Acunetix **Competitive Battlecard**

Product: Acunetix Premium v13

STRENGTHS

1. ### Comprehensive Application Security: DAST & DeepScan / IAST / Out-Of-Band / Network / Integrations:

Architected For Speed & Accuracy

- Multi-threaded, lightning fast crawler and scanner developed in C++ that can crawl hundreds of thousands of pages without interruptions.

DeepScan

- DeepScan Technology allows accurate crawling of AJAX-heavy client-side Single Page Applications (SPAs) that leverage complex technologies such as SOAP/ WDSL, SOAP/ WCF, WADL, XML, JSON, Google Web Toolkit (GWT) and CRUD operations. DeepScan also automatically detects Angular, React, and Vue, and optimizes crawling to these frameworks.

SmartScan

- SmartScan Technology prioritizes scanned pages and gives more priority to pages based on unique templates. This allows Acunetix to find approximately 80% of vulnerabilities in the first 20% of the scan.

Advanced Injection Engine

- Industry's most advanced and robust SQL Injection and Cross-site Scripting testing, including advanced detection of DOM-based Cross-site Scripting.

Incremental Scanning and Continuous Scanning

- Incremental scanning: You can configure Acunetix to scan only the web pages or elements that changed since the last scan.
- Continuous scanning: Web apps are constantly monitored for new vulnerabilities.

Login Sequence Recorder

- The LSR allows the automatic crawling and scanning of complex password protected areas including multi-step, Single Sign-On (SSO) and OAuth-based websites and can also integrate with Selenium to import existing scripts into the LSR.

Integrated AppSecurity (Grey Box) / IAST:

- AcuSensor improves the scan results with line of code visibility by being able to identify all the pages on your website, increases the information about the vulnerabilities detected and decreases false positives
- AcuSensor can identify vulnerabilities down to specific lines of code (for PHP applications), or provide detailed stack traces (for ASP.NET and Java applications). Furthermore, for discovered SQL Injection vulnerabilities, AcuSensor also provides a preview of SQL queries as they would have been run by the database.
- Since AcuSensor is designed to work on running applications, it does not need to be compiled-in, and can even work with signed code (signed JAR files in Java and strong-named assemblies in ASP.NET applications). This is a major advantage over IAST offerings that require you to compile sensors within your code, often requiring you to change your build process or add software dependencies to your project.

Detection of XXE, Blind XSS, SSRF, & Other Out-of-Band Vulnerabilities

- To detect out-of-band vulnerabilities, you need an intermediary service that the scanner has access to. Acunetix, combined with AcuMonitor, makes automatic detection of such vulnerabilities painless and transparent to the user running the scan.
- AcuMonitor can automatically detect the following vulnerabilities during a scan:
- Blind Server-side XML/SOAP Injection
- Blind XSS (also referred to as Delayed XSS)
- Host Header Attack
- Out-of-band Remote Code Execution (OOB RCE)
- Out-of-band SQL Injection (OOB SQLi)
- SMTP Header Injection
- Server-side Request Forgery (SSRF)
- XML External Entity Injection (XXE)

CMS Vulnerability Scanning

- Highest detection of WordPress vulnerabilities – scans for over *5000 known vulnerabilities in WordPress' core, themes and plugins.* We also scan for 186 vulnerabilities for Drupal and 216 for Joomla

Business Logic Testing with Selenium Integration

- Acunetix can leverage both Selenium IDE Test Cases as well as custom Selenium WebDriver scripts (regardless of the language-binding they are using).

Multiple Integrations and Imports/Exports

- Send vulnerabilities to supported Bug Tracking Systems:: Jira, GitLab, GitHub, Microsoft TFS, Mantis, Bugzilla, and Jenkins.
- Integrate Acunetix in SDLC with the Jenkins CI/CD integration plugin
- Web browser automation tools: Selenium
- Security testing proxies: Telerik Fiddler, Postman, Burp
- RESTful API definition languages: Swagger 2.0 and 3.0, and WADL
- SOAP API Definition Languages: WSDL
- ASP.NET Web Forms project files, HTTP archives (HAR), or simple text files with a list of URLs
- You can export Acunetix scan results to the following WAFs for temporary remediation before issues can be fixed:
- Imperva SecureSphere
- F5 BIG-IP Application Security Manager
- Fortinet FortiWeb

Network Scanning

- Test for over 50,000 known network vulnerabilities and misconfigurations
- Comprehensive security audits require a detailed inspection of the perimeter of your public-facing network assets. Acunetix Premium uses the popular OpenVAS scanner to provide a comprehensive perimeter network security scan engine that integrates seamlessly with your web application security testing. The network security scanner is directly available in Acunetix Online and automatically integrates with Acunetix for Windows and Acunetix for Linux.

Malware Scanning

- Automatically download scripts from scanned websites and web applications and test them for malware using Windows Defender (Windows, no configuration required) or ClamAV (Linux, installation

WEAKNESSES

Current product offering is not inclusive of SAST, RASP, or SCA capabilities.

Lackluster Industry Analyst (Gartner) Results

POSITIONING

Comprehensive Vulnerability Management Solution

- More than just another DAST -- SEE STRENGTHS SECTION
- More than just scan results:
  - Automatic triage (vulnerability assessment)
  - Internal vulnerability management functionality
  - External vulnerability management using issue trackers (Jira, GitHub, GitLab, Mantis, Bugzilla, Microsoft TFS)

Efficiency and Accuracy

- Engine tested to be one of the fastest if not the fastest in the industry and developed using a low-level language (C++)
- Focus on efficiency: minimizing the number of requests, prioritizing unique page templates
- Benchmarked to have very high detection rate and very low number of false positives

QUICK TIPS

If the client's Technology Stack includes

  - Java
  - PHP
  - .NET
- The AcuSensor technology for IAST / Grey Box Testing will make for a compelling solution.

Open-Source Content Management Systems

- Often enterprises will have Open Source content management systems in place for marketing or related activities. Acunetix boasts the highest detection of WordPress vulnerabilities – by scanning WordPress installations for over 1200 known vulnerabilities in WordPress' core, themes and plugins.

For teams that are not currently performing perimeter network level security scanning Acunetix includes OpenVAS scanner integration.

WHERE ACUNETIX WINS

Clients looking for more than just a standard DAST...a true vulnerability management offering

- Acunetix combines DAST, IAST, and Out-of-Band vulnerability monitoring along with Network Scanning and Malware Scanning perspectives

Large Network of In-Product Partner Integrations

- Bug Tracking:
  - JIRA
  - GitLab
  - GitHub
  - Mantis
  - Bugzilla
  - Microsoft TFS (Azure DevOps)
- CI/CD:
  - Jenkins
- WAF:
  - Imperva SecureSphere
  - F5 BIG-IP Application Security Manager
  - FortiWeb WAF

WHEN TO WALK AWAY

Unsupported Scanning Methods:

- For Teams that want a vendor with capabilities that include: Static Analysis (SAST), Runtime Application Self Protection (RASP) and/or Software Composition Analysis (SCA).
- Acunetix can run in conjunction with such systems, in order to provide even more vulnerability scanning functions.

March 2020