PICUS SECURITY

PARTNERSHIP OVERVIEW

Dynamically identify and mitigate security threats targeting your applications

Key Benefits

• Identify possible hacking exposures as they occur and continually measure cyber-threat readiness.

• Take mitigation actions as soon as an exposure is identified.

• Continually and better utilise F5 BIG-IP WAF infrastructure.

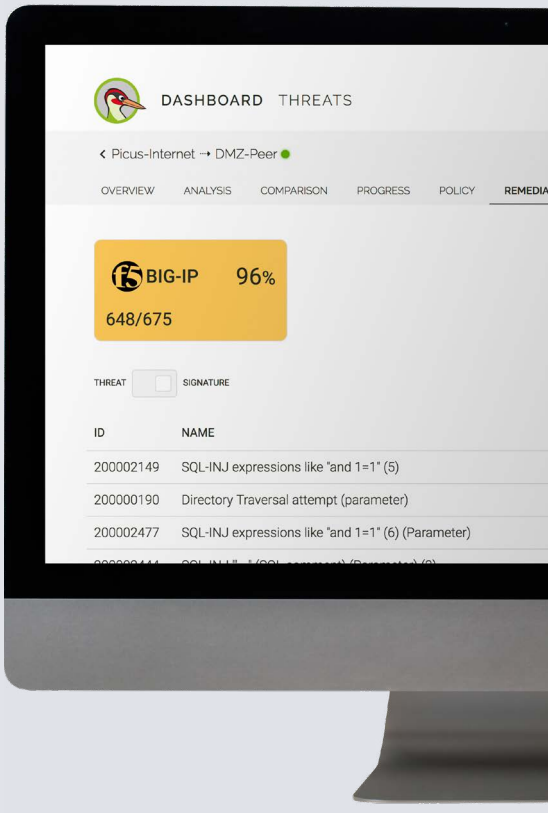

Figure 1: F5 WAF threat remediation on the Picus UI.

Web applications represent the business in today's economy and the need for rapid development shadow the cyber-security concerns. Web Application Firewalls (WAF) are one of the most efficient means to protect these applications. Fast changing attack surface and potential vulnerabilities in applications requires effective policies to be set and maintained on WAF's continuously, without causing any interruption on business. Picus Security's participation in the F5 technology alliance program aims at providing the insight and configuration recommendations to WAF admins and security managers to address this challenge.

F5 & Picus Security Interoperability

Breach and attack simulation platform of Picus Security helps enterprises measure their cyber-threat readiness continuously and apply fast fixes for the potential hacking exposures identified on security controls.

Unlike web application scanners, Picus run cyber-attacks among its software components, simulate both the victim and attacker systems in production networks. This enables efficacy assessment for F5 BIG-IP ASM configuration continuously, without harming any business applications. Using the insight of continual assessment, security teams pinpoint configuration change needs instantaneously. Picus reports help security managers to track effectiveness of their operations and their readiness to web application attacks.

Picus assessments not only help SecOps teams to identify configuration related issues, but also provide corresponding F5 signature name and ID to block missed attacks. Furthermore, category information (for example evasion based XSS attacks, header-based SQL injection, etc.) provided with the missed attack allows F5 admins to generate the required F5 ASM policies.

Picus also groups the cyber-threats related to each signature and shows how many cyber-threats would be stopped by each signature. This approach helps security operations teams to start remediating from the most comprehensive or most specific cyber-attack and signature set as per their needs.

About F5

F5 (NASDAQ: FFIV) makes apps go faster, smarter, and safer for the world's largest businesses, service providers, governments, and consumer brands. F5 delivers cloud and security solutions that enable organizations to embrace the application infrastructure they choose without sacrificing speed and control.

For more go to **f5.com**

About Picus Secuity

Picus Security offer "Continuous Security Validation" as the most realistic approach for ensuring and improving enterprise cyber-resilience. Picus assessments, independent from any vendor or technology, measure effectiveness of security defenses continuously using emerging threat samples in production environments. Picus assessments provide the required practical insight to better manage these complex technologies without any effect to running systems.

For more go to **picussecurity.com**

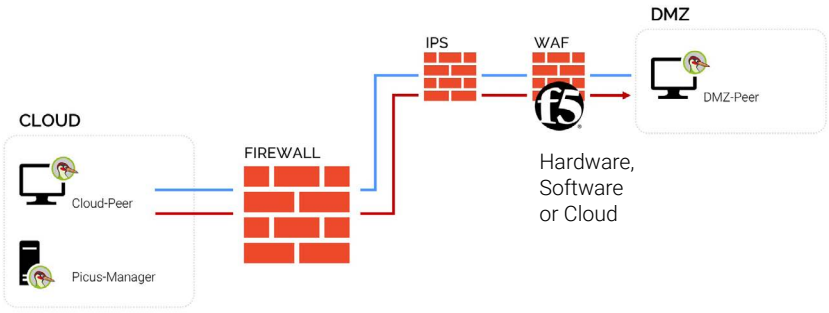

Figure 2: F5 WAF in Picus network topology

Picus Security and Web Application Attacks

Picus Threat Database contains web application threats from 18 main categories and 78 sub-categories. Both traditional attack types such as Injection, XSS, Directory Traversal, File Inclusion, Protocol Anomaly and emerging web application attack categories such as API attacks are included.

Picus Security Labs continuously tracks new attack categories and also new variants of traditional attack types. Therefore, injection attacks are not only limited to old-school SQL Injection, Command Injection and Code Injection attacks, but also includes new type of injection attacks such as XML, CSV, LDAP, SSI, SSJS, SST, NoSQL injection attacks. In order to test the resiliency of application security controls against evasion techniques, Picus Threat Database includes obfuscated attack payloads also. The database also includes application specific exploitation attacks, such as Apache Struts Remote Code Execution attacks.

A web application attack in Picus Threat Database is referenced by OWASP Top 10 2013/2017 and CWE (Common Weakness Enumeration) number. Picus Threat Database includes attacks for all OWASP Top 10 2013 and 2017 categories and main CWE categories.

Picus Security
180 Sansome St, 2nd Floor,
San Francisco, CA 94104 USA
info@picussecurity.com