Cautela Labs

Cloud Agile. Secured. 🟥 🟨 🟩

Vulnerability Management

Scanning and Assessment Service

Vulnerability Management Services

New network, application and database vulnerabilities emerge every day. Because they can be exploited by attackers, it is essential to eliminate these exposures to protect your critical IT assets and safeguard sensitive information. In order to stay on top of these Cautela Labs offers a series of Scanning services for internal and external scans across network devices, servers, Web applications, databases and other assets in your environment. The services can be provided as an on-demand service or as part of an on-going planned service.

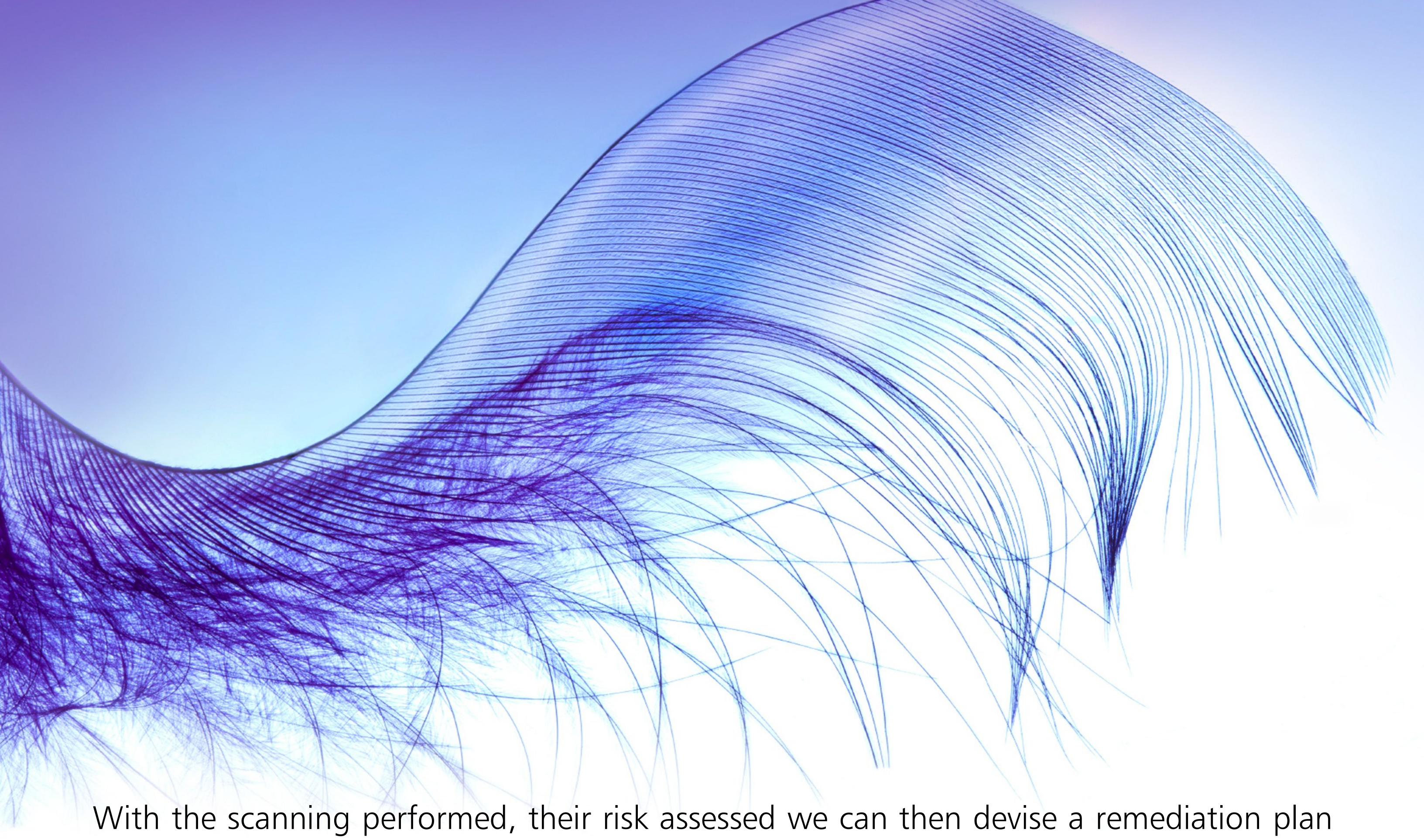
Cautela Labs offers a managed vulnerability assessment service that entails scanning all web applications, databases, networks, operating systems and other network-resident software to detect threats, assess their risk and devise a remediation plan to quickly mitigate them. It enables IT and security groups to implement a measurable and proactive vulnerability management process that eliminates security weaknesses in your network before the network is penetrated and sensitive information is compromised. Key to this service is the Cautela labs Scanning and Assessment Service and Penetration Testing.

Cautela Labs Scanning and Assessment Service

The complexity of your enterprise provides myriad points of potential intrusion. Certainly, most susceptible are external-facing web applications, but no less fundamental to your enterprise's security are the server and network infrastructure and the peripheral devices connected to it. Vulnerability scanning that aggressively addresses the core components of your infrastructure is essential for maintaining your security compliance, the integrity of your applications and files, as it will then allow a remediation plan to be put in place based on the assessment of those vulnerability.

The Cautela Labs Scanning and Assessment Service identify vulnerabilities efficiently and accurately, protecting critical network assets and intellectual property. It will run tests to verify that effective security policies are in place for the following components:

Firewalls
IPS
IDS
Application servers
Web servers
Active Directory controllers
Email servers
Layer2 and Layer3 Switches
Routers and gateways
All networked workstations and peripherals.



With the scanning performed, their risk assessed we can then devise a remediation plan to quickly mitigate them. The Plan enables IT and security groups to implement a measurable and proactive vulnerability management process that eliminates security weaknesses in your network before the network is penetrated and sensitive information is compromised. The ultimate benefits derived from this thorough and encompassing security assessment include:

- The process of doing a thorough assessment helps direct senior management's attention to IT security. It surfaces security issues, risks, vulnerabilities, mitigation options, and underscores best practices.

- Establishing or evaluating against a baseline. If a baseline has been established, an assessment is an opportunity to gauge the improvement or deterioration of an organization's security posture.

- Generating lists of vulnerabilities and potential responses is the main activity and outcome of an assessment.

- An assessment can be a vehicle for reaching corporate-wide consensus on a hierarchy of key assets. This ranking, combined with threat, vulnerability and risk analysis is at the heart of any risk management process.

Penetration Testing

Using the vulnerability assessment results, our analysts attempt to use the identified security weaknesses to bypass system controls. This assists the analysts in determining how a system may be compromised and where additional safeguards are needed. The vulnerability assessment identified and reported noted vulnerabilities, whereas a penetration test attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network penetration testing and application security testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network. At the conclusion of testing, Cautela Labs will deliver finding reports that detail specific findings. Finding reports are suitable for internal distribution and are intended to provide you with the information needed to begin remediation. These reports can be utilized for compliance reporting and the actual Penetration test can be performed on demand or as part of regularly schedule plan as is the case particularly with compliance driven organizations as part of their on-going compliance process.

Cautela Labs, Inc.
5080 N. 40th Street, Suite 300
Phoenix, AZ 85018
Phone: 800-997-8132
Fax: 714-862-2177
Email: Support@Cautelalabs.com