Secureworks®

WHITE PAPER

How to Enhance Your Cyber Defenses with Identity Threat Detection and Response (ITDR)

Bringing together identity protection and security operations for robust security posture

As organizations increasingly rely on digital systems and cloud services, protecting identities has become paramount. In fact, 90% of organizations experienced an identity breach in the last year[1]. Organizations face an ongoing battle against cybercriminals who continually refine their tactics. Identity protection solutions have evolved in response to these changes, moving beyond traditional identity and access management (IAM) systems to include more advanced identity threat detection and response (ITDR) platforms. This evolution reflects a shift from static access control to a more comprehensive and continuous approach that actively defends against identity-related cyberattacks.

From Usernames and Passwords to IAM

Up until the mid-2000s, identity protection primarily relied on usernames and passwords. However, over time, the limitations of this approach became evident. Passwords were often weak, reused, and easily compromised through phishing or brute force attacks.

To enhance security, multi-factor authentication (MFA) was introduced, requiring users to provide multiple verification factors. These factors typically include something the user knows (a password), something the user has (a smartphone or hardware token), and something the user is (biometric data like fingerprints or facial recognition). MFA significantly improved security by making it harder for attackers to gain access with just a stolen password and has become a standard security measure for many organizations.

As digital tools proliferated, managing multiple passwords became cumbersome, leading to the development of single sign-on (SSO). SSO allows users to access multiple applications with a single set of credentials, improving user experience and reducing the risk of password fatigue, where users might reuse passwords across different platforms.

While MFA and SSO improved general authentication processes, they did not fully address the management of privileged accounts — those with elevated permissions to access critical systems and data. Privileged access management (PAM) solutions were developed to control and monitor access to these accounts, ensuring only authorized users could perform high-risk actions. Implementing PAM helps reduce the risk of insider threats and limits potential damage from compromised privileged accounts.

Why IAM Solutions Fall Short

MFA, SSO, and PAM systems all fall into the category of IAM, a framework of policies and technologies for ensuring that the right individuals have the appropriate access to technology resources. But despite these advancements, identity threats can still bypass or neutralize IAM controls. IAM systems are complex and difficult to manage, with numerous and constantly evolving settings, policies and configurations. As a result, IAM systems are often riddled with misconfigurations and security gaps. Therefore, organizations need a comprehensive solution that not only enhances threat prevention by continuously monitoring and improving identity security posture, but also one that provides detection and response to monitor for attacks and stop them once they are in progress.

Improve Cyberattack Preparedness with ITDR

As cybercriminals have become more sophisticated, identities have become primary targets for attackers. Over the last three years, the Secureworks Counter Threat Unit™ has observed a 688% increase in stolen credentials offered for sale on a single dark web marketplace, fueling the criminal ecosystem[2]. Compromised identities can be used to bypass traditional security measures. This shift in tactics has necessitated a new approach to identity protection: ITDR.

ITDR solutions proactively prevent, detect, prioritize, and respond to identity-related threats and vulnerabilities in an organization's IT environment. They leverage advanced analytics, machine learning, and behavioral analysis to identify suspicious activities and potential compromises. Four critical components of an effective ITDR solution include:

1. **Continuous Security Posture Monitoring:** Continuously scanning IAM/IdP (identity provider) systems to identify changes in identity security posture and remediate exposures.
2. **Threat Detection:** Identifying unusual behavior patterns that may indicate a compromised identity.
3. **Automated Response:** Taking immediate action to mitigate identity threats, such as locking accounts.
4. **Dark Web Monitoring:** Monitoring and alerting when login credentials have been exposed on the dark web.

According to research firm Gartner, "conventional identity and access management and security preventive controls are insufficient to protect identity systems from attack. To enhance cyberattack preparedness, security and risk management leaders must add ITDR capabilities to their security infrastructure[3]." ITDR solutions combine data from IAM systems (like login attempts, access patterns, and user behavior) with SOC data (such as network anomalies and security alerts) to provide a comprehensive view of potential identity-related threats. By bringing together the strengths of IAM and the SOC, ITDR creates a more robust and integrated security framework that enhances an organization's ability to detect, respond to, and mitigate identity-related threats.

Over the last three years, the Secureworks Counter Threat Unit has observed a

688%

increase in stolen credentials offered for sale[2].

Enhance Your Cyber Defenses with Secureworks Taegis IDR

Secureworks Taegis™ IDR is an ITDR solution designed to improve your security posture by continuously monitoring your environment for identity misconfigurations and risks, while also providing dark web intelligence on compromised credentials. Taegis IDR uncovers identity risks in under 90 seconds[4] compared to days with legacy solutions and benchmarks the reduction of your attack surface over time. Secureworks protects against 100% of MITRE ATT&CK Credential Access techniques[5], enabling organizations to proactively detect sophisticated threats early in the attack chain and automatically respond with built-in automated playbooks. Gain comprehensive protection in a single platform across identity, endpoints, network, cloud, email, and other business systems, all without breaking your budget.

Next Steps

To learn more about how you can enhance your cyber defenses with Taegis IDR, request a demo today.

Read the Taegis IDR Datasheet.

Learn more at secureworks.com/IDR

TRY US TODAY

[1] Identity Defined Security Alliance (IDSA), 2023 Trends in Securing Digital Identities, July 2023

[2] Based on internally collected data by the Secureworks Counter Threat Unit™(CTU™)

[3] Gartner, Enhance Your Cyberattack Preparedness with Identity Threat Detection and Response, October 2022

[4] Average time to detect identity exposures calculated based on existing Secureworks customer data

[5] Based on Taegis detection capabilities mapped to the MITRE ATT&CK framework

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971
4 420 7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp