increase in attacks in 2023 using valid credentials obtained via social engineering to obtain initial access. A startling revelation in the report was that when valid credentials are compromised, the response by security teams becomes 200% more complex compared to incidents without credential compromise. IBM also notes a 266% increase in malware designed to harvest PII data, including credentials. These data points are in-line with a concerning trend associated with the increasing volume of phishing attacks that are targeting credentials as reported by the Anti-Phishing Working Group, now routinely reaching over 1 million phishing attacks per quarter, with 2023 the worst year on record.

Further evidence that identity is a prime target comes from the high frequency of recent attacks against identity providers (IdPs) like Microsoft and Okta. Compromising a privileged identity gives attackers easy access, visibility, and entitlements to carry out their mission with minimal resistance. Cloud environments are complex, and IAM best practices from cloud providers recommend using federation with an IdP and temporary credentials instead of long-term IAM users. While secure in theory, this doesn't prevent a compromised identity from exploiting federation and role assumption once authenticated. This complexity makes source-identity attribution very difficult at scale, allowing attackers to blend into normal operations undetected.

In the absence of high-profile exploits, misconfigurations, and malware, detecting a compromised identity in the environment is challenging. A new approach is needed—one that enables organizations to quickly detect deviations from normal entity behavior while providing contextual enrichment to ensure accurate detection across the multi-plane cloud environment.

THE DATA AND IDENTITY NEXUS

Securing the identities within your organization is crucial to protecting your most valuable asset: your data. The responsibility for securing identities and data across IaaS, SaaS, and PaaS environments lies solely with the customer.



IDENTITY THREAT USE CASES

To effectively safeguard against identity attacks, organizations must choose an ITDR solution with advanced capabilities to detect and mitigate attacks. These capabilities should address a range of use cases for both human and non-human identities, including but not limited to:

1. **Credential Compromise Detection:** Identify and alert on the use of stolen or compromised credentials within the environment.
2. **Privilege Escalation Detection:** Detect unauthorized attempts to escalate privileges within systems and applications.
3. **Anomalous Behavior Detection:** Monitor for deviations from normal user behavior that may indicate malicious activity.
4. **Insider Threat Detection:** Identify and respond to malicious or negligent actions by internal users.
5. **Multi-Factor Authentication (MFA) Bypass Detection:** Detect attempts to bypass or disable MFA mechanisms.
6. **Suspicious Login Activity:** Monitor and alert on unusual login patterns, such as logins from unexpected locations or devices.
7. **Identity Provider (IdP) Compromise Detection:** Identify signs of compromise within identity providers like Okta or Microsoft Entra ID.
8. **Third-Party Access Monitoring/Supply Chain Compromise:** Track and monitor access by third-party vendors or contractors to ensure it aligns with their intended use.
9. **Role and Entitlement Misuse Detection:** Detect misuse of roles and entitlements, such as access to sensitive data or critical systems.
10. **Compliance and Audit Reporting:** Provide detailed reports on identity-related activities to meet regulatory and compliance requirements.

RECENT IDENTITY BREACHES

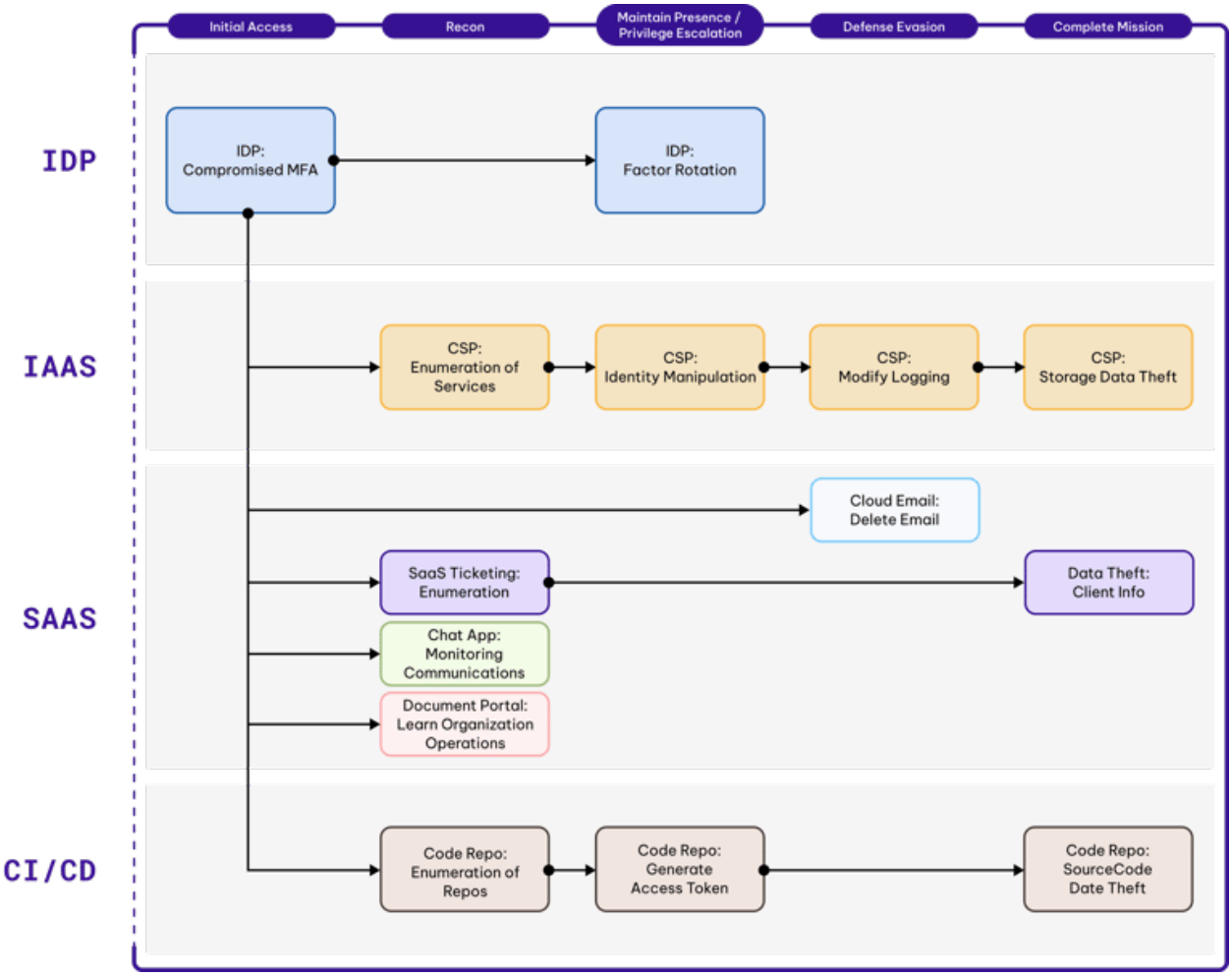
Below is a non-exhaustive list of some of the more prominent identity attacks over the past 24 months:

Target	Date	Cloud Services Layer	TTP	APT
Microsoft	Nov, 2023	IdP-> SaaS-> CI/CD	Password spraying; Access to email accounts and code repositories	APT 29/ Cozy Bear/ Midnight Blizzard
Cloudflare	Oct, 2023	IdP->IaaS->SaaS-> CI/CD	Stolen Okta access tokens; Lateral movement from IdP into SaaS (Confluence, Jira) and source code repos (Bitbucket)	APT 29/ Cozy Bear/ Midnight Blizzard
Okta	Oct, 2023	IdP->IaaS-> SaaS-> CI/CD	Adversary-in-the-middle Attack (HAR file Okta session token compromise) of a SaaS service portal. This allowed the threat actor to impersonate into customer environments (initial access, lateral movement). Customers impacted included 1Password, BeyondTrust and Cloudflare	Unknown
MGM	Sept, 2023	IdP->IaaS-> SaaS -> CI/CD	IdP compromise; Lateral movement from IdP to IaaS (AWS) and into SaaS (Slack) and source code repos	LUCR-3 / Scattered Spider

JumpCloud	June, 2023	IdP->IaaS-> SaaS -> CI/CD	IdP compromise; Lateral movement from IdP to IaaS and source code repos.	Lazarus Group /Hidden Cobra
CircleCI	Dec, 2022	IdP ->IaaS-> SaaS-> CI/CD	Malware-related credential compromise. Lateral movement, privilege escalation from IdP into code repos impacting customer environments, access tokens and keys	APT 29/ Cozy Bear/ Midnight Blizzard
Oktapus	Aug, 2022	IdP->IaaS-> SaaS -> CI/CD	Large-scale Okta-targeted phishing operation that impacted 136 organizations and netted close to 10,000 compromised customer accounts, including Cloudflare, Twilio, Cisco, DoorDash	LAPSUS$
T-Mobile	April, 2022	IdP ->IaaS-> SaaS-> CI/CD	Credential compromise; Lateral movement from IdP to SaaS (Slack) to source code repos (Bitbucket); Exfiltration	LAPSUS$
NVIDIA	Mar, 2022	IdP->IaaS-> SaaS -> CI/CD	Likely credential compromise; Privilege escalation (30k employees credential compromised); Lateral movement from IdP to source code repos	LAPSUS$

IDENTITY-BASED ATTACK SCENARIO (REAL-LIFE INCIDENT)

The following graphic below illustrates the LUCR-3, also known as Scattered Spider, attack that Permiso Security detected in a victim's environment. The attack tree graphic highlights the necessity of an ITDR solution capable of comprehensively tracking the threat actor's lateral movement across the multi-plane cloud, from the Identity Provider (IdP) through IaaS and into SaaS and beyond. The illustrated activity took place over 3 days, with 69 hours of dwell time within the IDP and SaaS layers and 3 hours of dwell time in the IaaS, PaaS, and on-premises environments.

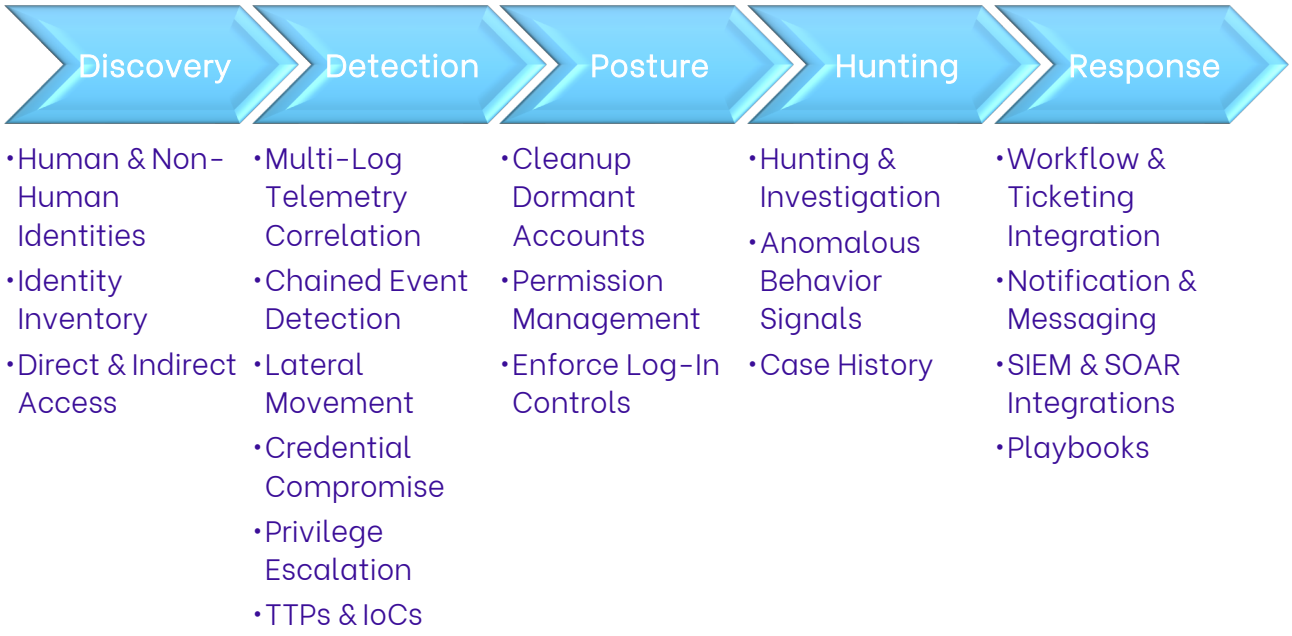


In the real-life example above, the threat actor successfully compromised the victim by targeting users with significant permissions, purchasing credentials for those users on dark web markets, and orchestrating advanced social engineering campaigns, often coupled with SIM swapping, to infiltrate the identity control plane. By compromising the identity infrastructure, they gained access to applications and services configured for federated access. To effectively defend against identity-based attacks in the cloud, organizations need a solution that comprehensively monitors all identities, both human and non-human, across multiple cloud environments.

This is where the next generation of identity-first security solutions, like Permiso Security, comes into play. With industry-leading ITDR capabilities, Permiso Security spans the multi-plane cloud, including IdP, IaaS, SaaS, on-prem applications, CI/CD, and code repositories.

PILLARS OF AN EFFECTIVE ITDR SOLUTION

Identity Threat Detection and Response (ITDR) solutions should be able to detect and respond to identity-based attacks. However, very few provide comprehensive coverage across the entire multi-plane cloud. This siloed nature of emerging ITDR solutions results in organizations receiving only a partial and incomplete snapshot of anomalous activity. Consequently, organizations often lack timely and actionable information, making it difficult to respond or determine how initial access was established and to prevent future compromises by the same or different threat actors.



The essential capabilities of an ITDR solution include:

1. Developing a universal identity profile for all users that encompasses all entity activity across cloud service layers, and where appropriate, in on-prem applications and services.
2. Pairing static analysis, posture management, and configuration of those identities with the runtime activity of those identities in the environment.
3. Monitoring and securing both human and non-human identities, tracking direct and indirect access paths, and monitoring the activity of all identities across the environment.
4. Orchestrating multi-plane detections that span identity providers, IaaS, PaaS, SaaS, and CI/CD applications to follow credentials wherever they go in the environment. This multi-plane coverage enables organizations to provide high-efficacy, correlated alerts across the entire attack surface, rather than high-volume, atomic alerts based on single events.
5. Generating high-efficacy, multi-plane alerts that represent deviations from an entity's typical behavior across the environment or activity resembling the TTPs of known threat actors.

QUESTIONS AN EFFECTIVE ITDR SOLUTION SHOULD ANSWER

1. IDENTITY INVENTORY AND ACCESS MANAGEMENT

What entity identities are present in our environment?

- Comprehensive inventory of human and non-human identities across all systems and applications.

What roles and permissions do these identities have?

- Details on roles, groups, and specific permissions each identity has across different cloud and on-premises environments.

What role/group gave a particular user access to a resource? What is the permission scope for that access?

- Specifics on roles/groups and permissions that grant access to resources.

2. RISK ASSESSMENT AND ANOMALY DETECTION

What are the top 10 riskiest identities across my cloud services layer? What would the blast radius be should one of those identities be compromised?

- Identification of the most at-risk identities and assessment of the potential impact of their compromise.

Are there any anomalies in identity behavior?

- Detection of deviations from normal behavior patterns for each identity, highlighting potential malicious activity.

Have any credentials been compromised?

- Alerts on the use of stolen or compromised credentials within the environment.

3. AUTHENTICATION AND ACCESS PATTERNS

How are identities being authenticated and accessed?

- Tracking authentication methods and access paths for all identities, including federated and non-federated access points.

What are the sources and locations of login attempts?

- Detailed logs of login attempts, including IP addresses, geographic locations, and device information.

How is my current environment being accessed by different types of entities (human and non-human)?

- Monitoring access patterns for different types of entities in the environment.

How broadly is MFA being enforced across the applications and cloud services layers in my environment?

- Assessment of the implementation and enforcement of Multi-Factor Authentication (MFA) across the environment.

4. ACTIVITY MONITORING AND CHANGE TRACKING

What changes were just made in my environment, who is responsible for those changes, and were similar changes made in other cloud services layers?

- Tracking and reporting recent changes, responsible users, and cross-layer consistency.

Which identities have accessed sensitive data or critical systems?

- Monitoring and reporting on identity access to sensitive data repositories, critical systems, and high-risk applications.

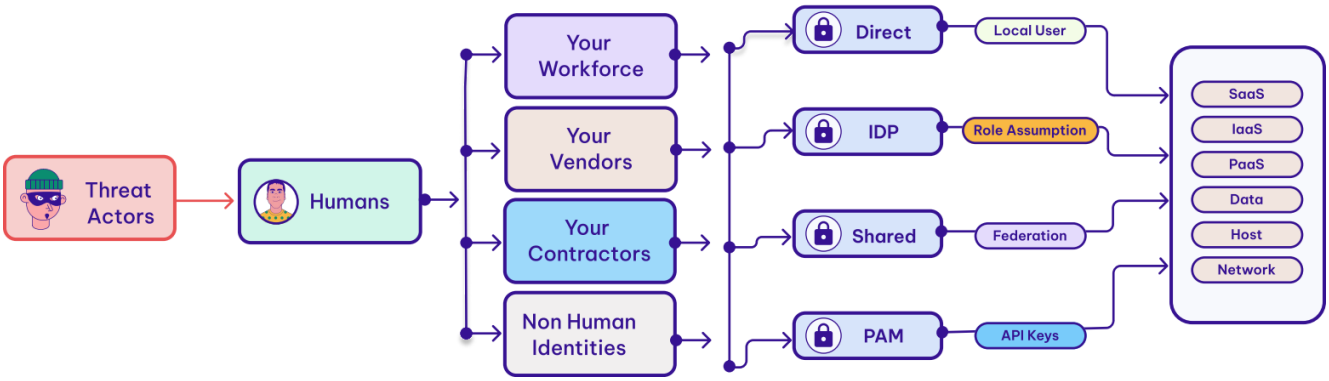
5. INCIDENT CORRELATION AND RESPONSE

How do identity-related incidents correlate across different environments?

- Correlation of identity activities and incidents across IdP, IaaS, PaaS, SaaS, CI/CD, and on-prem environments to provide a unified view.

What actions should be taken to mitigate identified threats?

- Actionable recommendations and automated response options to mitigate detected identity threats and prevent future incidents.



ITDR BUSINESS USE CASES

At a fundamental level, an Identity Threat Detection and Response (ITDR) solution enable organizations to manage and secure identities, detect and respond to anomalies, and maintain comprehensive visibility and control over identity activities across their entire IT environment.

MANAGE AND SECURE IDENTITIES

- Provides visibility across all parts of the identity lifecycle.
- Vulnerability Management
    - Quickly identify and remediate both hygiene and privilege escalation-related vulnerabilities within your environment.

DETECT AND RESPOND TO ANOMALIES

- Ability to compare baseline, good and bad access activity.
- Identify Malicious Insiders
    - Monitor the ongoing activity of overprivileged and high-risk identities.
- TTP comparison: Quickly identify compromised credentials across IdP, IaaS, PaaS, SaaS & on-premises applications, CI/CD and code repository environments.
- Reduce the Risk of Data Theft
    - Detect suspicious activity in your account related to sensitive database and snapshot access, email export and rule modification, and private storage bucket replication activities.
- Protect Against Resource Hijacking Attacks
    - Monitor real-time access anomalies, publicly exposed API credentials, detect compute credential hijacking attacks and usage of long-lived or dormant keys and tokens.
- Support Incident Response Operations
    - Utilize insights to assist in incident analysis and breach response operations across the IdP, IaaS, PaaS and SaaS layers.
- Supplement 3rd Party Security Tooling

- Enhance and validate external security alerts through the automated application of identity-centric session data and advanced threat hunting capabilities.

INCREASE OBSERVABILITY, UNDERSTANDING & CONTROL

- Source Identity Attribution and Access Chain Reconstruction
    - Gain a clear understanding of which identities (human, machine, vendor) are accessing your IdP, IaaS, PaaS, SaaS & on premises applications, and CI-CD and code repository environments both directly and throughout the federation and role-assumption process. Discover how access is occurring, and which entitlements are actively being used.
- Runtime Violation Visibility
    - Detect use of root, console access without MFA, and federated vs. non-federated access.
- Monitor Change Attribution
    - Provide the ability to track and attribute all sources of DevOps changes from GitHub, Terraform, and associated cloud environments back to an owner.
- Support Identity Governance Initiatives
    - User Offboarding – facilitate user offboarding through an identity dossier that consolidates all associated activity and identities attributed back to the top-level (IDP) source identity.
    - Access and Change Management – monitor, manage and support identity governance maturity with quantitative data around how the environment is being managed.
- Application Least Privilege Access (LPA)
    - Gain an understanding of used and unused application entitlements across your IdP users.
- Resource Optimization
    - Identify unused and orphaned resources across your environment.

RFP TEMPLATE

General Capabilities	
Requirement	Vendor Response
General Setup	
Agentless Collection and Data Ingest via API	
IdP, IaaS, SaaS, On-Premises, and CI/CD & IP tool support	
Data Correlation and Normalization	
IdP Coverage	
ITDR for Multiple Identity Providers (Okta, Entra ID, Google Cloud Identity)	
IaaS Coverage	
Coverage for AWS, AZURE, & GCP	
SaaS Coverage	
Productivity (Google Workspace, M365)	
Collaboration Platforms	
IP/ Development	
HR	
Finance/Payments	
ITSM	
Project Management	
Technical /Design	
Sales/ Marketing	
Critical Data: Code Repos & IP Development Coverage	
Code Repos (GitHub)	
IP Development (Miro, Jira)	

General Capabilities	
Requirement	Vendor Response
Identity Inventory	
Identify and Report Organizational Identities, Secrets, Roles from Across IdP, IaaS and SaaS	
Identify Related Identities and Visualize a Unified identify for Workforce	
Monitor and Report on Each Identity's Activity Including Life Cycle Actions Performed on Resources	
Monitor and Report on Identify Lifecycle, Creation and Modifications Made to Each Identity or Credential	
Visualize Entitlements to Organization Apps and Cloud Assets via Identity Graph	
Identify all Organizational Entity Identities, Human, Machine and Vendor/Service	
Identity Posture Management	
Identify Orphan User Accounts	
Identity Ghost User Accounts and Permissions	
Identify Shared Accounts	
Identify Accounts with Unused Permissions	
Identify Accounts with Excessive Permissions	
Identify Users Accounts Not Enrolled in MFA	
Identify Users with Weak Password and MFA Configuration	
Identify when MFA is Bypassed, or Suspicious Activity is Observed with Respect to MFA Configuration	
Identify and Visualize Attack Pathways Across Cloud Environments Including IdP, IaaS and SaaS	
Provide Blast Radius Visualization to Demonstrate Potential Compromise	

General Capabilities	
Requirement	Vendor Response
Identity Detection & Response (Runtime Malicious Activity)	
Rule and Policy Creation	
Automated Monitoring	
Failed Logins After No Activity	
Credential Attacks	
Impossible Travel Alerting	
Account Takeover	
User Behavior Analytics / Identity activity baselining	
Privilege Abuse and Escalation	
Session Hijacking / Parallel Session Use	
Comparison of Runtime Behavior to Attack Frameworks / IoCs	
Comparison of Runtime Behavior to Self	
Alert Visualization	
Event Risk Scoring	
Ability to Support Better Identity Attribution of the Attack	
Ability to Prove Malicious Intent	
Digital Playbooks	
Detections Mapping to MITRE ATT&CK	
Support Human-led Investigation	
MTTR in Minutes	
Integrations to SIEM & SOAR	
Email Notifications	
Slack Notifications	
Workflow and Ticket Management Integration	
Webhooks and APIs	
Guided Remediation	

Cloud Detection Capabilities		
Requirement	MITRE ATT&CK	Vendor Response
Identity Provider		
Modify Authentication Process (IDP, MFA, Password changes)	Credential Access; Impact; Persistence; Defense Evasion	
MFA Exempt Credential Creation and/or Usage	Initial Access, Persistence	
Push Fatigue	Credential Access	
MFA Bypass	Persistence; Privilege Escalation	
Anomalous Logon	Initial Access	
Anomalous Application Access	Initial Access	
Credential Stuffing	Persistence	
Identity Created or Modified to Be Over-Privileged	Privilege Escalation	
Identity Impersonation	Privilege Escalation	
Change Detected on Email Domain (Updated, Created, Deleted)	Privilege Escalation; Persistence; Defense Evasion; Initial Access; Impact	
IDP Detected a High-Risk Session (API Token Creation Event Occurred)	Persistence; Credential Access	
Permissive IDP Policy or Group Created	Credential Access, Defense Evasion, Persistence	
IDP Token Generation	Persistence; Privilege Escalation	
IDP Security Features Disabled	Defense Evasion	

Cloud Detection Capabilities		
Requirement	MITRE ATT&CK	Vendor Response
IaaS		
Modify Authentication Process (IDP, MFA, Password Changes)	Credential Access; Impact; Persistence; Defense Evasion	
Secrets Harvesting	Privilege Escalation; Persistence; Lateral Movement; Credential Access	
Machine Identity Hijacking	Initial Access, Persistence, Privilege Escalation	
Resource Hijacking	Persistence; Impact	
Compromised AWS Access Key is Re-Activated	Persistence	
Service Enumeration	Discovery	
Console Access Without MFA	Initial Access, Persistence	
Service Hijacking (i.e.: SES)	Resource Development	
AWS Access Key Compromised	Persistence	
External Access Enabled	Privilege Escalation; Defense Evasion; Initial Access; Persistence	
Security Features Downgraded or Disabled	Privilege Escalation; Defense Evasion; Initial Access; Persistence	
Overly permissive Identity, Credential, Policy Created	Privilege Escalation; Defense Evasion;	

Cloud Detection Capabilities		
Requirement	MITRE ATT&CK	Vendor Response
	Initial Access; Persistence	
Account or Subscription Hijacked	Persistence; Impact	
SaaS		
Modify Authentication Process (IDP, MFA, Password Changes)	Credential Access; Impact; Persistence; Defense Evasion	
Email Compromise	Persistence; Exfiltration	
Data Exfiltration	Exfiltration	
Permissions Changed	Privilege Escalation	
Mailbox Permission Changes	Persistence; Evasion; Exfiltration	
Sensitive Search Queries	Impact; Persistence; Defense Evasion	
Malicious Inbox Rule Creation	Defense Evasion	
Data Exfiltration	Exfiltration	
CI/CD and IP Development		
Code Repository		
Modify Authentication Process (IDP, MFA, Password Changes)	Credential Access; Impact; Persistence; Defense Evasion	
Organization SAML Settings Updated	Credential Access; Impact; Persistence; Defense Evasion	
Outside Collaborator Added	Exfiltration; Collection; Reconnaissance; Discovery	

Cloud Detection Capabilities		
Requirement	MITRE ATT&CK	Vendor Response
Triage or Write Permissions Granted	Resource Development; Execution; Persistence; Impact	
IP Allow List Created	Defense Evasion; Impact	
Repository Exfiltration	Collection; Impact	
Repository Visibility Updated to Public	Collection	
Repository External Integration Add/Update/Delete	Resource Development; Execution; Persistence; Impact	
Mass Repository Access (Download/Export)	Exfiltration	
Deployment Automation		
Create or Modify System Process	Defense Evasion, Persistence, Impact	
Workflow Action Correlation to Trigger (Code/PR/Deploy) i.e.: Commit -> PR -> Deploy -> Cloud Resource Change	Command & Control; Resource Development; Execution; Persistence; Impact	
IP tools		
Modify Authentication Process (IDP, MFA, Password Changes)	Credential Access; Impact; Persistence; Defense Evasion	
Data Exfiltration	Exfiltration	

REFERENCES

Anti Phishing Working Group 2024

CrowdStrike 2024 Global Threat Report

CyberHut 2024 Identity Threat Detection & Response: Questions for Vendors

KuppingerCole 2024 Leadership Compass: Identity Threat Detection and Response (ITDR): IAM Meets the SOC

IBM X-Force Threat Intelligence Index 2024

Verizon 2024 Data Breach Investigations Report

PERMISO

THANK YOU

QUESTIONS? CONTACT US AT HELLO@PERMISO.IO