VULNERABILITY ASSESSMENT CHECKLIST

clarify360.com

Vulnerability Assessment solutions identify, categorize and prioritize vulnerabilities as well as orchestrate their remediation or mitigation. Their primary focus is vulnerability and security configuration assessments for enterprise risk identification and reduction, and reporting against various compliance standards.

Vulnerability Assessment can be delivered via on-premises, hosted and cloud-based solutions, and it may use appliances and agents. Core capabilities include:

- Discovery, identification and reporting on device
- OS, software vulnerabilities and configuration against security-related criteria
- Establishing a baseline for systems, applications and databases to identify and track changes in state
- Reporting options for compliance, control frameworks and multiple roles

Standard capabilities include:

- Pragmatic remediation prioritization with the ability to correlate vulnerability severity, asset context and threat context that then presents a better picture of true risk for your specific environment
- Guidance for remediating and configuring compensating controls
- Management of scanner instances, agents and gateways
- Direct integration with, or API access to, asset management tools, workflow management tools and patch management tools

VULNERABILITY ASSESSMENT CHECKLIST

BROAD SCANNING CAPABILITIES

	Vendor:	Vendor:	Vendor:
Agent-based architecture			
Expansive visibility			
Hybrid vulnerability management			
Select target hosts by their Internet Protocol (IP) address, asset grouping or asset tagging			
Scan manually, initiate upon a schedule, or continuously on 24×7 basis			
Scan behind the firewall with Scanner Appliances which are remotely managed by Vendor			
Internal networks may be scanned, including those with overlapping private IP address space			
Authentication credentials may be used securely to log in to each host, database, or web server scan on Amazon EC2			
Configuration information may be stored offsite with a secure audit trail			

VULNERABILITY ASSESSMENT CHECKLIST

CUSTOM REPORTING

	Vendor:	Vendor:	Vendor:
Create different reports for different audiences.			
Document that policies are followed, and also document when lapses in policy are remediated.			
Track ongoing progress against vulnerability management objectives.			
Provide the right data needed to document each vulnerability, including changes in status (trends), possible predictions and potential approaches to remediation.			
Share data with GRC systems & other enterprise applications using a flexible XML-based API.			

RISK TRIAGE

Track vulnerabilities over time and show continual status and changes			
Monitor digital certificates deployed throughout your network			
See which hosts need updates after Patch Tuesday every month			

VULNERABILITY ASSESSMENT CHECKLIST

RISK TRIAGE (cont'd)

	Vendor:	Vendor:	Vendor:
Examine your network's vulnerabilities over time			
Predict which hosts are at risk for Zero-Day Attacks			
Configuration information may be stored offsite with a secure audit trail			

REMEDIATE VULNERABILITIES

Automatically generate and assign remediation tickets for identified vulnerabilities.			
Produce consolidated reports of which hosts need which patches.			
Allow Integration with IT ticketing systems.			
Allow for exception management—it is sometimes the case that a vulnerability might be riskier to fix than not.			
Automatically expire exceptions after a period of time for later review			
Configuration information may be stored offsite with a secure audit trail			

VULNERABILITY ASSESSMENT CHECKLIST

INSIGHTS PROVIDED

	Vendor:	Vendor:	Vendor:
Overall system summary			
Overall scan summary			
Total number of scans			
Total number of vulnerabilities			
Top 10 vulnerabilities			
Security issues by asset			
Security issues by vulnerability			
Indicators of Compromise			
Major security changes needed			
Recommendations for remediation			
Effectiveness of remediation			

VULNERABILITY ASSESSMENT CHECKLIST

VULNERABILITIES UNCOVERED	Vendor:	Vendor:	Vendor:
Common Backdoors Detection			
Backup Files			
Captcha Detection			
Code Injection			
Common Directories			
Card number disclosure			
Cross-site request forgery			
Directory Listing			
File Inclusion			
.htaccess LIMIT misconfiguration			

VULNERABILITY ASSESSMENT CHECKLIST

VULNERABILITIES UNCOVERED (cont'd)

	Vendor:	Vendor:	Vendor:
Insecure Cookies			
LDAP Injection			
ASP Localstart			
Command Injection			
Auto-complete password fields			
Path Transversal			
Private IP address disclosure			
Response splitting			
Remote File Inclusion			
Session Fixation			
Source code disclosure			
SQL Injection			

VULNERABILITY ASSESSMENT CHECKLIST

OTHER FEATURES

	Vendor:	Vendor:	Vendor:
Visually maps your network using a graphical host map.			
Help teams remediate and triage vulnerabilities by assigning a business impact to each asset.			
Identify which OS, ports, services, and certificates are on each device on your network.			
Control which hosts can be scanned by which appropriate users.			
Allows for the continuous monitoring of your perimeter for unexpected changes with an optional Continuous Monitoring Service			
Dynamically assign assets to categorize hosts by tags like network address, software installed, vulnerabilities, and more			