Buyer's Guide to Identity Threat Detection and Response

Cyberattackers are often creative, persistent and focused. But they are also quite methodical. In most cases, as attackers traverse the middle of the attack chain, they use readily available tools and techniques to discover and understand your IT environment. They seek to escalate their privileges and move laterally through your network on their way to their ultimate goal: your most critical IT assets, or "crown jewels." And given enough dwell time, once they gain a foothold in your network, they will indeed reach their ultimate destination. That is, unless you detect them and respond effectively.

Sophisticated attackers rely on target organizations to leave behind identities and credentials that they can use to advance their attacks. But they also expect that what they see is real and that the network, user and system data they collect is reliable. This is a key weakness. With the deployment of identity threat detection and response systems, this reliance is their Achilles heel. These systems protect against the progression of identity-based threats. They defend the middle of the attack chain, where privilege escalation and lateral movement occur.

This buyer's guide highlights the critical required capabilities for identity threat detection and response systems. The advice it provides is based on Proofpoint expertise in security control areas as well as our years of experience in the emerging identity threat detection and response category.

It describes the following areas of coverage:

- General requirements
- Discovery and remediation of identity vulnerabilities
- Detection and response to active threats

This guide also discusses the emerging importance of deception technologies. It explains how they are changing the game for identity threat detection and response systems when compared with traditional signature or behavior-based detections.

General

In high-impact cyberattacks, adversaries often use credential phishing, malware or insider threats to initially compromise an environment. After gaining entry and disabling local agent-based security, they then move to their ultimate target. This movement—lateral within the enterprise or cloud; vertical to and from the enterprise and cloud—requires both credentials and connectivity. At this point, the threat actors are in the middle of the attack chain. Using myriad tools and automation, attackers begin "living off the land" through further credential harvesting, network scanning and privilege escalation. Because this activity often looks like normal user or application activity, it can be very challenging to detect using traditional tools. But this is where identity threat detection and response systems can shine.

The following table provides an overview of the general capabilities that an identity threat detection and response solution must provide to address this challenge, both before and after the arrival of a threat actor.

General Areas of Coverage

CUSTOMER NEED	REQUIRED CAPABILITY
Understand precisely where the organization is currently vulnerable to privilege escalation and lateral movement	An identity threat detection and response system should identify currently vulnerable identities and associated credentials that would provide an attack path to an attacker post initial compromise. The solution should also make this data available as context to systems that track the most highly attacked and privileged people in the organization.
Continuously discover and eliminate the paths for lateral movement and privilege escalation	An identity threat detection and response system must: • Find and present high-risk attack pathways to critical IT assets • Uncover forgotten connections and errant credentials that facilitate attacker mobility • Automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.
Improve detection and response	An identity threat detection and response solution should detect and respond to active threats with high fidelity (low false positives and false negatives). In addition, it should collect source-based forensic data in real-time from compromised machines to assist with incident response.
Identify what and who is being targeted and actively attacked and understand the root cause of a successful attack	An identity threat detection and response solution should provide contextual information—who, what, when and how—to inform all stages of the attack chain. This information provides critical context for initial compromise, lateral movement, and what control failures contributed to any data exfiltration or other forms of business impact. A solution should provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.

Discover and Remediate Identity Vulnerabilities

An identity threat detection and response solution should allow you to discover and remediate identity vulnerabilities before the attackers can take advantage of them. It must be able to map and provide a comprehensive view of the presence of vulnerable and privileged identities across the entire enterprise, including endpoints, directories, identity stores, and PAM systems.

Vulnerability Discovery and Remediation

CUSTOMER NEED	REQUIRED CAPABILITIES
Discover and track vulnerable identities across the enterprise	An identity threat detection and response solution should discover: • Insufficient or improper PAM configuration and management of service-account, local-administrator, and privileged-domain credentials • Unintentional creation of shadow admin accounts that have excessive privileges. • Improper termination of RDP sessions • Stored credentials on endpoints—including web browsers, SSH, FTP, PuTTY, command lines, and databases—that cache credentials and cloud access tokens on endpoints.
Discover and track account-based policy violations	An identity threat detection and response solution should identify: • Misconfigured accounts • Legacy app accounts • Stale accounts • Password policy violations • Kerberoastable credentials • Unmanaged user accounts • Unmanaged service accounts
Automatically remediate identity threats without impacting business operations	An identity threat detection and response solution should use continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Cloud tokens • Stale or disconnected RDP sessions • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems.
Initiate the remediation of identity vulnerabilities leveraging integration with an IT Service Management system (ITSM)	For those vulnerabilities which cannot be safely remediated with automation, an identity threat detection and response solution should be able to open tickets in the organization's ITSM system so that these vulnerabilities can be managed and remediated as part of the organization's normal IT business processes

CUSTOMER NEED	REQUIRED CAPABILITIES
Visualize and prioritize available attack paths	An identity threat detection and response system should: • Discover vulnerable identities, exposures and misconfigurations • Provide insight into how a combination of these vulnerabilities can provide attack paths to crown jewel IT assets or other critical or sensitive systems • Present attack paths and how to remediate them in an actionable and visually effective way • Provide an interactive graphic that provides deeper context and remediation guidance
Discover and track crown jewel IT assets	Identity threat detection and response-based security controls should: • Begin with understanding what IT systems are a priority to protect. • Be able to automatically discover and flag hidden or shadow Tier 0 assets
Integrate with a broad set of security and IT systems	An identity threat detection and response solution should be able to: • Interoperate with and complement an organization's security and IT stack • Discover identity vulnerabilities and their relationship to each other and the organization's crown jewel IT assets • Pull and analyze identity data from AD, Entra ID, cloud identity stores, PAM systems and endpoints, both clients and servers - PAMs including: CyberArk and Delinea • Provide broad endpoint coverage, including Windows, Linux, and Mac operating systems • Integrate with SIEMs/XDRs, SOARs and host operating systems to detect, investigate and respond to active threats. - Including CrowdStrike Falcon, Splunk, LogRhythm, Microsoft Defender • Integrate with the organization's ITSM and software distribution systems to facilitate the collaboration between security and IT teams

Detect and Respond to Threats

An identity threat detection and response solution must detect with high-fidelity and aid the efficient response to active threats. The following table provides a review of the key customer detection and response needs and required capabilities for an identity threat detection and response system.

Threat Detection and Response

CUSTOMER NEED	REQUIRED CAPABILITIES
Catch threat actors in the act of attempting to escalate privileges and lateral movement, before they can reach the organization's crown jewels.	An identity threat detection and response solution should help you detect threat actors' actions and attempts at lateral movement and privilege escalation. It should not require a persistent agent and should not impact the daily work and risk of agent tampering. The solution should use the following methodologies: • File-based deceptions, for example with MS Office files such as MS Word or MS Excel, using the organization's document templates and realistic passwords to increase authenticity. • Beacon files to track usage inside & outside the organization, also using the organization's brand templates. • Monitoring the use of beacon files using a DLP solution to initiate detective alerts on the movement of deceptive files • Planting (or using existing) orphaned Active Directory objects as deceptive breadcrumbs • Use of the production AD system only. Eliminating the need for creating a fake AD domain with trust to the production AD system • Broadly deploy deceptive artifacts to provide network, application and system-level detection capabilities, including: - Browser histories - Database connections - Scanner data - Emails and Teams messages - FTP, RDP, PuTTY and SSH sessions - Scripts - File shares - Windows credentials - Ransomware deception - ADRecon and Bloodhound deceptions - Swift and mainframe deceptions

CUSTOMER NEED	REQUIRED CAPABILITIES
Collect incident and system forensic data to facilitate rapid and precise understanding of the attacker's activity in near real-time.	An identity threat detection and response solution should collect "source" forensics immediately after tripping the detection from the endpoints where attackers are operating, including volatile and non-volatile data, including capturing screenshots • Gather source and target-based telemetry without creating a fingerprint and without a persistent agent to avoid agent tampering or agent bypass. • Provide the unified presentation of both source- and target-based telemetry data in a timeline view. • Collect, manage, and present telemetry to the incident responder without requiring 3rd party systems or extra hardware. • Support on-demand forensic collection—from any endpoint to support ad-hoc investigations or threat hunting not directly related to a detection made by the incident detection and response system • Collect screen captures while the attacker is on the endpoint. • Provide STIX-formatted files for threat intel sharing. • Integrate with VirusTotal for additional context on file hashes used in attacks. • Collection of PCAP data to support network-level visibility of the incident • Push incident data into other technologies such as SIEM/XDR or SOARs via integrations for improved incident management. • Collect and deliver endpoint memory information. • Capture of command line input and output • Capture of PowerShell history • Collect attack path details, including protocols used. • Gather detailed process information from effected hosts. • Collect information on user and computer data from Active Directory for improved context and risk exposure.
Detect attackers with high fidelity	An identity threat detection and response solution should: • Detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent. Comprehensive coverage dramatically reduces the dwell time of an attack. • Detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege. This significantly reduces the possibility of false negatives. • Detect an attacker in the organization with near-zero false positives (all deceptions should be concealed from legitimate users).

The Role of Deception

Systems that detect active threats should not rely solely on signature- or behavior-based detections. These are not as effective as they should be and they often yield high rates of false positives and false negatives. The use of widely deployed high-quality deceptions can mitigate this problem and greatly improve the efficacy of an identity threat detection and response system.

Deception technologies accurately replicate credentials, connections, files and other data that an attacker needs to progress through the attack chain. Good deception technologies craft and deploy deceptive artifacts that both appear to be real and are tailored to each organization. They identify network systems and connections as well as Tier-1 (or "crown jewel") assets. And they are very hard to discern from real IT assets, artifacts, services and resources.

To avoid discovery and bypass by threat actors, deceptions should be agentless. They should be capable of:

- Scaling to cover an organization's entire endpoint inventory to ensure that attackers are discovered early, soon after initial compromise
- Being refreshed dynamically and automatically
- Being adjusted in response to changes in the IT environment

Deception-triggered alerts should integrate seamlessly into existing monitoring, threat-hunting, visualization and telemetry technologies. This helps with informed responses, containment and remediation measures. When a deception is triggered, the system should gather source forensics in real-time from the endpoint. This data includes details about the who, what, when and where of the attack. The system should provide this data to the SOC and incident response teams. It should also provide visibility into the attacker's proximity to critical business assets and domain administrator credentials.

LEARN MORE

For more information, visit **proofpoint.com**.