January 2024

Safeguarding Digital Identities in the Modern Era through Identity Threat Detection and Response (ITDR)

www.pwc.nl

Table of Contents

Executive Summary

The digital landscape has evolved significantly, and digital identities have become a prime target for malicious threat actors, leading to a surge in identity-related breaches. The breaches are often a result of password attacks, multi-factor authentication (MFA) bypass techniques, and even Identity infrastructure attacks; all of which highlight the importance and need for a preventive approach: Identity Threat Detection and Response (ITDR).

ITDR is a cybersecurity discipline that focuses on protecting user identities and identity-based systems. It involves a combination of security tools, human processes, and best practices to effectively detect and respond to identity-related threats.

The effectiveness of ITDR relies on four primary pillars:

1. **Identity Baseline** – establishing a solid foundation based on the identity-first security capabilities, inclusive of identities, accounts, authentication, and authorization of various entities;
2. **Risk Identification –** recognizing and comprehending risks associated with the relevant threats and vulnerabilities within your specific digital ecosystem;
3. **Detection & Alert Management** – identifying malicious and fraudulent access to identity data, and determine if identities have been compromised; and
4. **Response Mechanisms** – automated playbooks to triage and in manual human response to ensure an effective outcome is achieved inline with the organization's strategy.

These pillars are crucial for strengthening identities and protecting sensitive organizational data. As the threat landscape evolves, ITDR continues to adapt, underpinned by its core pillars, making it a long-lasting success factor in cybersecurity.

Introduction

The digital landscape has undergone a rapid transformation in recent years, becoming vastly interconnected, but extending beyond just technology to now include digital identities. Sitting at the core of this interconnectedness is Identity and Access Management (IAM). IAM is positioned at the heart of cybersecurity and digital transformation, and because of its importance, has made digital identities prime targets for malicious threat actors.

With identities in the crosshairs of threat actors, there is a surge in identity-related breaches that underscore the necessity of robust Identity Threat Detection and Response (ITDR) disciplines. ITDR is a relatively new concept of cybersecurity solutions that focuses on protecting user identities and identity-based systems, including those operating in the cloud. ITDR is not another piece of technology nor a silver bullet for stopping threats, but it involves a combination of security tooling, human processes, and best practices to effectively detect and respond to identity-related threats that are constantly evolving.

This paper embarks on the exploration of ITDR's multifaceted realm, underscoring its critical role within modern cybersecurity frameworks. Against the backdrop of an ever-evolving threat landscape, there are four primary pillars to ITDR's effectiveness: Identity Baseline, Risk Identification, Detection & Alert Management, and Response Mechanisms. All of these pillars are pivotal in fortifying identities and protecting sensitive organizational data. Anchored by the core tenets of the zero-trust paradigm, ITDR emerges as an indispensable guardian, fortified by a synergy of technology, processes, and human elements.

Setting the stage: The threat landscape

Before diving into the four core pillars of ITDR, we need to understand what is driving its need and resulting in the increase in identity-related breaches and attacks. In PwC's annual Year in Retrospect report [1], we assessed that in 2023 the threat landscape would be dominated by the targeting of identity and privileged access capabilities, as a broad range of threat actors continue to evolve and employ new techniques to bypass security mechanisms. This assessment, by most accounts, has proven to be true.

According to the annual Verizon Data Breach Investigations Report [2], since 2022, a staggering 80% of breaches have been attributed to such targeted identity attacks, prompting a proactive approach to safeguarding individual and collective digital identities. Recent reports from the Identity Defined Security Alliance (IDSA) also parallel Verizon's figure, with a staggering 84% of organizations surveyed encountered identity-related breaches [3]. Phishing, spear phishing, and brute force attacks, constitutes 62% of those reported breaches [4]. The increase of adversary-in-the-middle (AiTM) attacks, in conjunction with a proliferation of commodity malware with the capability to hijack valid sessions or steal security tokens that bypass authentication controls are all becoming major concerns for organizations trying to protect digital identities.

In an attempt to show some of the most common and concerning identity-related threats, we have created an overview of the threat landscape as it relates to observed identity-related attacks, grouped by specific attack type and ordered from opportunistic to targeted attacks.

- **Password attacks** target different aspects of password security and are often opportunistic and easy to achieve, regardless of an organization's environment (i.e., on-premises, hybrid, or cloud). Common types of password attacks include credential stuffing, password spraying, phishing, and pass-the-hash.
- **Post-authentication attacks** occur after a user has successfully authenticated and gained access to a system. These attacks can be highly effective as they operate within a valid user session and are not dependent on any specific technology or environment to be effective in an attack. Common post-authentication attack methods include token theft, consent phishing, and kerberoasting.
- **Multi-factor authentication (MFA) attacks** aim to bypass or compromise the security provided by MFA mechanisms. These attacks are often more targeted and include methods such as SIM swap, MFA fatigue, and adversary-in-the-middle (AiTM). MFA attacks span a wide range of environments similar to password and post-authentication attacks (i.e., on-premises, hybrid, or cloud).
- **Authentication bypass attacks** exploit vulnerabilities in authentication mechanisms to gain unauthorized access without valid credentials. These attacks can be targeted or occur due to misconfigurations, often observed with misconfigured cloud environments. Common authentication bypass methods include exploits and SSO misconfigurations.
- **Identity infrastructure attacks** target the foundational systems and services responsible for managing both human and non-human identities within an organization. These sophisticated attacks, often orchestrated by skilled threat actors, specifically aim at compromising the integrity of identity management. Common identity infrastructure attacks encompass threats directed at critical components such as federation servers, instances of token forgery, and deliberate attacks on identity providers. These attacks pose significant risks as they can compromise the trust and functionality of automated processes, system-to-system interactions, and other non-human identity-related functionalities vital for organizational operations

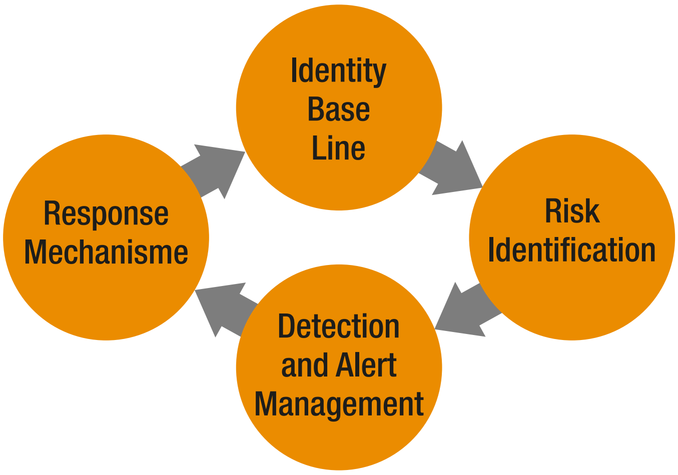
This provided overview is intended to frame the always evolving and sometimes complex attacks against identities. As the threat landscape continues to evolve, so does ITDR; but the next section will look at the pillars that help underpin the core concepts of ITDR which make it a long lasting success factor regardless of how the threat landscape evolves.

The 4 Pillars of ITDR

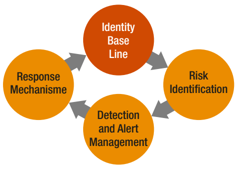
Gartner defines ITDR as a security discipline that includes tools, processes, knowledge base, best practices, and threat intelligence to protect identity systems [5]. Implementing ITDR requires more than just a product or technology; organizations need to implement key capabilities and processes to mitigate, detect, and respond to identity threats quickly.
To support our clients in their ITDR implementation program, we have defined an ITDR framework aiming to act as a safeguard against identity threats in the modern digital age.

The ITDR framework comprises four pillars and a continuous delivery and continuous improvement approach that helps organizations starting from any ITDR maturity level and collect fast results.

In this section, we'll break down the four key pillars of our ITDR framework and show how they work together to spot and counter identity-related threats effectively.

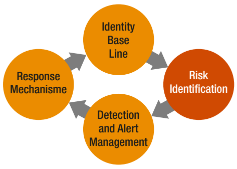


1. Identity Baseline



The first pillar of the ITDR framework is dedicated to establishing a solid identity foundation based on the identity-first security capability. It encompasses defining and meticulously monitoring the identities, accounts, authentication, and authorization of various entities, which can be employees, customers, partners, machines, applications, or IoT devices. As part of the identity-first security implementation, behavioral analytics can be used to enhance this definition.
This technology continually observes user activities, transactions, and interactions across digital platforms, analyzing historical and real-time data and adjusting the behavioral profiles, for example, when an identity travels to a new location, or changes its role.

2. Risk Identification



In this pillar of the ITDR framework, our primary focus is on recognizing and comprehending risks. ISACA* defines risks as the potential for unfavorable outcomes stemming from incidents, events, or actions. It's imperative to recognize that each organization confronts distinct and often industry-specific risks. These risks can manifest in various ways, including but not limited to brand damage, financial loss, legal ramifications, and other adverse consequences.

Risks are inherently interconnected with the variables of threats and vulnerabilities. The formula Risk = Threats x Vulnerability underscores this connection. Risks emerge when potential threats – events or actions that could harm an organization's assets – intersect with vulnerabilities, which represent weaknesses within the organization that threats can exploit.

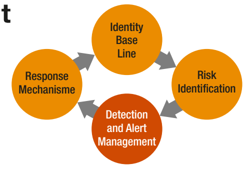
To effectively manage these risks, organizations rely on threat intelligence. This essential resource provides insights into emerging threats, tactics, and trends, helping pinpoint those relevant to the organization's unique circumstances.

* ISACA is an international professional association focused on IT governance.

In this pillar, we also prioritize the assessment of vulnerabilities within the digital ecosystem and the level of user security awareness. The identification of these vulnerabilities and the potential gaps in security awareness is equally critical. It ensures that the organization is well-prepared to address and mitigate risks effectively. This comprehensive risk identification serves as the cornerstone for the creation of a customized defense strategy in the ever-evolving threat landscape.

3. Detection and Alert Management

In this pillar of the ITDR framework, we delve into the critical process of detecting and managing identity threats. Proactive monitoring must be implemented to support on identifying malicious and fraudulent access to Identity data, and to determine if identities have been compromised. In combination with the identity monitoring defined in the identity baseline pillar, SIEM tools and threat intelligence are crucial to analyze the collected data for patterns, anomalies, known attack signatures, emerging threats, and generate alerts or request additional information from the users.



However, it’s crucial to underscore that this pillar should only follow the clear identification of risks, threats, and vulnerabilities from the previous “Risk Identification” pillar. This sequence is vital for creating a robust detection mechanism. By doing so, organizations can avoid the pitfall of alert fatigue, a scenario where a barrage of alerts overwhelms security teams, rendering them unable to address the genuine threats. Alert fatigue can be extremely perilous, as it leaves organizations exposed to potential breaches.

The key to mitigating alert fatigue lies in the establishment of actionable use cases. It is essential to clearly define the conditions under which alerts should be triggered. This involves identifying specific use cases that are both relevant and actionable. When an alert is received, it must be accompanied by a set of clear and actionable steps. These actions should guide security teams on how to respond effectively. If an alert lacks actionable instructions, it is considered irrelevant. An actionable use case not only identifies a potential threat but also prescribes the necessary response, reducing response time and minimizing the risk of falling victim to identity threats.

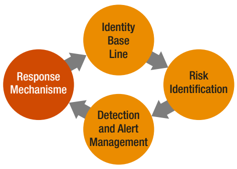
A key component to creating actionable use cases, while also being able to detect the threat is cyber threat intelligence. In simple terms, threat intelligence is intelligence on the hacking of computers and networks. It refers to information that is collected, analyzed and used to understand and respond to cyber threats. It involves gathering data on attacks, identifying the actors behind them, and assessing the risks they pose to an organization. This information is used to proactively adjust defenses and detection strategies according to emerging threats, attack vectors, and adversary tactics.

Threat intelligence applied within the context of ITDR is often geared toward technical and operational practitioners, integrated with security systems and reliant on collection, processing and exploitation of technical information.

Most likely deep dark web intelligence (DDW) will be used to identify compromised credentials Security teams can then use this intelligence to validate the authenticity of user credentials and take necessary actions, such as requiring password resets. For example, consider a use case of “User Credentials are Compromised.” This use case involves the detection of unauthorized access or a breach of user credentials often initially alerted on by threat intelligence.

When an alert for “User Credentials are Compromised” is received, the security team is provided with a clear set of actionable steps based on the relevant threat intelligence. These may include isolating the affected account, resetting passwords, and conducting a thorough security audit. The predefined actions guide the response and enable a swift and effective countermeasure. Furthermore, custom hunting rules based on threat intelligence can be crafted to further match on indicators against various logging sources. Also, intelligence integration into User and Entity Behavior Analytics (UEBA) systems could help with monitoring user and entity behavior to detect anomalies. By comparing observed behavior with known threat indicators, organizations can identify suspicious activities like unusual login times, geolocations, or access patterns.

4. Response Mechanisms
You've seen how important actionable use cases are and how crucial they are before starting this pillar. In response to identified identity threats, two primary response mechanisms can be employed:



First, automated playbooks come into play. These playbooks are designed to swiftly execute predefined responses to common threat scenarios. In this pillar, you will find that a significant majority of attacks can be effectively mitigated. These automated actions encompass a range of potential responses, including isolating compromised accounts, patching vulnerabilities, and restoring affected systems. By automating these actions, organizations can respond with efficiency and consistency, ensuring that well-known threats are mitigated promptly.

Technology vendors are increasingly integrating GenAI capabilities into the design of automated response mechanisms. By employing machine learning and AI to continuously analyze and learn from historical threat data and evolving attack patterns. This integration allows automated playbooks to become more adaptive and proactive in response to emerging threats, effectively enhancing an organization's defense posture in an evolving threat landscape.

Second, manual human response is another essential component of the response pillar. This approach involves the expertise of security professionals and incident response teams. They come into action when dealing with more complex, uncommon, or novel threats that may not be covered by automated playbooks. Human response extends beyond the technical realm, encompassing communication strategies, stakeholder engagement, reputation management, and regulatory compliance. This comprehensive approach ensures that the organization can effectively manage and recover from identity threats, even in unique and challenging circumstances.

Case Study

So, you might ask yourself, what does all of this look like in practice? Let's take a look at a real case study that involved a real threat actor, abusing real identities, and how this data enhanced defenses for ITDR.

The provided case occurred in July 2022, when a threat actor attempted to compromise an environment to exfiltrate sensitive data [6].

A Russia-based threat actor that PwC tracks as Blue Dev 5 is most well known for the Solar Winds supply chain compromise. Blue Dev 5 uses unique tactics and techniques. Broadly, the threat actor relies on compromising cryptographic roots of trust in order to undermine authentication processes; this has included SAML signing certificates, Duo 2FA keys, and cryptographic certificates used to authenticate email protection products.

PwC responded to an incident associated with Blue Dev that showed an account in the victim's environment was compromised. The threat actor authenticated to an account in the victim's Entra ID (formerly known as Azure AD) tenant, using valid credentials from a specific IP address. There were no observed failed authentication attempts to this account on the date of the successful login, indicating that the credentials were acquired some time before.

The account in question was of an individual who no longer worked at the victim organization. The account was created and used prior to the victim organization enforcing MFA, and so, no MFA method was enrolled with the account. As a result, the first sign-in failed as the user needed to enroll a second authentication factor to access the victim's Entra ID. The threat actor then enrolled a new MFA method, a software OATH token. As such, the targeting of this dormant account allowed the threat actor to gain access to the victim's cloud environment.

The described activity shows the variety of techniques at this threat actor's disposal to abuse or circumvent identity security practices and controls. The insights obtained, particularly the indicators of compromise and specific threat actor capabilities, were directly fed into our threat intelligence service for clients to consume for better defenses. Ultimately resulting in identifying this threat, reducing associated risks, and responding in a timely manner.

Conclusion: The Harmonious Ensemble

In today's world of digital transformation and accompanying cyber threat landscape, the provided ITDR framework plays a crucial role for securing an organization against the modern threat. Cyber security can often feel at times like playing jazz, improvising a response to a call using complex cords, but the momentum of keeping pace with the threats can be achieved through ITDR. It's the harmonious ensemble where each of the four pillars of ITDR are the key to keeping pace, as they operate like members of a symphony orchestra. Picture a scene where the orchestra [security operations team] takes its place on the stage, and each musician [specialist or engineer], with their unique instrument [role and skills], represents one of the four pillars: Identity Baseline and Behavioral Analytics, Risk Identification, Detection and Alert Management, and Response Mechanisms.

Just as in a symphony, where the strings, woodwinds, brass, and percussion sections seamlessly blend their sounds to create a breathtaking composition, these four areas come together to orchestrate the security of the organization. The Identity Baseline sets the foundation, while Risk Identification identifies the notes of potential risks. Detection and Alert Management act as the conductor, ensuring that the melodies of security threats are heard and addressed. Finally, Response Mechanisms are the performers, translating the sheet music of prepared actions into a graceful, coordinated response.

The synergy among these components defines the strength of the ITDR framework, much like a masterful performance of an orchestra. Just as every instrument in an orchestra has a unique role, every pillar in the ITDR framework contributes to the organization's security symphony, ensuring a harmonious and effective defense against identity threats.

How can we help?

Our suite of services is tailored to strengthen your organization’s security posture by thoroughly assessing, designing, implementing, and managing digital identity frameworks aligned with the Zero Trust model.

Digital Identity Assess and Design Service
Our Digital Identity Assess and Design service forms the cornerstone of our approach, meticulously tailored to the principles of Zero Trust. This service involves a comprehensive assessment and strategic blueprinting of your organization’s security infrastructure:

- **Understanding Your Risks and Challenges:** Collaboratively identifying and comprehending the intricacies of your organization’s unique risks and challenges.
- **Blueprint for Security:** Crafting a security architecture precisely tailored to align with your security and business aspirations.
- **Assessing Your Present:** Evaluating your current security posture to reveal areas ready for optimization and enhancement.
- **Clear Roadmap:** Delivering a detailed roadmap, derived from our assessment, to guide your organization towards a secure and fortified future.

This service, fortified by the Zero Trust paradigm and bolstered by Identity Threat Detection and Response (ITDR), facilitates the creation of a robust access framework tailored to your business fabric. It empowers your security strategy to adapt and evolve, keeping pace with the ever-evolving threat landscape.

Implement and Operate Services
Complementing Digital Identity Assess and Design, our Implement and Operate service extends beyond design to operational implementation and management of these solutions:

Our experts not only design your security framework but also implement, monitor, and fine-tune these solutions in real-time, ensuring their effectiveness against evolving threats. Leveraging the detailed roadmap derived from the Assess and Design phase, the Implement and Operate service strategically employs this roadmap as a guiding blueprint for the implementation phase. This ensures a seamless transition from design to operational implementation, fortifying your digital security and continuously adapting to emerging threats.

Contacts

For further details or to initiate the assessment process, kindly find our contact information provided below.

Gerald Horst
Partner, Cybersecurity & Digital Identity
gerald.horst@pwc.com
Tel: +31 (0)65 517 51 51

Ivo Van Bennekom
Partner, Cybersecurity & Digital Identity
ivo.van.bennekom@pwc.com
Tel: +31 (0)63 911 54 02

Fadi Daood
Manager
fadi.daood@pwc.com
Tel: +31 (0)63 875 94 32

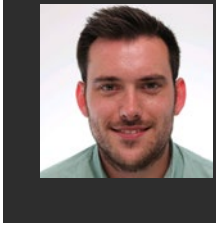
References

1. **PwC Cyber Threats 2022: A Year in Retrospect**
   https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html
2. **2023 Verizon Data Breach Investigations Report**
   https://www.verizon.com/business/resources/T282/reports/2023-dbir-executive-summary.pdf
3. **2022 Trends in Securing Digital Identities report**
   https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/
4. **2023 Trends in Securing Digital Identities report**
   https://www.idsalliance.org/white-paper/2023-trends-in-securing-digital-identities/
5. **Gartner ITDR Definition**
6. **PwC Threat Intelligence, CTO-QRT-20220720-01A - Blue Dev 5 - MFA Evasion using dormant accounts**

About the Authors:

Fadi Daood: Fadi is an experienced Information Security architect leading PwC's Zero Trust community in EMEA.

Rogerio Rondini: Rogerio is a Senior IAM Architect with vast experience on designing and implementing complex IAM solutions.



Curtis Hanson: Curtis is Experienced threat intelligence expert specializing in researching threat actors, tools, techniques, and recent attack vectors.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. At PwC in the Netherlands over 5,300 people work together. Find out more and tell us what matters to you by visiting us at www.pwc.nl.