INSIGHT® - VULNERABILITY MANAGEMENT SUITE

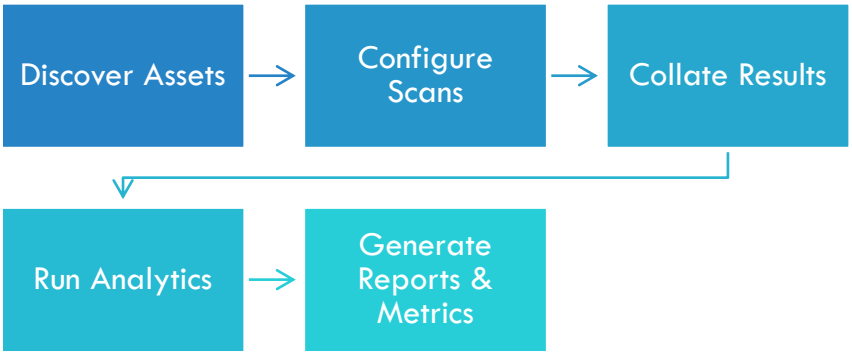
DESCRIPTION

InSight® is a single vulnerability management platform from where you can manage your assets, assess their vulnerabilities, determine compliance status, and adopt an effective workflow to address the discovered vulnerabilities. Further, a rich reporting interface and customizable dashboards allow you to get real insight into the effectiveness of your vulnerability management program. By combining business values of assets with the weighted vulnerability scores, you can demonstrate real business risk from open vulnerabilities.

With limited resources and numerous constraints you need to know which aspects of your vulnerability management program need your direct attention, and how do you prioritize your mitigation efforts. With InSight® you now get the true picture of the vulnerabilities and the risk they pose to your business.

KEY BENEFITS:

- Discover assets as well as new services or ports that open up on existing assets
- Discover vulnerabilities – both internally as well as on your perimeter
- Leverage our cloud-based architecture to constantly scan your perimeter
- Configure scan frequencies in line with risk levels
- Integrate output from multiple scanners and audit reports into a single manageable portal
- Get effective metrics around your vulnerability management program
- Use metrics to drive conversations with vendors and internal IT teams to get issues fixed
- Use metrics to demonstrate business risk to application owners



SPECIFIC CAPABILITIES

AUTO-DISCOVERY OF ASSETS AND SERVICES

InSight® is able to discover the appearance of new assets on your internal network as well as on your external perimeter. Given a range of IP addresses, InSight® runs continuous monitoring to scan for new assets as well as new ports or services that appear on existing assets.

SCHEDULED VULNERABILITY SCANNING

InSight® integrates with multiple scanners such as Nmap, Nessus, Qualys, Acunetix, Netsparker and many others to schedule scans, set up scanning policies, and retrieve scan results all through a single portal. Scans can also be triggered on-demand for any given asset or asset group.

DE-DUPLICATION OF VULNERABILITIES

InSight® comes with built-in capability to de-duplicate vulnerabilities discovered from multiple scanners on the same asset. This is done based on CVE IDs. This ensures that your administrators and web developers do not receive multiple reports containing overlapping and repeated issues. A simple counter keeps track of how many times the same issue has been discovered

REMOVAL OF FALSE POSITIVES

The false positive removal is done manually once the scan results are retrieved. This differentiates us from the run-of-the-mill continuous scanning services that pay little heed to the importance of manual intervention in delivering quality results to you. It is counter-productive to receive a 1000-page report over half of which consists of false positives. Our 24/7 SOC team reviews each report before it is released to you.

MALWARE MONITORING AND WEBSITE DEFACEMENT

The external perimeter scanning service also has the capability to scan for any malware injection on your website as well as determine any defacements of your web pages. Using a proprietary approach, we are able to determine heuristically for any malware that may have been injected onto the site. Our web defacement algorithm has a user-configurable sensitivity level that reduces false positives for pages that are regularly updated by the client.

VULNERABILITY MANAGEMENT WORKFLOW

InSight® comes with an extensive vulnerability management workflow that allows for issues to be tracked, commented upon, revalidated, and escalated if not fixed within a user-defined number of days or after a specific number of repeat discoveries. This ensures that you have exact insight into which issues are open across which assets and under the responsibility of which specific teams.

REPORTS AND METRICS

The key metrics around determining the effectiveness of your vulnerability management program are:

- Number of vulnerabilities by severity across asset groups
- Number of vulnerabilities by aging – i.e. number of days since open
- Number of vulnerabilities affecting a specific type of asset – say your databases
- Vulnerabilities by number and severity that are vendor-dependent
- Vulnerabilities discovered repeatedly – i.e. issues that are not being fixed over multiple scans
- Compliance across ISO 27001, PCI DSS, HIPAA, SOX, etc.

These are just some of the analytics and reports that can be generated by InSight®

ARCHITECTURE

InSight® can be installed on premise or it can run completely in the cloud if you're only focused on scanning your perimeter. In combination with the on premise engine, you get a 360° view of vulnerabilities within your network as well as those on your perimeter.

With InSight® you know exactly which vulnerability on which asset needs your most immediate attention and where your key problems lie.

FOR MORE INFORMATION

Network Intelligence (I) Pvt. Ltd.
Mumbai ● Pune ● Delhi ● Chandigarh ● Dubai
Email: info@niiconsulting.com
Web: www.niiconsulting.com

NETWORK INTELLIGENCE
ISO 27001 Certified | PCI DSS QSA