Cortex Identity Threat Detection and Response Module

Identity threats and malicious insiders are two significant threat vectors organizations face today. Identity threats often involve unauthorized access to user accounts, which can occur due to stolen or weak credentials, phishing attacks, or other social engineering tactics. On the other hand, malicious insiders are individuals within an organization who abuse their authorized access to conduct fraudulent or illegal activities, such as stealing sensitive data or committing financial fraud.

75%

Of insider threat cases involved a former employee[1]

85 days

The time to contain an insider threat incident[2]

216 days

Average time to identify and contain a data breach by malicious insider[3]

[1] 2022 Unit 42 Incident Response Report, Palo Alto Networks, July 26, 2022.
[2] 2022 Cost of Insider Threats: Global Report, Ponemon Institute, January 25, 2022.
[3] Ibid.

The Growing Challenge

While many organizations rely on traditional security approaches to protect against these threats, more than these solutions may be needed to detect identity threats and malicious insiders. These attacks often occur within an organization's network, making them difficult to detect using perimeter-based security tools.

Moreover, detecting identity-related threats is, essentially, distinguishing between suspicious but benign activity and truly malicious activity, which in most cases requires expertly crafted learning algorithms to identify and respond to potential threats accurately.

Lastly, identity threats and malicious insider attacks are often carried out over an extended period, making them harder to detect using traditional detection engines.

Understanding the Risks

Regular risk evaluations are an essential component of handling cyberwarfare properly. Regular evaluations can help ensure an organization's risk posture is aligned with its business objectives. As an organization evolves, its risk profile may change as new business units, applications, and systems are added. Regular evaluations can help identify changes in risk exposure and enable organizations to adjust their security posture accordingly.

Additionally, risk evaluations over time can assist organizations in keeping up with changes in the threat landscape. The tactics, techniques, and procedures (TTPs) used by malicious actors are constantly evolving, and organizations need to be able to adapt their security posture to stay ahead of emerging threats. Regular risk evaluations can help identify new and emerging threats and enable organizations to implement new security measures to protect against them.

To effectively manage the risks associated with identity threats and malicious insiders, organizations need to have a clear view of the potential risks and make informed decisions about mitigating those risks. This requires a comprehensive understanding of the organization's risk posture and the ability to monitor and analyze user behavior to identify potential threats.

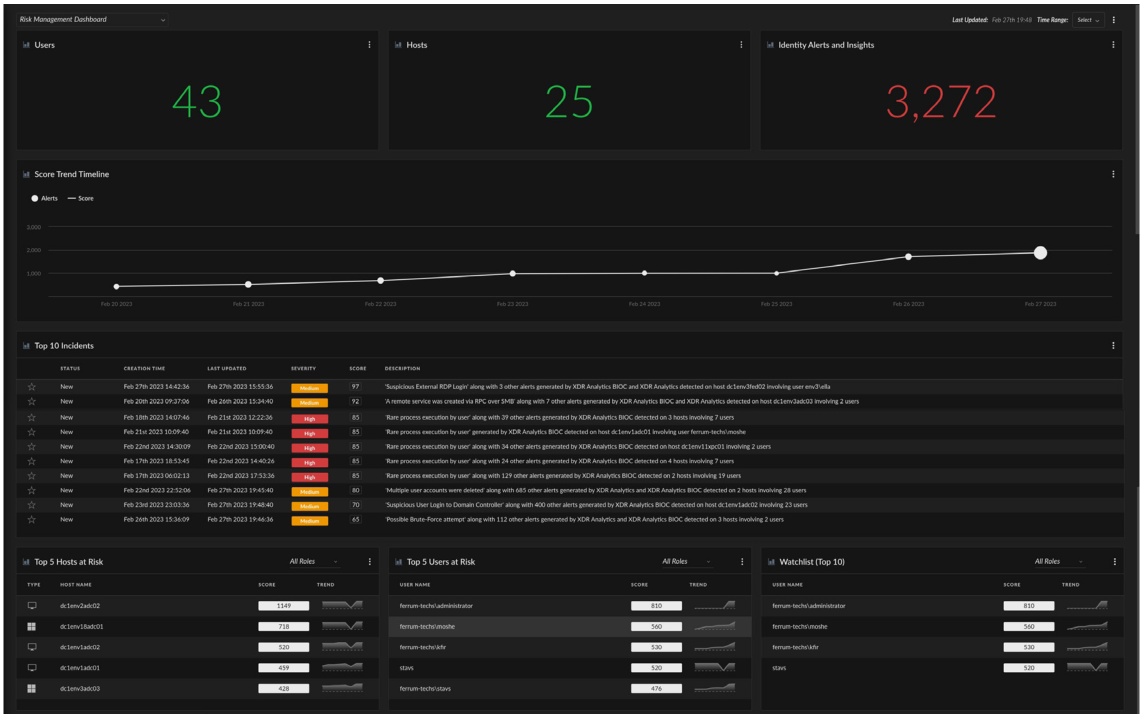
By taking a comprehensive approach to security, organizations can significantly reduce their exposure to identity threats and malicious insiders and better protect their assets and reputation.

Cortex Identity Threat Detection and Response Module

Built from the ground, the new Cortex Identity Threat Detection and Response (ITDR) Module is a cutting-edge offering designed to provide proactive protection against identity-related threat vectors, such as compromised accounts and malicious insiders. By leveraging the power of AI and automation, the module provides advanced detection capabilities that enable organizations to quickly identify, investigate, and ultimately respond to identity threats.

The new module empowers our customers to:

- Make decisions faster with enhanced views of an organization's risk posture.
- Gain forensic-level visibility into the asset to easily uncover hidden threats.
- Automate and customize the continuous analysis of user and host activities.
- Swiftly triage and investigate alerts with precise profile information.



Risk Management Dashboard

Last Updated: Feb 27th 19:48 Time Range: Select

Users

43

Hosts

25

Identity Alerts and Insights

3,272

Score Trend Timeline

Top 10 Incidents

	STATUS	CREATION TIME	LAST UPDATED	SEVERITY	SCORE	DESCRIPTION
☆	New	Feb 27th 2023 14:42:36	Feb 27th 2023 15:55:36	Medium	97	'Suspicious External RDP Login' along with 3 other alerts generated by XDR Analytics BIOC and XDR Analytics detected on host dc1env3fed02 involving user env3\ella
☆	New	Feb 20th 2023 09:37:06	Feb 26th 2023 15:34:40	Medium	92	'A remote service was created via RPC over SMB' along with 7 other alerts generated by XDR Analytics BIOC and XDR Analytics detected on host dc1env3adc03 involving 2 users
☆	New	Feb 18th 2023 14:07:46	Feb 21st 2023 12:22:36	High	85	'Rare process execution by user' along with 39 other alerts generated by XDR Analytics BIOC detected on 3 hosts involving 7 users
☆	New	Feb 21st 2023 10:09:40	Feb 21st 2023 10:09:40	High	85	'Rare process execution by user' generated by XDR Analytics BIOC detected on host dc1env1adc01 involving user ferrum-techs\moshe
☆	New	Feb 22nd 2023 14:30:09	Feb 22nd 2023 15:00:40	High	85	'Rare process execution by user' along with 34 other alerts generated by XDR Analytics BIOC detected on host dc1env11xpc01 involving 2 users
☆	New	Feb 17th 2023 18:53:45	Feb 22nd 2023 14:40:26	High	85	'Rare process execution by user' along with 24 other alerts generated by XDR Analytics BIOC detected on 4 hosts involving 7 users
☆	New	Feb 17th 2023 06:02:13	Feb 22nd 2023 17:53:36	High	85	'Rare process execution by user' along with 129 other alerts generated by XDR Analytics BIOC detected on 2 hosts involving 19 users
☆	New	Feb 22nd 2023 22:52:06	Feb 27th 2023 19:45:40	Medium	80	'Multiple user accounts were deleted' along with 685 other alerts generated by XDR Analytics and XDR Analytics BIOC detected on 2 hosts involving 28 users
☆	New	Feb 23rd 2023 23:03:36	Feb 27th 2023 19:48:40	Medium	70	'Suspicious User Login to Domain Controller' along with 400 other alerts generated by XDR Analytics BIOC detected on host dc1env1adc02 involving 23 users
☆	New	Feb 26th 2023 15:36:09	Feb 27th 2023 19:46:36	Medium	65	'Possible Brute-Force attempt' along with 112 other alerts generated by XDR Analytics and XDR Analytics BIOC detected on 3 hosts involving 2 users

Top 5 Hosts at Risk — All Roles

TYPE	HOST NAME	SCORE	TREND
🖥	dc1env2adc02	1149	
⊞	dc1env18adc01	718	
🖥	dc1env1adc02	520	
🖥	dc1env1adc01	459	
⊞	dc1env3adc03	428	

Top 5 Users at Risk — All Roles

USER NAME	SCORE	TREND
ferrum-techs\administrator	810	
ferrum-techs\moshe	560	
ferrum-techs\kfir	530	
stavs	520	
ferrum-techs\stavs	476	

Watchlist (Top 10) — All Roles

USER NAME	SCORE	TREND
ferrum-techs\administrator	810	
ferrum-techs\moshe	560	
ferrum-techs\kfir	530	
stavs	520	

Figure 1: High-level oriented dashboards providing risk statistics and trends

By combining advanced detection capabilities as part of identity analytics with the new ITDR Module that protects identity threats later on along the attack lifecycle, Cortex solutions deliver superior protection against identity-related threats all across the attack lifecycle. This integrated approach ensures that potential threats are detected and mitigated as early as possible, reducing the risk of data breaches and other security incidents.

Proactive Coverage for Stealthy Identity Threats

The ITDR Module in XSIAM and XDR delivers a machine-powered, human-enabled identity and insider threat detection capability to solve the most complex security use cases.

Combine the detection capabilities of ITDR, insider threat with analytical and risk-based detections, and UEBA.

- Reduces a disparate technology stack and lower cost.
- Replaces existing UEBA capabilities.
- Replaces some ITDR vendor capabilities.

Eliminate the need for internal advanced detection engineering to support complex analytic and risk-based detection.

- Takes advantage of Unit 42 and Cortex research driving analytic detections.
- No longer requires long-term maintenance by folks on staff.
- Offload complicated and prolong security research activities and let your internal teams focus on what really matters.

Risk-based profiles help focus investigations on the higher priority incidents.

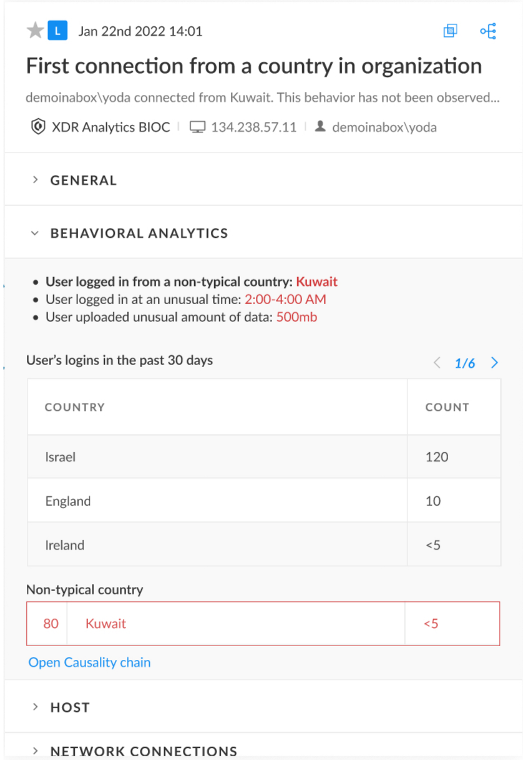
- Delivers valuable insights via peer grouping and shows users' and hosts' historical trends and patterns.
- Automated insights gained from designated classification analytics based on the applied data sources.
- Replaces risk profiling and peer grouping found in adjacent solutions today.

Faster detection and response for historically challenging security outcomes.

- Delivers with out-of-the-box detection analytics designed to uncover the stealthiest threat vectors, such as compromised accounts and insider threats.
- Automatically applies learnings from your environment to pinpoint suspicious events that deviate from baselines.

Continuous monitoring and safety net for authentication and identity solution failures.

- Support for ZTNA architectures to extend capabilities and detect violations of trust.



L Jan 22nd 2022 14:01

First connection from a country in organization

demoinabox\yoda connected from Kuwait. This behavior has not been observed...

XDR Analytics BIOC | 134.238.57.11 | demoinabox\yoda

› GENERAL

⌄ BEHAVIORAL ANALYTICS

- User logged in from a non-typical country: Kuwait
- User logged in at an unusual time: 2:00-4:00 AM
- User uploaded unusual amount of data: 500mb

User's logins in the past 30 days ‹ 1/6 ›

COUNTRY	COUNT
Israel	120
England	10
Ireland	<5

Non-typical country

80	Kuwait	<5

Open Causality chain

› HOST

› NETWORK CONNECTIONS

Figure 2: Profile exposure of the main features triggered by the detector

With the launch of Cortex XSIAM 1.4 and XDR 3.6, we continue to advance our mission to help customers protect their organization and make it easier for them to do this. The new advanced ITDR Module from Cortex XSIAM and XDR provides comprehensive coverage for stealthy identity threat vectors, including compromised accounts and insider threats, allowing you to protect your organization without slowing down the business.

How to Get the ITDR Module

Palo Alto Networks has two offerings to address identity threat use cases in Cortex XSIAM and Cortex XDR. One is with Identity Analytics, which is already part of XSIAM and XDR. The other is the Identity Threat Detection and Response Module which is offered as a paid module for XSIAM and XDR. Each module addresses the following use cases, plus more:

Table 1: Use Cases for the Identity Threat Detection and Response Module

	Identity Analytics Initial Access	Identity Threat Detection and Response Module Paid Access
Suspicious logins to SSO, AD, and VPNs (suspicious hours, geolocation, OS, user, and more)	✓	✓
MFA spamming	✓	✓
Brute force, password spray, and excessive logins	✓	✓
Irregular resource access	✓	✓
Anomalous insider activity	–	✓
Abnormal configuration manipulation	–	✓
Suspicious files	–	✓
Modification of permissions	–	✓
Exfiltration to physical devices	–	✓
Sensitive file gathering and manipulation	–	✓

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com