ServiceNow Application Vulnerability Response

Applications represent a growing attack vector

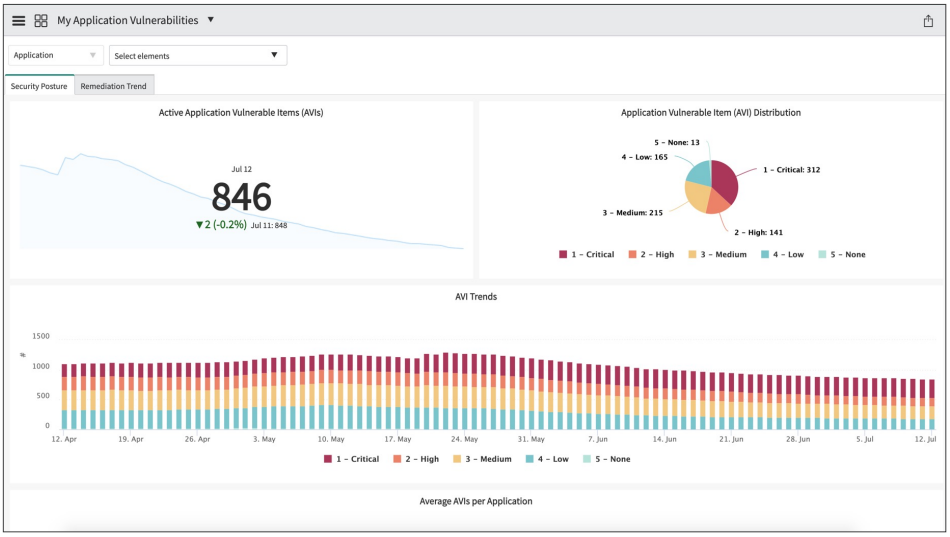
Organizations are increasingly developing their own custom software applications, but these can unfortunately lead to new security risks. 39% of data breaches in 2020 stemmed from web application compromise, according to the Verizon Data Breach Investigations Report. One cause is using open-source code, as while it enables faster application development, it is also readily available for cyber criminals to study and exploit.

To determine security flaws in deployment-stage applications, most organizations use testing tools such as Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), and Software Composition Analysis (SCA). These provide different ways to find weaknesses, whether in a running application or by examining source code. Using multiple testing tools creates a new layer of complexity for security teams to collect data points, identify relevant development teams, and determine next steps.

Applications also can be developed in a variety of different programming languages and tools. This means that any remediation solution must be customized to the application, which requires tight coordination between the software development owners and security analysts. Without a single pane of glass to understand priority and scope, drive remediation, and coordinate actions with development, it hampers the ability to swiftly address application vulnerabilities and reduce risk.

The ServiceNow solution

ServiceNow® Application Vulnerability Response is part of ServiceNow Vulnerability response, providing a central location to manage and respond to vulnerabilities across infrastructure and applications. It works with application vulnerability scanners and the Common Weakness Enumeration (CWE) to assesses DAST and SAST results to identify vulnerable applications and coordinate fixes with developer teams. It offers



The Application Vulnerability Response dashboard displays trends and summaries of vulnerabilities.

Focus resources on the most critical risks

Automate prioritization and assignment with configurable risk score calculators and rules. Reduce the amount of time spent on basic tasks with orchestration tools

Drive faster, more efficient response across security and development teams

Coordinate response across teams for smoother task handoffs between groups and quicker resolution. Ensure accountability with remediation targets.

Pinpoint development issues proactively

Get actionable insight from remediation data and adapt policies accordingly. Leverage reporting insights to tune development practices and reduce organizational risk.

a single location for all application vulnerabilities from multiple sources, determines their priority, and helps coordinate the remediation process with relevant stakeholders across security, development, and risk.

Built-in dashboards help you understand your security posture as well as remediation progress and trends for application vulnerabilities. A scoreboard ranks vulnerabilities by application to see which applications have the most issues due to critical or overdue vulnerabilities. This can help identify development process issues to keep them from recurring.

Find and prioritize application vulnerabilities

It starts with scanning your deployed applications. Dynamic (DAST) scans assess a running service, and results come with a URL location of the discovered vulnerability. Static (SAST) scans use the source code of the application and return a file and line number location of the vulnerability. The scan data is pulled into ServiceNow to see which applications and releases thereof are impacted. Data is also normalized for easier prioritization when using multiple scanners.

Weaknesses can also be discovered via penetration testing. Application Vulnerability Response allows application owners to request an assessment easily from the service catalog. The request goes to your ethical hacking team, who can scope the request and create a test environment. Findings are reported manually by creating application vulnerable items, or a combination of a specific vulnerability and an application release.

Application vulnerabilities, whether from a scanner or penetration testing, are then prioritized using a risk score. This score is determined by a configurable calculator that includes the severity of the vulnerability and the business criticality of the affected services or other dependencies. With Service Mapping from IT Operations Management, you can see how an application is related to other parts of the network, including the supported services. Risk scores are used consistently across the broader ServiceNow Security Operations to help you understand your overall security posture.

Remediate with visibility across teams

Each application vulnerable item is assigned a remediation target date. This applies an expected timeframe for remediation that can be determined based on the criticality, application impacted, or other factors. The remediation target can notify assignees or escalate as the time elapses. This ensures nothing is missed while also allowing some flexibility.

Not all vulnerabilities are urgent, and you can assign low priority ones a later remediation target date based on your organization's policies.

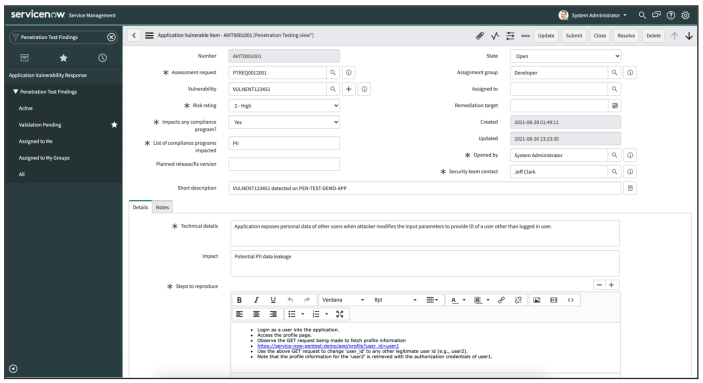
ServiceNow also can automatically assign each application vulnerable item to the appropriate group for remediation. This means security team members don't need to know who owns each application that is scanned. Application developers will update the application vulnerable item record when they have implemented a fix. This gives the security team visibility into remediation progress. When the next scan confirms the vulnerability is fixed, the record will be closed.

Business risks due to critical vulnerabilities or overdue remediation can also be tracked as part of your enterprise risk management program. This helps ensure good security hygiene with a holistic approach.

ServiceNow Security Operations

Application Vulnerability Response is part of ServiceNow Security Operations, a security orchestration, automation, and response engine built on the Now Platform. Designed to help security teams respond faster and more efficiently to incidents and vulnerabilities, Security Operations uses intelligent workflows, automation, and a deep connection with IT to streamline security response.

To learn more about ServiceNow Security Operations, please visit: **www.servicenow.com/sec-ops**



Request, report, and remediate penetration test findings using Application Vulnerability Response.

servicenow

SN-DataSheet-ApplicationVulnerabilityResponse-100621