InterVision Professional Services

Vulnerability Assessment Service

Validating and Improving Your Security Posture Through Network Security Testing and Reporting

AWARENESS: Identify what vulnerabilities exist in your externally-facing or internal systems to understand risk in the environment.

ENABLEMENT: Specific results and prescriptive recommendations enables remediation of vulnerabilities and minimizes the attack surface.

RISK REDUCTION: Ensure that security compliance requirements are met and reduce risk by identifying and closing security gaps.

Vulnerability Scanning for Risk Mitigation and Compliance

IT Security continues to be a primary focus for well-established companies, especially as it relates to Internet-connected services and assets. Similar to viruses, techniques are constantly being developed to take advantage of vulnerabilities either at the host layer or within the application it serves. But unlike how anti-virus software protects endpoints, web applications and hosts do not proactively scan and protect against malicious activity in real-time. Instead, its most often up to the administrator to harden those assets at deployment time and then apply patches and configuration updates on a regular basis to protect against newly discovered exploits. Even then there is no way to ensure that these systems are protected against the most current threats without scanning them for vulnerabilities.

Our **Vulnerability Assessment** service safely examines your systems and web applications to identify weaknesses against all currently known exploits. The Vulnerability Assessment service leverages best of breed vulnerability scanning technology that is constantly updated to ensure that even the latest well-known exploits are included in the system examination process.

Assessing Internal and External Risk

Most security investments in terms of both cost and effort are, for obvious reasons, applied towards protecting Internet-facing systems and the services they provide. These systems may exist in your datacenter (on premise), in a co-location facility, or within a public cloud provider and all should be periodically assessed.

While great care is taken to protect these Internet-facing systems, the company's greatest assets, which tend to exist within the environment, are also at risk. The same hacks launched from the Internet can be applied to internal system should the wrong person gain entry into your network using any number of methods. Our **Vulnerability Assessment** service offers our customers the flexibility to search for and identify vulnerabilities that may exist in both your Internet-accessible as well as internally-facing hosts and web applications.

Making Sense of the Findings

Our Vulnerability Assessment relies on best-of-breed scanning technology that is constantly updated to identify the latest threats affecting a wide range of commonly used services and operating systems. However, it takes expertise and experience to assess and validate the severity of the discovered weaknesses. Our security consultants not only guide our customers through the scanning preparation and execution process, but then organize and analyze the results to provide our customers with a comprehensive understanding of their current system and web application security posture and prescriptive recommendations for eliminating their vulnerabilities.

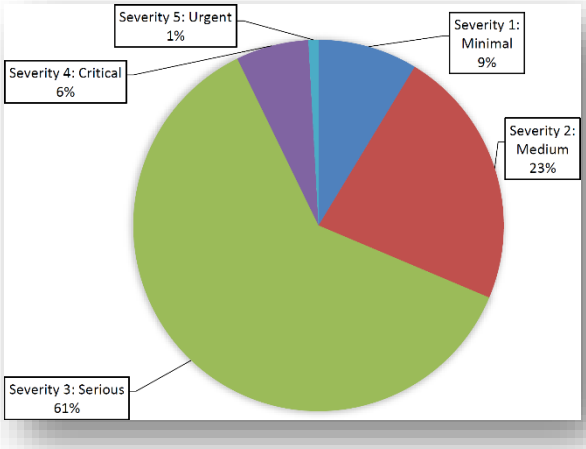
Turning Data into Actionable Information

Vulnerability scans generate a lot of data, especially in larger environments. Our consultants organize that data into different views and levels of detail that cater to each audience from IT executive to systems engineer.

SEVERITY	LEVEL	DESCRIPTION
	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

An executive level summary highlights those vulnerabilities of the highest severity levels found to be present in the environment and provide an initial view of where focus should be applied to mitigate risk.

Discovered vulnerabilities are then organized by severity level, type, and count of occurrences across the scanned environment. This offers the IT professional context and a 'big picture' view of the overall security posture of systems and web applications in the environment.



Lastly, our assessment report presents detailed information about each unique vulnerability type and the systems impacted. Such details include:

- Title
- Affected Hosts
- Port
- CVE-ID
- Findings
- Impact
- Solution

Beyond the Vulnerability Assessment

InterVision offers an extension option to the Vulnerability Assessment where high-severity vulnerabilities are manually tested and confirmed preventing our customers from spending time addressing false-positives. The toolkit used to confirm internal host and web application vulnerabilities can be left in place after the engagement to allow our customers to perform their own post-remediation tests.

Inside the Vulnerability Assessment Service

This assessment service is intended to identify vulnerabilities in your IT environment with details and prescriptive recommendations to mediate and reduce risk. By default, the Vulnerability Assessment Service engagement involves the following activities:

- Discovery
  - Identify environments to be scanned
  - Perform discovery scan(s)
  - Determine & document scope of systems to test (IP selection)
  - Determine & document scope of web apps to test (URL selection)
- Preparation
  - Provide scanning tool (internal scans)
  - Validate scanning tool communication (internal scan)
  - Configure scanning scope
  - Assist in coordination / communication with 3rd Party providers
  - Schedule scan(s)
- Execution
  - Perform scan(s)
  - Capture scan results
- Analysis
  - Parse & organize results data by threat type
  - Analyze results to create key findings
  - Validate and reproduce significant findings
  - Develop prioritized recommendations
  - Produce scan assessment report
- Delivery
  - Review findings with Customer
  - Update report per Customer feedback (if applicable)

SCANNING SCOPE
Apache Web Server
Apache Tomcat Server
Checkpoint Firewall
Cisco (assorted devices)
Docker
HTTP / HTTPS
IBM DB2
IBM WebSphere
Linux / UNIX
Load Balancer (assorted)
Microsoft IIS
Microsoft SQL
Microsoft Windows Server
Oracle DB
Oracle WebLogic
Password Brute Forcing
Password Vaults (assorted)
SNMP
Sybase
TCP / UDP Ports
VMware ESX / ESXi

The Vulnerability Assessment Service requires approximately three weeks to deliver from project kickoff through knowledge transfer and documentation handoff. The service includes planning questionnaires for both IP-based Host scans as well as URL-based Web Application scans to assist in the identification of systems and/or networks to include in the service.

Next Steps

To learn more about how InterVision can help you validate and improve your security posture, visit www.intervision.com or contact your InterVision sales representative.

InterVision helps customers optimize IT infrastructure, better manage risk, & gain a competitive advantage with IT integration and broad capabilities.