

IDENTITY THREAT DETECTION (ITDR).



Attackers increasingly log in rather than break in, authenticating with stolen valid credentials and tokens that never touch a monitored endpoint. ITDR watches the identity infrastructure itself for the specific patterns credential theft produces, since nothing else is built to catch it.

- CREDENTIAL ABUSE DETECTION
- HONEYTOKENS & DECEPTION
- KERBEROS ATTACKS
- SESSION REVOCATION

01 THE MECHANISM

Credential-Based Attacks, Not Malware

Attackers increasingly authenticate with stolen valid credentials or tokens rather than dropping malware, so **signature and file-based detection tools see nothing to flag**.

Directory & Identity Provider Telemetry

ITDR watches the authentication infrastructure itself — Kerberos ticket requests, sign-in logs, conditional access changes — for **the specific patterns credential-theft techniques produce**.

Deception & Honeypots

Decoy credentials and accounts with no legitimate purpose generate a **near-zero false-positive signal** the moment anyone touches them, since nothing should ever use them.

02 THE FLOW

The Monitored Identity Layer

CONTAINED

1

Kerberos ticket requests, sign-in anomalies, and conditional access changes are **continuously correlated against known attack patterns**.

2

A honeypot account with no legitimate use gets authenticated against, **flagging the attacker's presence with high confidence** and minimal noise.

3

The session's tokens are revoked and the account force-reauthenticated **before the attacker can escalate or move laterally** with the stolen credential.

The Unmonitored Identity Layer

EXPOSED

1

An attacker harvests a service account's Kerberos ticket offline and cracks its password **without ever touching an endpoint that EDR would flag**.

2

The stolen credential authenticates normally — **no malware, no unusual process**, nothing an endpoint agent has any reason to catch.

3

Because directory and identity-provider logs are never monitored for these patterns, the attacker **moves laterally using credentials that look completely legitimate**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Identity Telemetry & Detection	Continuous monitoring of directory service and identity provider logs for the specific patterns credential-theft and ticket-forgery techniques produce.
Deception (Honeytokens)	Decoy accounts and credentials with no legitimate use, so any authentication against them is an inherently high-confidence compromise signal.
Exposure & Posture Assessment	Ongoing discovery of identity infrastructure weaknesses — unconstrained delegation, exposed KRBGT risk, excessive standing privilege — before an attacker finds them first.
Response & Containment	Session and token revocation, forced re-authentication, and credential rotation scoped to identity infrastructure specifically, not just endpoint isolation.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Endpoint Detection (EDR) Alone	No	Credential-theft attacks that never drop a malicious binary or touch a monitored process produce nothing for EDR to flag.
IAM/PAM Governance Without Runtime Monitoring	No	Provisioning least-privilege access controls who should have access; it doesn't detect a valid credential already being actively misused.
Anomaly Detection (UEBA) Alone	No	Behavioral baselines generate false positives on legitimate unusual activity and can miss attacks that mimic normal-looking authentication.
Password Rotation as the Primary Control	No	Stolen tickets, tokens, and hashes remain valid within their own lifetime regardless of how often the underlying password is rotated.
Directory/IdP Telemetry + Honeytokens + Exposure Assessment + Token Revocation	Yes	Combines high-confidence deception signals with continuous posture monitoring and real containment capability.

IDENTITY THREAT DETECTION (ITDR).

MONITOR · DETECT · REVOKE

05 PROGRAM OPERATIONS

Attackers who authenticate with stolen valid credentials produce no malware for an endpoint agent to see. Identity telemetry, not endpoint telemetry, is what actually catches this class of attack.

A honeytoken's value comes from its near-zero false-positive rate. No legitimate process or user should ever touch it, unlike behavioral anomaly detection which is inherently noisier.

Standing privileged access is a bigger blast radius than just-in-time elevation. A stolen credential with permanent admin rights is worth far more to an attacker than one with none until elevated.

Kerberos ticket lifetimes mean a stolen or forged ticket stays valid regardless of password rotation. Revoking the specific session, not just changing the password, is what actually contains it.

06 CONTROL MAPPING

MITRE ATT&CK

Credential Access & Lateral Movement tactics — Kerberoasting, Golden/Silver Ticket forgery, Pass-the-Hash — map directly to what ITDR detections catch.

NIST SP 800-207

Zero Trust Architecture defines continuous identity verification as a core tenet ITDR operationalizes, rather than trusting a session because initial authentication succeeded.

NIST SP 800-63

Digital Identity Guidelines establish the identity assurance levels and authentication strength baselines ITDR risk signals are measured against.

CISA IDENTITY GUIDANCE

Advisories and best practices specifically addressing Active Directory and Kerberos attack detection and mitigation.

07 WHAT THIS DOES NOT SOLVE

Initial Credential Theft

ITDR detects misuse of a stolen credential; it doesn't stop the **phishing or infostealer** that got the credential stolen in the first place.

Over-Provisioned Access by Design

Detecting misuse of excessive standing privilege doesn't fix the **governance failure that granted it** — that's an IAM/PAM problem, not a detection one.

Third-Party Identity Provider Compromise

If the identity provider is compromised at the vendor level, **no tenant-side monitoring** catches an attack originating upstream of it.

Non-Identity Attack Vectors

Malware, vulnerability exploitation, and exfiltration that **don't involve identity infrastructure** fall outside what identity-focused detection is built to see.

08 MYTHS VS. REALITY

MYTH

"Our EDR/XDR platform already covers this."

REALITY

Credential-theft attacks that never touch a monitored endpoint process **produce nothing for EDR to see** — identity telemetry is a different data source entirely.

MYTH

"Strong password policies stop credential-based attacks."

REALITY

Pass-the-Hash, Pass-the-Ticket, and forged Kerberos tickets **don't require knowing the actual password** at all.

MYTH

"MFA makes identity-based attacks a non-issue."

REALITY

Token theft and session hijacking bypass MFA by **stealing the proof of authentication that already happened**, and push-bombing can trick a user into approving it directly.

MYTH

"Rotating passwords regularly contains a credential compromise."

REALITY

A stolen session token or forged ticket remains valid within its own lifetime regardless of a password change — **the specific session needs to be revoked**.

MYTH

"IAM and ITDR are the same thing."

REALITY

IAM governs who should have access; **ITDR detects and responds to active misuse** of access that was already granted.

09 SPEAK THE PROGRAM — KEY TERMS

KERBEROASTING

Requesting Kerberos service tickets for accounts with an SPN and **cracking the ticket offline** to recover the service account's password.

GOLDEN TICKET

A forged Kerberos ticket-granting ticket built from a stolen KRBTGT hash, granting **persistent, near-total domain access**.

PASS-THE-HASH

Authenticating using a captured password hash directly, **without ever knowing or cracking** the actual plaintext password.

HONEYTOKEN

A decoy credential or account with no legitimate use, so **any authentication attempt against it** is an inherently high-confidence compromise signal.

STANDING PRIVILEGE

Access rights that remain active at all times rather than granted just-in-time, **expanding what a stolen credential is immediately worth**.

UEBA

User and Entity Behavior Analytics — behavioral baselining used to flag **anomalous authentication or access patterns** like impossible travel.