PALO ALTO NETWORKS AND ATTACKIQ PLATFORM

Continuous Security Validation for Panorama

Benefits of the Integration

- Ensure Palo Alto Networks Next-Generation Firewalls are configured correctly and detecting threats.
- Run continuous assessments that emulate real attacker behavior against your network to help you determine where to prioritize investigation efforts.
- Correlate events in Panorama to the attack simulation in AttackIQ's API-first dashboard.

The Challenge

Your network security controls are a powerful layer of defense against unwanted attacker behavior. However, your controls are only as effective as you've configured the policies to be. Ensuring best practice policy configuration and enforcement has traditionally been difficult to verify and measure, leaving your infrastructure vulnerable to unknown risk.

With AttackIQ®, you can ensure and validate the efficacy of Palo Alto Networks Next-Generation Firewalls and Panorama™, which provides network security management, by testing them against real adversary behavior. Results from AttackIQ will help you determine how to optimize the configuration of your Palo Alto Networks products.

AttackIQ Platform

Even with the number of security controls in the enterprise growing rapidly, there hasn't been an automated way to test the efficacy of these controls. To get the most out of your security investment, you need the ability to continuously measure and validate that your controls are working as expected, catching the latest attacker tactics, techniques, and procedures (TTPs). AttackIQ provides a powerful platform for attack emulation in a production environment without impacting your operations.

Palo Alto Networks

The Palo Alto Networks Security Operating Platform® prevents successful cyberattacks through intelligent automation. It combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle.

Palo Alto Networks and AttackIQ

Palo Alto Networks and AttackIQ have integrated to provide confidence via verifiable evidence in your enterprise network security controls. Palo Alto Networks Next-Generation Firewalls capture rich user and application context to enable granular control of applications and prevention of advanced threats. AttackIQ emulates adversarial behavior against Palo Alto Networks Next-Generation Firewalls, rolling it up into Panorama. Based on testing results, your security analysts can determine how best to address any detection gaps or misconfigurations. AttackIQ extends the industry-leading capabilities of Palo Alto Networks Next-Generation Firewalls and Panorama by delivering powerful reports and dashboards that help security teams get the most out of their investments. Combining Palo Alto Networks with AttackIQ's award-winning Continuous Security Validation platform helps your organization efficiently comply with regulations, secure your network, and optimize the performance of your controls.

Use Case No. 1: Validate Correct Firewall Configuration

Challenge: Validate correct firewall configuration when using Panorama in a high availability configuration to manage multiple firewalls on your network.

Answer: AttackIQ enables you to validate the configuration of each firewall across multiple network segments by emulating adversarial behavior, exercising each firewall against an assumed configuration policy you set within Panorama. This ensures consistent enforcement of policies across your firewalls.

Use Case No. 2: Validate Application Policies

Challenge: Validate application policies when using Panorama to set specific application policies, such as SSH or RDP, for your network.

Answer: AttackIQ enables you to measure the efficacy of your current policies by emulating controlled application layer traffic through Panorama, exposing where you need to adjust specific configurations to fortify the acceptable use policies.

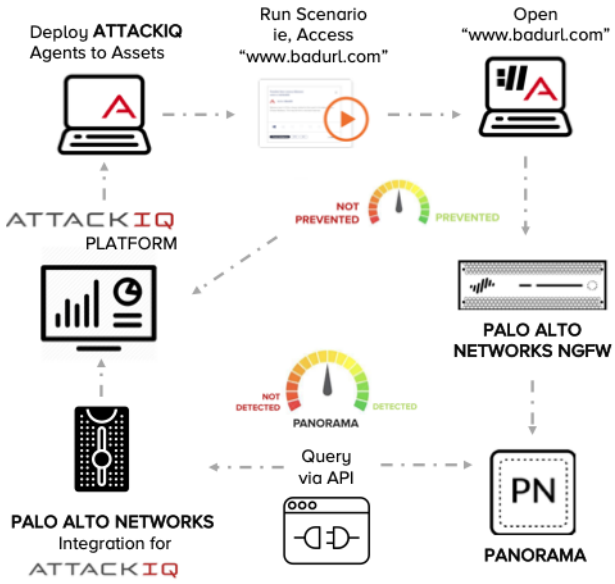

Figure 1: Palo Alto Networks and AttackIQ integration

Use Case No. 3: Map Defensive Capabilities to MITRE ATT&CK

Challenge: Validate prevention and detection capabilities against the MITRE ATT&CK™ framework when enabling specific security controls in Panorama to detect and prevent various adversarial behaviors.

Answer: AttackIQ emulates—in a safe, controlled manner—adversarial behavior to exercise, validate, and measure your network security controls. AttackIQ has fully operationalized the MITRE ATT&CK framework, enabling you to select and run specific assessments to exercise your network security controls and provide efficacy metrics for prevention and detection against specific adversarial TTPs and attacker groups.

Use Case No. 4: Improve Security Analyst Response Time

Challenge: Improve security analyst response times with mock adversarial training exercises to make use of the visibility tools—such as incident notifications, threat logs, WildFire® logs, and data filtering logs on Panorama—that can help with incident response.

Answer: AttackIQ can run specific techniques from the MITRE ATT&CK framework to exercise specific controls within Panorama. This helps your security analysts fully understand all components and features available so that once a real incident occurs, they can be prepared and respond quickly.

About AttackIQ

AttackIQ is the leader in continuous security validation and has built the first platform that enables organizations to measure and validate the effectiveness of their security program.

Leveraging the MITRE ATT&CK framework, AttackIQ provides organizations with evidence to prove current capabilities and also determine the highest probability risk exposures and gaps in their defensive strategy. Empowered by data, organizations can now make data-driven decisions to minimize the risk to their business.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

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

palo-alto-networks-and-attackiq-tpb-072419