Proven Success Protecting Web Applications

SANGFOR

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Scanning Process

Prevents port/server scanning
Prevents app vulnerability scanning
Weak password protection
Anti-brute force attack
Core URL protection
Website structure anti-scanning
Web Crawler defense

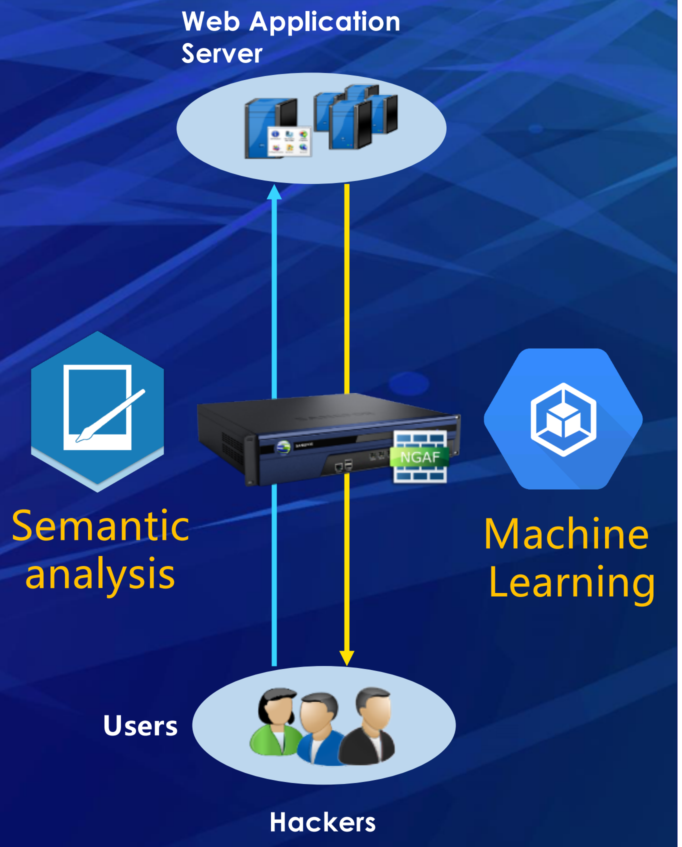
Attack Process

Enhanced Web Defense
- SQL injection defense
- OS command injection defense
- XSS attack & CSRF attack

IPS Application Based
- Server vulnerability defense
- Terminal vulnerability defense

Theft Process

DOS attack
Application layer DOS attack
CC attack
Authority control
Exe file upload filtering
Upload viruses & Trojan filtering
Prevention of web shell dataflow


Web Application Server
NGAF
Semantic analysis
Machine Learning
Users
Hackers