ATTACKIQ®

Datasheet

Network Control Validation

Network Control Validation

AttackIQ®'s Informed Defense Architecture (AIDA) is the only architecture on the market built to test machine learning (ML) and artificial intelligence (AI)-based cyberdefense technologies using a multi-stage, comprehensive adversary emulation platform. The Network Control Validation module adds to AIDA by testing ML- and AI-based network security controls in-line.

AttackIQ has updated its architecture and capabilities to help our customers better validate their security effectiveness against multi-stage, comprehensive adversary attacks. This innovation accounts for a significant evolution in security technologies. In recent years, the cybersecurity industry's adoption of machine learning (ML)- and artificial intelligence (AI)-enabled defense capabilities has improved the world's security posture against advanced persistent threats. Yet one should never assume that the best technologies, the best personnel, and the best processes will always perform as intended. Even the most advanced cyberdefense capabilities need to be constantly tested and validated to ensure effectiveness. In order to do so, automated security validation platforms need to keep pace with both adversary attack patterns and advanced cybersecurity technologies.

On this basis, AttackIQ has launched its Network Control Validation Module to help customers better validate their advanced security technologies. The Network Control Validation Module supports end-to-end validation of network-deployed security controls and gives technology-specific remediation guidance, ensuring that customers get the most out of their cyberdefense investments. No matter the defense technology type — including those based on complex, behavioral models — AttackIQ provides unique insights into the state of a customer's total security program from network to endpoint, on-premises or in the cloud. And it does so with industry-leading ease of use.

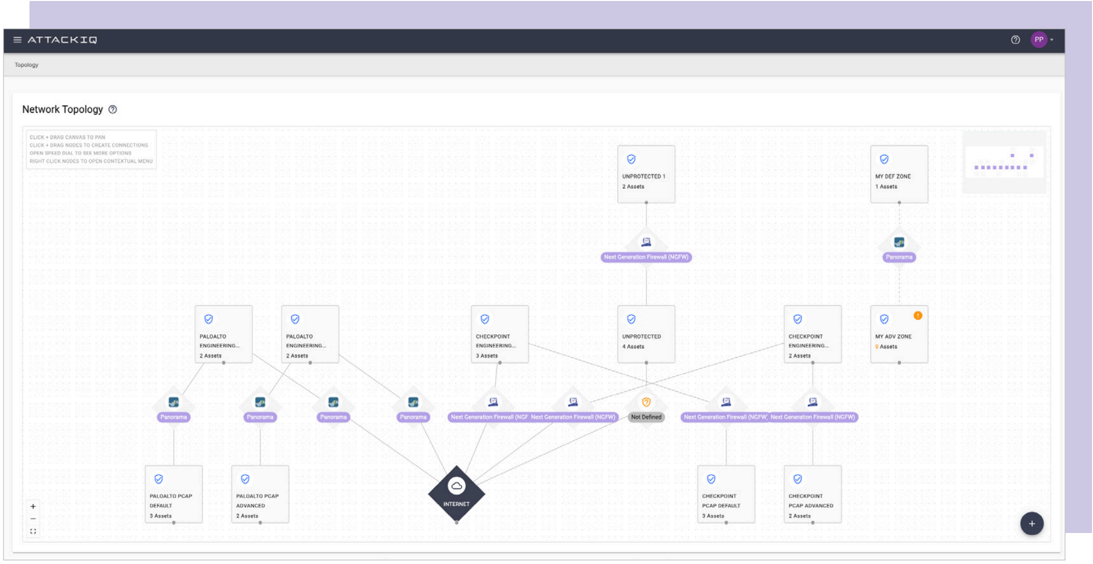
PRODUCT FEATURES

- Evaluates network security controls using in-line PCAP reply.
- Allows users to tailor testing to critical and non-critical assets, and security zones.
- Produces clear reports on effectiveness.
- Creates mitigation recommendations.
- Works on-premises and in SaaS environments.

How Does the Network Control Validation Module Do This?

Using already-deployed AttackIQ test points on the network, AttackIQ's Network Control Validation module evaluates the performance of network-deployed security controls with prescriptive guidance to maximize customers' investments in next-generation firewalls (NGFW) and similar technologies. The Network Control Validation module allows customers to replay traffic using packet capture (PCAP) reply between an attacking asset and target asset to determine whether the in-line security controls detect and prevent the attack. It then provides clear mitigation recommendation options for customers to improve their security posture.

How Does the Network Control Validation Module Do This? (cont.)



CLICK + DRAG CANVAS TO PAN
CLICK + DRAG NODES TO CREATE CONNECTIONS
OPEN SPEED DIAL TO SEE MORE OPTIONS
RIGHT CLICK NODES TO OPEN CONTEXTUAL MENU

Figure 1: NCV Topology Screenshot

ATTACKIQ

Network Executive Report

REPORT:
EXEC REPORT

ASSESSMENT:
PALO ALTO DEFAULT SECURITY PROFILES HEALTH CHECK

Report Generated on
03-04-21 11:15am

Report Generated by:
username: Paula Pedret
email: paula.pedret@attackiq.com

ATTACKIQ

EXECUTIVE SUMMARY

Assessment: Palo Alto Default Security Profiles Health Check

EXECUTIVE SUMMARY

This is a report containing a summary of the results from an assessment.

The NCV generates remediation reports about detection and prevention assessments

Better Insights, Better Decisions, Real Security Outcomes

Customers who use next-generation firewalls and other AI- and ML-based defense technologies can operate with increased confidence in their program effectiveness, knowing that they are testing their most advanced cyberdefenses against comprehensive and multi-stage adversary emulations. The outcome is an increase in defense capability and performance.

ATTACKIQ®

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.