Fortinet and Picus Security Integrated Security Solution

Broad, integrated and automated solution for next-generation prevention with threat simulation and mitigation

Organizations are increasingly at risk from nation-state sponsors, cyber gang groups, local insiders and malicious software. Security Operations teams are under increasing pressure to defend their organizations. Cyber criminal actions and knowledge gap between attackers and defenders are mandating fundamental changes to cybersecurity products. Moreover, building an effective detection capability is not straightforward. Selecting the right technology for effective detection requires real-world experience and knowledge of attacker tools, tactics, and procedures, all of which are continuously evolving according to different attacker objectives and levels of sophistication.

Challenges continue evolving on a daily basis. SecOps teams lack the agility of responding by updating deployed security controls against ever-growing cybersecurity challenges. Therefore, SecOps teams are looking for solutions that provide full cyber-threat readiness visibility and control across their entire network, across endpoints as well as their cloud, and virtualized infrastructures with an objective of maintaining business continuity at all times.

The Picus and Fortinet partnership addresses the above-mentioned challenges by assisting every SecOps decision with real and actionable insight, enabling the Fortinet customers with increased efficiency and potential of their advanced Fortinet Technology. Backing decisions with fact based consistent results improves Fortinet customers' risk-based decision-making process and ensures cyber resiliency.

Joint Solution Benefits

- Faster identification and mitigation of security gaps
- Increased effectiveness of network security policies with continuous assessment of deployed security configuration against the attack library
- Validate defense-in-depth architecture with possible defensive countermeasures
- Maximized security posture with prioritized mitigation actions
- Increased cognition of real-world activities through the empirical use of examples
- 6300+ threats tested as of January 2019, including APT Campaigns, Exploit Kits, Vulnerability Exploitation, Web and Endpoint threats

The Joint Solution Description

The Picus and Fortinet partnership brings together cutting-edge technologies for the continuous automation of detection and identification of unaddressed cyber-threats, misconfigurations, and errors. Without continuous testing, errors and deficiencies may go unnoticed for a long time, or worse, be discovered by real attackers during a real incident. Continuous oversight of the deployed Security Controls and consistent identification of security gaps help the security teams to prioritize events and mitigate risks.

Picus Security offers an automated security control gap validation and migration solution that provides provide continuously automated security posture analysis for security teams and managers to successfully identify, prevent, detect and respond to process or technology failures by:

- Continuous oversight of the security readiness of the business and IT Controls
- Identifying the scenarios of risk for organization
- Gaining visibility of the IT Controls and setting metrics for cyber-threat readiness

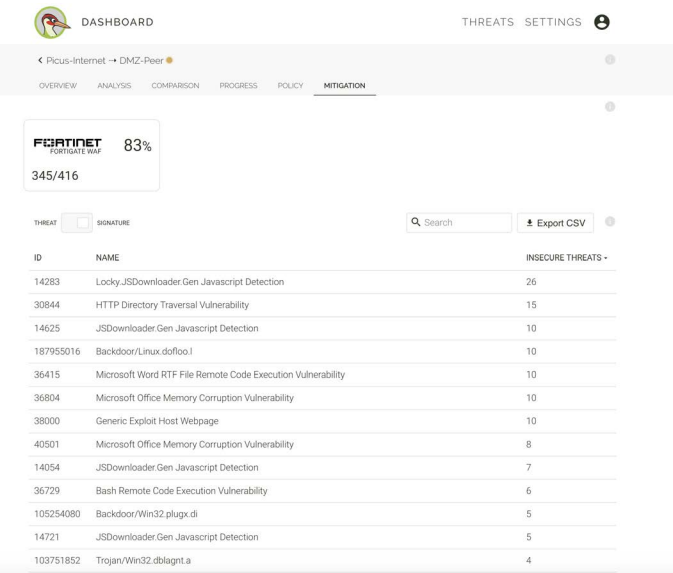
Picus Lab adds emerging cyber-threats in its database on a daily basis. These attack simulations are played against Fortinet's NGFW to list matching signatures. During the continuous assessment process, whenever an attack in the Picus Threat Database is not blocked by the firewall, a notification on the corresponding signature is shared with the SecOps teams.

Picus can also group cyber-threats related to each signature and indicate the number of cyber-threats that can be stopped by each signature. This provides the security operations teams with the options to mitigate from the most comprehensive or most specific cyber-attack and signature set while mitigating the threats on their systems.

The Continuous Security Validation & Mitigation approach by Picus and Fortinet empowers SecOps teams with measuring cyber-threat readiness in real-time, identifying security gaps before hackers do and mitigating actions instantaneously. By automating this process, mitigation time is shortened to minutes than weeks or months. Picus's Continuous Security Validation as an integrated part of the SecOps process enhances and optimizes Fortinet's NGFW defensive policies.

The functionality of the joint solution is summarized in the illustration below.

Diagram of Joint Solution



Fortinet FortiGate WAF threat mitigation on the Picus UI

FortiGate Enterprise Firewall

FortiGate enterprise firewalls offer flexible deployments from the network edge to the core, data center, internal segment, and the Cloud. FortiGate enterprise firewalls leverages purpose-built security processors (SPUs) that delivers scalable performance of advanced security services like Threat Protection, SSL inspection, and ultra-low latency for protecting internal segments and mission critical environments.

FortiGate NGFW provides automated visibility into cloud applications, IoT devices and automatically discovers end to end topology view of the enterprise network. FortiGate is a core part of security fabric and validated security protect the enterprise network from known and unknown attacks.

Picus Security Technology

To support the efforts of enterprises in coping with today's cybersecurity challenges, Picus Security's innovative technology automates the security control gap identification and mitigation processes. Contrary to ongoing security practices, which are focused on vulnerabilities and depend on point-in-time assessments, Picus solution helps enterprises measure their cyber threat readiness on a 24/7 basis and apply fast mitigation actions to security controls.

Once deployed in production networks, Picus virtual agents start mimicking both the attacker and the victim, running cyber-threat scenarios with each other and challenging security defenses, as if real attacks are occurring.

Picus Labs add new cyber threat samples every day to ensure defense infrastructures of customers are continually validated against new threats. These threats do not affect users or corporate assets.

The key advantages of using Picus are:

- Real-time measurement of security posture with actionable risk metrics
- Increased return on investment and utilization of security investment
- Better cyberattack preparation for your "agile SecOps

About Picus Security Inc.

Picus Security offers Continuous Security Validation and Mitigation as the most proactive approach to ensure cyber-resilience. The Picus Platform measures the effectiveness of defenses by using emerging threat samples in production environments, providing the insight required to build the right security strategy to better manage complex operations.

Find out more at www.picussecurity.com

February 6, 2019 9:14 PM

123456-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray