PALADION
HIGH SPEED CYBER DEFENSE

ahornloesungen
deutschland gmbh

Vulnerability Management Program

Identify and remediate vulnerabilities before attackers weaponize them

Tracking a steady flow of vulnerable data from software updates, patches, security advisories, threat bulletins, etc. can be overwhelming for a security analyst. But, following it is a crucial step in your vulnerability management (VM) program, because attackers can discover vulnerabilities announced by researchers and weaponize them before a patch or update is applied, so reducing remediation time is a key defence against such threats.

Prioritize the latest, High Risk Vulnerabilities

Monitoring this steady stream of information of relevant vulnerable data can take up time, attention, and resources that an enterprise cannot afford. A professional vulnerability management can solve this problem and bring additional value to your VM program.

Get Tailored Vulnerability Management

Our security researchers use their years of experience in working with over 700 different businesses from different industries to create a Vulnerability Intelligence Database that is unique to your business. This is plugged into the VM program, so you can proactively address vulnerabilities and exposures.

Fully Managed Vulnerability Management Program

Paladion works with leading partner solutions to provide first-rate vulnerability management with your existing hardware and software set-ups. The program is fully managed by Paladion security professionals, so you are not burdened with administration and maintenance.

Mitigate Risk and Streamline Audits

- Compliance Reports
- Enterprise Integration
- Centralized Vulnerability Visibility
- Triaging:Remediation Prioritization
- Expert guidance on tap

SERVICE FEATURES

Reduce your Threat Landscape and Secure Your Business

Continuous Testing

Application Security Assessments

Safeguard your applications from security threats

Assessments on servers and devices cover authentication system and business-related threats to improve the overall security posture of applications

Secure Configuration Audits

Extensive audit to enhance IT security posture

Identify insecure configuration settings on servers and network devices and define corrective actions. Improve defence-in-depth posture of the organization

Network Vulnerability Assessments

Reduce false positives and negatives

Internal and external tests performed manually and automatically provide accurate analysis of vulnerabilities on software and firmware on servers, databases and network devices

Management Framework

Asset Risk Profiling

Establish a risk-driven framework for assessments

Achieve compliance, vulnerability mitigation and improvement of overall security posture with a risk-driven framework

Analytics

Achieve centralized vulnerability visibility

Collate data and present a unified risk status for assets and view trends for better decision making and remediation.

Integrated Workflows

Automate mundane operational tasks

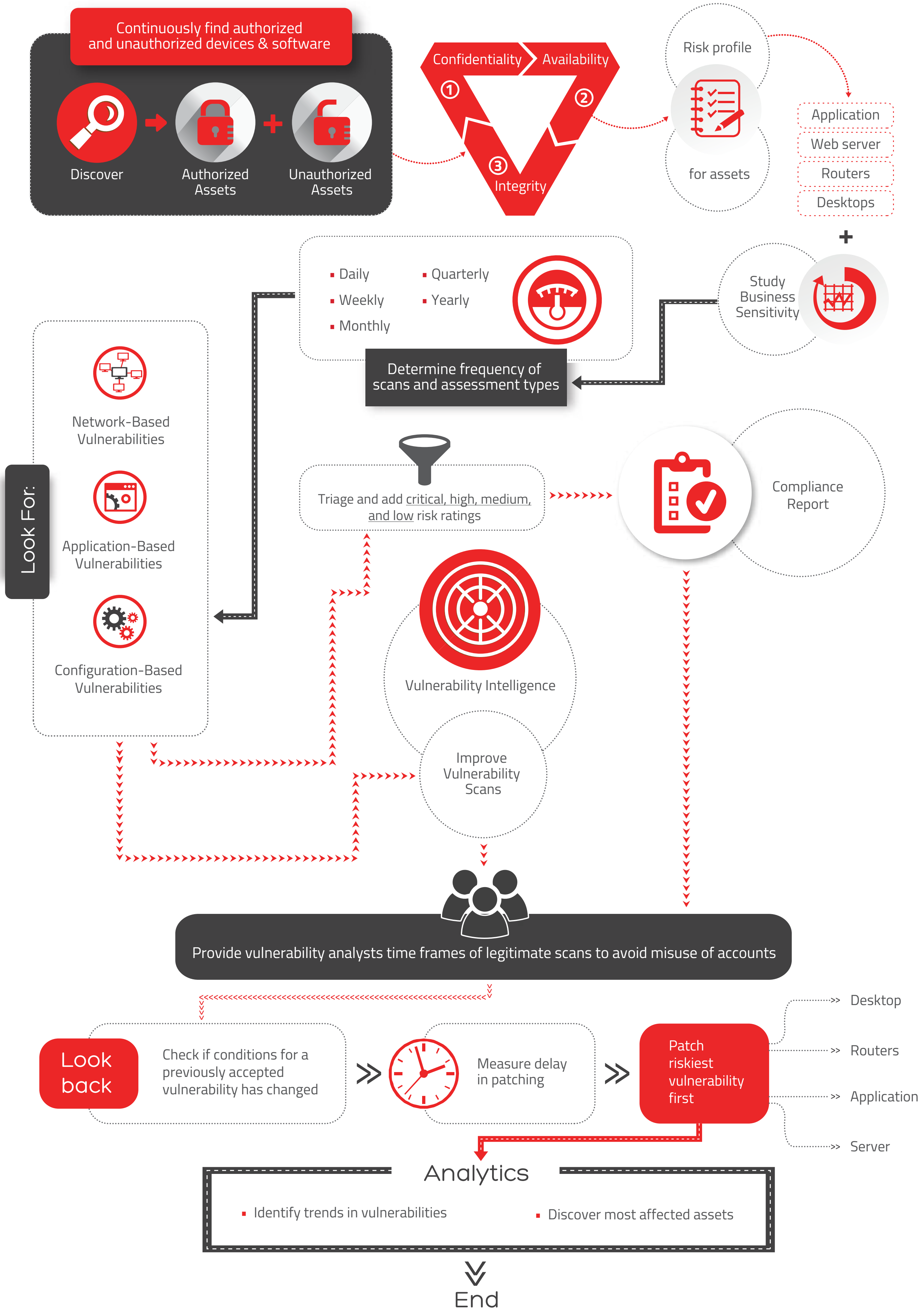
- Schedules scans and tests
- Conduct test preparations and gather requirements
- Prepare and distribute reports
- Multiple discussion for solution related activities
- Track vulnerability closures

Vulnerability Triaging

Prioritize based on multiple parameters

- External/Internal Threat intel, asset, user data, controls, business risk
- De-duplicate vulnerabilities
- Remove false positives

How We Reduce Vulnerabilities in Your Environment



Continuously find authorized and unauthorized devices & software

Discover → Authorized Assets + Unauthorized Assets

① Confidentiality

② Availability

③ Integrity

Risk profile for assets

Application

Web server

Routers

Desktops

+

Study Business Sensitivity

- Daily
- Weekly
- Monthly
- Quarterly
- Yearly

Determine frequency of scans and assessment types

Look For:

Network-Based Vulnerabilities

Application-Based Vulnerabilities

Configuration-Based Vulnerabilities

Triage and add critical, high, medium, and low risk ratings

Compliance Report

Vulnerability Intelligence

Improve Vulnerability Scans

Provide vulnerability analysts time frames of legitimate scans to avoid misuse of accounts

Look back

Check if conditions for a previously accepted vulnerability has changed

Measure delay in patching

Patch riskiest vulnerability first

Desktop

Routers

Application

Server

Analytics

- Identify trends in vulnerabilities
- Discover most affected assets

End

BENEFITS

Continuous Testing

Assessments of greater depth

A combination of automated scans and manual exploits, provides an accurate analysis of network vulnerabilities. The program maps compliance requirements like PCI, standards such as SANS and OWASP, and also adheres to OSSTM standards. Expert guidance on fixing issues on live systems is also provided

Identify and mitigate threats

Our advanced VM program provides threat profiles for applications that can be followed by developers and QA analysts alike. It also aims to cover application layer, host layer, and business logic threats, and assesses the application against stringent criteria. Our actionable solutions enable application owners to deliver secure applications on time, every time

Improved defence-in-depth posture

The program gives you a holistic view of your IT infrastructure by exposing insecure configurations, weak policy settings, and non-compliance to baselines on your IT assets. Use of custom-built audit tools for each platform, quickly and accurately identifies weak settings, policies and configurations in multiple assets across your organization

Management Framework

Context-aware security testing

Our advanced VM Framework aims at risk profiling of IT assets to make security testing context and risk aware. Our proprietary VM platform performs in-depth and frequent testing on critical and important IT assets while covering baseline assessments for all other assets

Mature model to reduce your security burden

Our VM framework is supported by a highly evolved proprietary vulnerability management platform that helps reduce operation management burden while optimizing on security costs. Such a model allows customizable auditing scans with minimum burden to IT resources

Vulnerability intelligence for a better security program

Our VM framework helps derive key metrics like mean-time-to-remediate, most vulnerable assets, and frequently occurring vulnerabilities. For some of our clients, we were able to achieve 50% reduction in vulnerability remediation time thus achieving lower breach exposure.