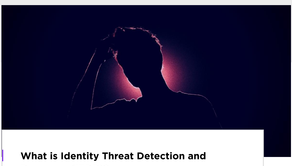

What is Identity Threat Detection and Response (ITDR)?

August 2, 2021
by SentinelOne

With identity-based attacks on the rise, today's businesses require the ability to detect when attackers exploit, misuse, or steal enterprise identities. This need is particularly true as organizations race to adopt the public cloud, and both human and non-human identities continue to increase exponentially. Given the penchant for attackers to use credentials and leverage Active Directory (AD), it is now critical to detect identity-based activity.

Identity Threat Detection and Response (ITDR) is a new security category adjacent to Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Network Detection and Response (NDR), and other detection solutions. While some might want to ask whether the industry needs yet another acronym amid cybersecurity's seemingly endless alphabet soup, ITDR fills a significant gap in the identity security landscape. ITDR differentiates itself from identity protection systems in that it focuses on protecting credentials, privileges, cloud entitlements, and the systems that manage them. It represents an important step forward, marking the introduction of a new category of security tools.

Understanding Today's Threats

The threat to identities is genuine, and given the damages occurring with their misuse, it should be a priority for every CISO. According to the 2021 Verizon Data Breach Investigations Report, credential data now factors into 61% of all breaches. More broadly, the "human element" factor into 85% of breaches, while phishing is present in 36% of them. These stats highlight that attackers consistently attempt to access valid credentials and use them to move throughout networks undetected. Credential misuse has also enabled the growth of attack tactics like Ransomware 2.0, with ransomware now making up 10% of all breaches (double what it was in 2019).

Verizon is not the only organization to note this shift. In a recent publication, Gartner estimated that "75% of security failures will result from inadequate management of identities, access, and privileges" by 2023, up from 50% in 2020. With this in mind, the need for more robust identity security is clear—especially the ability to detect suspicious activity leveraging valid account credentials.

What Sets ITDR Apart

At its core, Identity Threat Detection and Response features the ability to detect credential theft and privilege misuse and attacks on Active Directory and risky entitlements that create attack paths. ITDR solutions are specifically about protecting identities, entitlements, and the systems that manage them. This emphasis is in stark contrast to existing identity protection tools like IAM, PAM, or IGA, which generally focus on authorization and authentication and making sure the right people have access to the resources they need. ITDR, alternatively, steps in to provide visibility to credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to AD to multi-cloud environments.

Some organizations believe that they are protected if they have deployed EDR. EDR is a robust control for looking at attacks on endpoints and for collecting data for analysis. ITDR solutions operate differently and work by looking for attacks targeting identities. Additionally, once an ITDR solution detects an attack, it adds a layer of defense by providing fake data that redirects the attacker to a decoy. It can also automatically isolate the compromised system conducting the query. ITDR solutions also assist in the incident response by collecting forensic data and gathering telemetry on the processes used during the attack.

Some ITDR solutions will also manage the identity attack surface by providing an organization with visibility to exposures that leave enterprise identities open to attack. These could be stored credentials on endpoints, AD misconfigurations that allow attackers to extract data or conduct attacks, or overly permissive entitlements in cloud environments that can give attackers access to sensitive or critical workloads and data. Reducing these exposures limits protects enterprise identities by limiting what attackers can exploit.

An increasing number of attacks are jumping from on-premises to the cloud. ITDR solutions seamlessly extend to the cloud and deliver detailed entitlement visibility for identities that include users, applications, containers, serverless functions, and other assets. With so many human and non-human identities to manage, permission sprawl has become a severe issue. The widespread shift to remote working, cloud migration, and increasing adoption of DevOps practices have further elevated the need to limit the ability of attackers to obtain excessive rights or the privileges they need to move across domains.

Rethinking Security with ITDR

Today, identity security is central to the cybersecurity threat landscape, and the ability to detect and respond to identity-based threats is essential. While many tools intend to keep networks secure, ITDR gives organizations a critical new weapon in their arsenal to find and fix credential and entitlement weaknesses and detect live attacks on a real-time basis. As modern cybercriminals attempt to exploit vulnerable credentials and entitlements to move through networks undetected, ITDR solutions play a meaningful role in stopping them, whereas other tools simply cannot.

SentinelOne Identity Threat Detection and Response Solutions

SentinelOne has leveraged its deep experience in privilege escalation and lateral movement detection to become a significant player in the ITDR space. In the last year, the company has secured its leadership position based on its broad portfolio of ITDR solutions, which include:

Singularity™ Identity for:

- protection against credential theft and misuse
- attack path visibility and attack surface reduction
- detection of unauthorized activity and attacks on Active Directory

Ranger® Identity Assessor for AD for:

- continuous visibility to exposures with Active Directory and activities that would indicate an attack

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Windows Security Identifier (SID) History Injection Exposure
- Detecting Unconstrained Delegation Exposures in AD Environment
- Building Blocks For Your XDR Journey: Part 3 | The Value of Securing Identity
- Identity-Based Attack Innovation Drives the Demand for a New Security Approach
- Top 10 Ways to Protect Your Active Directory
- Protecting Your Active Directory from AdminSDHolder Attacks