Understanding Application Risk Management

Syed Abdur, Director of Product Management, Brinqa
Application Risk Management

Knowledge-driven, risk-centric discipline that activates an organization’s existing investments in application testing and monitoring tools (SAST, DAST, FOSS, Pentest) by enhancing their results with other relevant data sources (Asset Management, Threat Intel, ITSM) with the goal of identifying and remediating the most critical risks in an organization’s software infrastructure.
Agenda

• Need & Scope
• Challenges
• Process
• Case Study
• Technical Capabilities
• Data Sources (Integrations)
PART 1

Need for better Application Risk Management
Breaches per pattern

Web Applications: 414
Miscellaneous Errors: 347
Point of Sale: 324
Everything Else: 308
Privilege Misuse: 276
Cyber-Espionage: 171
Lost and Stolen Assets: 145
Crimeware: 140
Payment Card Skimmers: 111
Denial of Service: 0

Source: Verizon DBIR 2018
http://www.verizonenterprise.com/resources/dbir
Since the 2014 report, a series of nine patterns have been used to categorize security incidents and data breaches that share similar characteristics. This was done in an effort to communicate that the majority of incidents/breaches, even targeted, sophisticated attacks, generally share enough commonalities to categorize them, and study how often each pattern is found in a particular industry's dataset. This year, 94% of security incidents and 90% of data breaches continue to find a home within one of the original nine patterns.
Pattern Web Applications

Incidents Across All Patterns

Show
- Breaches only
- All incidents

Measure
- Ratio
- Value

This line chart shows how the breaches in Web Applications compare to the other patterns over time.

Source: Verizon DBIR Interactive Tool
http://www.verizonenterprise.com/verizon-insights-lab/dbir/tool/
Since the 2014 report, a series of nine patterns have been used to categorize security incidents and data breaches that share similar characteristics. This was done in an effort to communicate that the majority of incidents/breaches, even targeted, sophisticated attacks, generally share enough commonalities to categorize them, and study how often each pattern is found in a particular industry’s dataset. This year, 94% of security incidents and 90% of data breaches continue to find a home within one of the original nine patterns.
Understanding the relationship between patterns and industries is a cheat-sheet for how to plan what to protect in your organization. If you know the most likely doors attackers will use to access your defenses, then you also know where to put the most locks. While all basic security controls must be addressed, this inside knowledge allows you to place priority for resource allocation on the areas where your organization needs it most.
Application Risk Management Scope

- Web Applications / Desktop Applications
- Internally Developed / Third Party
- Open Source / COTS / Custom
- Business Applications
- Enterprise Software
- Web Services / APIs
PART 2

Common Challenges
Common Operational Challenges

• Data overload
• Changing technology ecosystems
• Changing attacker landscape
• Lack of business context
• Lack of security intelligence
• Manual processes & Operations model
Common Programmatic Challenges

- Scanning performance & accuracy, false detections, and verification
- Poor asset management
- Lack of objective RACI model
- Remediation is always time-consuming, availability comes first
- Lack of contextual risk-based prioritization
- C-Level or board do not relate with technical program metrics
PART 3

Application Risk Management Process
Collect, normalize, and **analyze** all of your application asset and vulnerability data into one integrated platform.

Contextualize and **prioritize** by enriching vulnerability information through business context and threat intelligence feeds, and adjust weighting based on your organization’s needs.

**Remediate** through automated rule-based ITSM integration, reduce volume with powerful consolidation features and increase efficiency.

Report out on your program stakeholders with targeted reports and dashboards, presenting metrics that matter to your executives. **Learn** from risk insights and **adapt** to improve software provisioning and development processes.
Analyze: Data Ontology
Prioritize: Critical Questions of Risk

1. Which vulnerabilities, if exploited, pose the greatest risk of disrupting critical business functions?

2. Which vulnerabilities, if exploited, pose the greatest risk of exposing vital or confidential data?

3. Which vulnerabilities stand the greatest risk of being exploited?
### Prioritize: Context

<table>
<thead>
<tr>
<th>Application Information</th>
<th>Application Details</th>
<th>Ownership Information</th>
<th>Application Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Status</td>
<td>COTS</td>
<td>Owner</td>
<td>Criticality</td>
</tr>
<tr>
<td>Description</td>
<td>Yes</td>
<td>James Waltz</td>
<td>Mission Critical</td>
</tr>
<tr>
<td>Is Web App</td>
<td>Yes</td>
<td>Security Analyst</td>
<td>Public</td>
</tr>
<tr>
<td>PCI</td>
<td>Yes</td>
<td>Informed Users</td>
<td>Medium</td>
</tr>
<tr>
<td>PII</td>
<td>No</td>
<td>Business Unit</td>
<td>Critical</td>
</tr>
<tr>
<td>Development Team</td>
<td></td>
<td>Payment Capture Team</td>
<td>High</td>
</tr>
</tbody>
</table>

**Operational Status**: Operational

**Description**: Web app used for demos.

**Is Public**: Yes

**Is Verified**: True

**License Type**: Subscription
Remediate: Steps

1. Target Critical Vulnerabilities
2. Associate Ownership and SLAs
3. Validate Closed Loop Remediation
4. Consolidate Vulnerabilities
5. Integrate ITSM Tools & Processes
6. Measure & Communicate Remediation Effectiveness

bringqa
Learn & Adapt: Program Performance

Top 10 Application Security Risks
- Cross-Site Scripting: 429
- Cross-Site Scripting: 376
- Code Quality: 235
- Insufficient Input Validation: 210
- CRFL Injection: 200
- Information Leakage: 56
- Directory Traversal: 55
- SQL Injection: 71
- Error Handling: 38
- Encryption: 35

Window Of Exposure
- Cross-Site Scripting: 516
- Cross-Site Scripting: 397
- Cryptographic Issues: 444
- Cryptographic Issues: 396
- Code Quality: 493
- Insufficient Input Validation: 493
- CRFL Injection: 607
- Information Leakage: 495
- Directory Traversal: 367
- SQL Injection: 377
- Error Handling: 409
- Encryption: 35

0 Issues in last 30 days
429 Cross-site scripting issues
Cross-Site Scripting: Most Common Issue
ID DB - USA: Highest Risk Application
eFiles DB: Most exposed application
Learn & Adapt: Risk Ownership

Static Issue Count by Owner

Static Issue Age by Application

Dynamic Finding Count by Owner

Dynamic Finding Age by Application

Average Application Score

17 Application(s)

ID DB - USA
Most Critical Application

339 Day(s)
Most Recent Static Code Analysis

0 Day(s)
Most Recent Dynamic Code Analysis
PART 4

Case Study
Problem Statement

The customer wanted to ensure that applications that tie in to critical business functions are being assessed and prioritized for vulnerabilities effectively, and automated remediation actions are taken in compliance with internal and external SLA goals.

Data sources

- ServiceNow for business applications inventory
- JIRA for SDLC tracking
- Checkmarx static application testing
- Qualys web application scanning
- Penetration testing service
- Data protection program
- ServiceNow and JIRA both used for ticketing by different teams
- FireEye Threat Intelligence
- LDAP
Case Study: Fortune 500 Healthcare Firm

Benefits

• Identification of **critical applications** based on internal asset repository, business context and data lifecycle management.
• Automated user task creation to complete missing business context and ownership information through business rules.
• Evaluation of **vulnerability risk scores** based on severity, asset value, data context, threat intelligence as well business impact and compliance requirements.
• Drastic improvement in **remediation coverage** of critical applications through automated workflows and actions.
• Consistent ticket creation, ownership assignment, and SLA enforcement across multiple ITSM tools and remediation teams through automated rule-based ticket creation.
• Real-time **risk** and **performance reporting** and monitoring for critical business functions, services and assets.
PART 5

Necessary Technical Capabilities
Necessary Technical Capabilities

- Data Modeling
- Data Connector Framework
- Intelligence Engine
- Automation Engine
- Analytics Interface
Create an accurate representation of the technology and business environment, highlighting all entities that have an impact on or are impacted by cyber risk and delineating flow of information between them.

Desired Characteristics

- Accurate
- Comprehensive
- Future-proof
Data Connector Framework

Collect, normalize and collate information from different sources and organize data into a standard ontology.

Desired Characteristics

• Wide coverage

• High-performance

• Transformative
Intelligence Engine

Create new knowledge by automatically applying encoded logic to collected information.

Desired Characteristics

• Near Real-time
• Transparent
• Adaptive
Automation Engine

Automatically create, assign and track necessary user and machine tasks for knowledge-driven outcomes.

Desired Characteristics

• Consistent
• Interactive
• Documented
Analytics Interface

Communicate risk and performance metrics to all stakeholders to inform and engage them effectively.

**Desired Characteristics**

- Actionable
- Collaborative
- Self-service
PART 6

Relevant Data Sources
Relevant Data Sources

- Asset Management
- Application Testing (SAST, DAST)
- Open Source Vulnerabilities
- Penetration Testing
- Threat Intelligence
- ITSM
Asset Management Data Sources
Application Testing Data Sources

- Acunetix
- Burp Suite
- Checkmarx
- AppScan
- Micro Focus Fortify on Demand
- Micro Focus Fortify Static Code Analyzer
- Micro Focus Fortify Software Security Center
- Micro Focus Fortify WebInspect
- Netsparker Cloud
- Netsparker Desktop
- Qualys Web Application Scanning
- AppSpider
- Sonatype IQ Server
- Synopsys Black Duck
- Synopsys Coverity
- Veracode
- White Hat Security
Threat Intel Data Sources

- Accenture iDefense
- AlienVault USM Appliance
- BITSIGHT
- CrowdStrike
- Digital Shadows
- FireEye
- NVD
- Recorded Future
- Secureworks
ITSM Data Sources
Thank You!

Contact us at info@brinqa.com