From the Bottom to the Top: The Evolution of Application Monitoring

Narayan Makaram, CISSP
Director, Security Solutions
HP/Enterprise Security Business Unit

Session ID: SP01-202
Session Classification: Intermediate
Your Headline Here (in Title Caps)

- Your talking point bullet text here
- Your next talking point bullet text here
- Third talking point, etc.
  - Bullet can be indented by pressing the Tab key
    - Third-level bullet created by pressing Tab key again
- Reverse indents with Shift + Tab keys
Application Security
Business Problem
Application Security - A Real Challenge!

- Companies focused on speed of doing business and ease-of-access
- Developers focused on application functionality more than security
- Web protocol (HTTP) is inherently not secure – security is bolted on
- IT Infrastructure security measures not enough to secure applications

Cost of lost business due to breach can range from $1M to $52M per year per company. Median cost - $3.8 million/year. (source: Ponemon Report 2010)
Application Vulnerabilities Easily Exploited

OWASP Top-10

A1 – SQL Injection
A2 – Cross-Site Scripting (XSS)
A3 – Broken Authen. And Session Mgmt.
A4 – Insecure Direct Object References
A5 – Cross-Site Registry Forgery
A6 – Security Misconfiguration
A7 – Insecure Cryptographic Storage
A8 – Failure to Restrict URL Access
A9 – Insufficient Transport Layer Protection
A10 – Unvalidated Redirects and Forwards
Focus shifts to User & Application Access
With Cloud Adoption and Consumerization of IT

- IaaS → PaaS → SaaS

- Increasing security responsibilities at the information, application, and user layers
- Reducing visibility into O/S, Network, and Physical layers
Best Practices for Application Security

- Adopt Secure software development life cycle (SDLC)
  - Follow secure coding practices and conduct security code reviews
  - Perform static code analysis and dynamic web scanning tests
- Build-in application level logging
  - Embed security logging capability within applications
  - Capture security and application transactional information in the logs
- Correlate application events with SIEM
  - Correlate in real-time across network, system, and applications
  - More accurately identify business risks closer to application transactions
Why best practices are NOT followed?

- Adopt secure software development life cycle (SDLC)
  - Slow Adoption: It takes years to train developers/testers to build in security
  - 3rd Party Code: Cannot impose SDLC practices on 3rd parties and SAAS providers

- Build-in application level logging
  - Developers accustomed to logging functional use-cases not abuse-cases
  - Developers collect too little information in logs – not usable to assess business risk

- Correlate application events with SIEM
  - Many sophisticated attacks cannot be detected by monitoring individual applications
  - Need to correlate across multiple applications, firewalls, IPS/IDS and other sources
HP Enterprise Security
Strategy for Applications
Establish complete Visibility across all applications and systems

Analyze vulnerabilities in applications and operations to understand risk

Respond adaptively to build defenses against the exploitation of vulnerabilities

Measure security effectiveness and risk across people, process, and technology to improve over time

Intelligence integration of security and IT operations technologies
Business Risk Management Strategy
Using Security Intelligence Platform

(1) Unify the security layers

Security
- Users
- Applications
- Data
- Systems
- Networks

(2) Integrate Security & IT management

Business
Risk management & compliance

(3) Rollup to security intelligence

IT
- Users
- Applications
- Data
- Systems
- Networks

Mobile
Virtual
Cloud
(1) Unify the security layers

Provides Situational Awareness

Traditional Security Monitoring

Hybrid Security Monitoring
User and Application Risk Monitoring

- Top Blocked Departments
- Top URLS Accessed
- Top Users Accessing Applications
- Top Bandwidth by Identity
- Top Apps Attacked
- Top Application Attack Types
(2) Integrate Security and IT Management

Remove Blind Spots between Operations Silos
(3) Pro-Active Business Risk Management

Are We Secure at Risk?

Business Risk Centric Views:
- Heat maps - real-time analysis
- Long-term trending
HP Enterprise Security Solutions for Applications
HP Application Security Solutions

Secure Software Development

Design → Code → Test → Staging

Static Code Analyzer → Application Security Monitor → Adaptive WAF

Applications Run-time

SIEM Platform

Network Devices → Email/Web Gateways → Identity Mgmt. Systems → Physical Access

Endpoints Servers → Databases

Operations

End-to-End Visibility
HP Fortify Static Code Analyzer (SCA)

Securing your application code in development

Features:
- Automate static application security testing to identify security vulnerabilities in application source code during development
- Pinpoint the root cause of vulnerabilities with line of code details and remediation guidance
- Prioritize all application vulnerabilities by severity and importance

Benefits:
- Reduces the cost of identifying and fixing vulnerabilities
- Reduces risk that a vulnerability will slip by and cause a problem later
- Saves valuable development time and effort

Problem it solves:
Identifies all risks in the source code for applications in development
HP Adaptive Web Application Firewall (WAF)

TippingPoint IPS and WebInspect

Problem it solves:
- Protects web-application with residual vulnerabilities using IPS signatures customized from results of penetration testing web-applications

What it is:
- Advanced web application scanning to uncover vulnerabilities combined with adaptive IPS response
- WebInspect information passed to WebAppDV to generate IPS filters for virtual vulnerability patch

Benefits:
- Protection for custom and commercial web applications
- Inspection of encrypted and non-encrypted traffic (ideal for web commerce apps)
- Elimination of tuning required by legacy WAFs
HP ArcSight Application Security Monitor (AppSM)

What it is?
- Monitors multiple applications without additional instrumentation
- Detects standard security threats from inside the applications during run-time
- Identifies those application threats that pose overall business risk

Benefits:
- Rapid time to deploy – no custom coding of applications required to collect logs
- Prioritized business risks with real time correlation across network, system and applications
- Streamlines regulatory compliance needs (e.g. PCI-DSS req. 6) for maintaining security of applications

Problem it Solves:
Identifies security threats in applications that pose business risk and impact compliance during run-time
HP ArcSight Application Security Monitor (AppSM)

- AppSM Runtime: AppSM rules pre-configured to detect “standard” security threats, security related session data, and forward them to ArcSight ESM
- AppSM Content: ArcSight ESM Correlation Rules, Dashboard and Reports for viewing standard threats in applications
HP ArcSight AppSM Dashboard

Top Applications Attacked

Attacks from Internal Systems

Attacks from External Systems

Attacks detected from “other” sources

Top Application Attack Types
How to Apply What You Have Learned Today

- **Long Term: Adopt secure software development life cycle**
  - Train software developers/testers to build in security during SDLC
  - Use tools to identify security risks early during software development

- **Medium Term: Build-in application level logging**
  - Embed security and app. transactional information in the logs as far as possible
  - Use tools that automatically detect app. level threats without modifying applications

- **Short Term: Deploy applications with counter measures to handle residual risks!**
  - Correlate application threats with enterprise wide activity using SIEM
  - Proactively adapt your IPS to handle application level threats
Visit HP Enterprise Security booth #1717 to see our application security solutions in action.

Thank You