Palo Alto Networks and Tidal Cyber Enterprise Edition

Optimize Your Palo Alto Networks Cortex XDR Threat-Informed Defense Coverage

Key Benefits

- Get visibility into how Palo Alto Networks is addressing the most significant threats.
- Assess MITRE ATT&CK® risk with visibility into gaps and depth of defense.
- Optimize Palo Alto Networks deployment by understanding how configuration changes affect ATT&CK™ coverage.

The Challenge

Adversaries and their tactics, techniques, and procedures (TTPs) change almost daily, and threat volumes are increasing at such a steady velocity it becomes impossible to protect against every one. Security teams are working at least double time to keep up with the different intelligence and detections needed to stave off these attackers while also spending most of their time fighting high-priority issues. Even if an organization has great security tools in their tech stack, until they face an attack, they can't confidently know if they're configured correctly and doing their job defending from the threats attacking their industry.

The Solution

What if an organization could operationalize threat-informed defense by continuously comparing their security stack against MITRE ATT&CK, curated threat intelligence, and other cyber-threat intelligence (CTI) data? With this approach, an organization can fine-tune their existing defenses, identify coverage gaps, and ensure they're protected against the most relevant adversary TTPs. By mapping their current tool coverage to known threats, an organization can gain clear visibility into where they're strong and where they need to improve. Plus, by toggling between different tool configurations, they can explore how changes impact coverage—empowering smarter, data-driven decisions to strengthen their defense.

Tidal Cyber Enterprise Edition

Tailoring defenses to adversary behavior is a smarter, more strategic way to protect organizations. Tidal Cyber® Enterprise Edition makes it easy to identify the most relevant threats, understand how the current security stack addresses them, and improve the overall cybersecurity posture. They remove the guesswork by showing whether deployed tools are effectively protecting the organization.

Tidal Cyber structures critical threat and defensive intelligence around the MITRE ATT&CK framework and prioritizes adversary TTPs using threat profiles. This helps clients understand their confidence in defending specific behaviors and pinpoint remaining gaps. Tidal Cyber's unique coverage maps calculate the risk reduction provided by an organization's existing tools and their overall defensive confidence—empowering teams to save time and money, maximize current investments, and focus on the threats that matter most.

Palo Alto Networks Cortex XDR

Palo Alto Networks Cortex XDR® is an extended detection and response platform that empowers organizations to stop sophisticated attacks across endpoints, networks, cloud, and identities. By unifying data and applying AI-driven analytics, Cortex XDR delivers high-fidelity alerts, automates investigations, and accelerates response times—helping security teams reduce alert fatigue, lower mean time to respond (MTTR), and gain comprehensive visibility into threats. It streamlines operations by consolidating multiple tools into a single solution, reducing complexity and operational overhead.

Palo Alto Networks and Tidal Cyber

Palo Alto Networks and Tidal Cyber deliver an integrated solution that empowers joint customers with visibility into MITRE ATT&CK risk, defense configuration assessments, and recommendations to increase operational efficiency. By integrating Palo Alto Networks Cortex XDR into the Tidal Cyber Product Registry, organizations can leverage a unified platform to optimize their threat-informed defense strategies and maximize the value of their cybersecurity investments.

Use Case 1: Defensive Stack Optimization

Challenge

Organizations aren't confident that they're leveraging their existing capabilities. Fully understanding the true capabilities of their entire security stack and keeping track of every tool configuration is time-consuming and intensive, leading to critical blind spots.

Vendors feel their customers aren't configuring their solutions optimally. Without the data to justify these security investments, organizations risk overspending on unnecessary tools or underinvesting in critical areas, all while still leaving vulnerabilities undefended.

Solution

Tidal Cyber brings transparency and efficiency to managing the security stack, helping organizations understand how their tools defend against adversary behaviors as configured—and how to use them more effectively. By automating defensive stack optimization and aligning resources with real threats, Tidal Cyber enables teams to maximize tool value, reduce redundancies, and close gaps. Data-driven recommendations help teams do more with less by refining configurations or guiding smart investments, while clearly identifying each tool's unique value, overlaps, and areas lacking coverage.

Use Case 2: Threat Assessments

Challenge

Managing threat intelligence at scale is challenging. Fragmented sources and high data volumes make it hard to identify and prioritize relevant threats. Mapping to frameworks like MITRE ATT&CK is resource-intensive, and sifting through constant updates to find urgent threats is time-consuming and prone to error.

Solution

With the Tidal Cyber Confidence Score, Tidal Cyber provides security teams with an index to define how well security solutions defend against the latest threat information and as both defenses and threats evolve, continually reassesses coverage.

This streamlines and enhances threat intelligence management at scale by automating the collection, evaluation, and mapping of open-source, third-party, and reported threat data into a unified platform. It helps to ensure a continually updated view of threats, including emerging TTPs—allowing organizations to stay ahead of quickly evolving adversaries and reduce exposure to critical threats through actionable and targeted efforts.

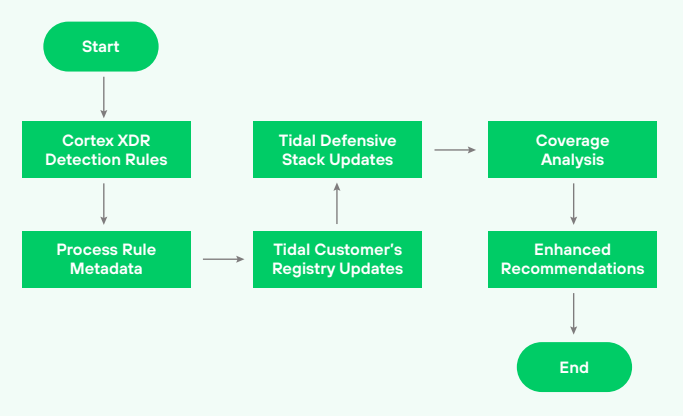

Figure 1. Capabilities workflow: Pulls detection rules, updates product registry, and synchronizes defensive stacks in the Tidal Cyber platform

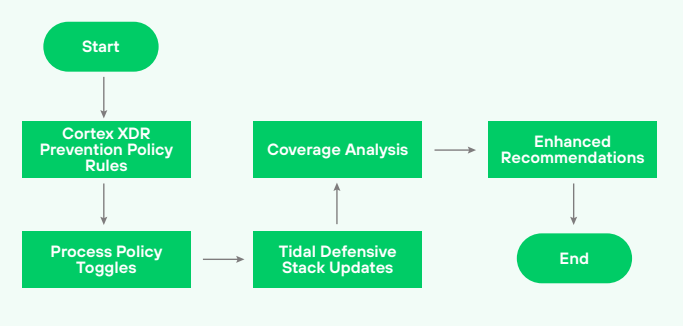

Figure 2. Configuration: Pulls prevention policy rules and synchronizes defensive stacks in the Tidal Cyber platform

About Tidal Cyber

Tidal Cyber empowers organizations to adopt threat-informed defense strategies by leveraging the MITRE ATT&CK framework. Through its innovative platform, Tidal Cyber simplifies the complex process of assessing, configuring, and optimizing security tools, enabling organizations to stay ahead of evolving threats. By integrating threat intelligence and defensive capabilities, Tidal Cyber helps ensure organizations maximize their security investments. For more information, visit https://www.tidalcyber.com.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Discover more at www.paloaltonetworks.com.

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

parent_pb_tidal-cyber_050725