CyStack

DATA SHEET

Vulnerability Management

Keep your business safe from security vulnerabilities

Security Challenge

In today's digital age, businesses are facing a growing number of cyber risks, making it more challenging to protect their networks and data. These challenges can include:

- **Shortage of skilled cybersecurity professionals**: As the demand for cybersecurity expertise continues to grow, many businesses struggle to find and retain qualified professionals to manage their security needs.
- **Keeping up with the latest threats**: New cyber threats are constantly emerging, and it can be difficult for businesses to keep up with the latest trends and best practices to protect against them.
- **Managing multiple security solutions**: Businesses often have to manage multiple security solutions, such as firewalls, intrusion detection systems, and antivirus software. This can be time-consuming and confusing for businesses to manage.
- **Staying compliant with industry regulations**: Many industries have specific regulations and standards that businesses must meet, such as HIPAA or PCI DSS. Compliance can be challenging, and non-compliance can result in hefty fines.
- **Limited budget**: Small and medium-sized businesses often have limited budgets, which can make it challenging to invest in the necessary security solutions and personnel.

Managed security services can help businesses overcome these challenges. By outsourcing security responsibilities to a managed security service provider (MSSP), businesses can access a team of experts dedicated to staying up-to-date on the latest threats and best practices. MSSPs can also help businesses manage multiple security solutions, stay compliant with industry regulations and standards, and provide regular reporting on the client's security posture. Furthermore, by outsourcing security, businesses can save resources and reduce the risk of costly security incidents.

Customer Benefits

- Improve the overall security posture by using a comprehensive and ongoing assessment of the security risks, vulnerabilities, and controls
- Reduce security-related costs by eliminating the need to hire and maintain an in-house security team
- Streamline the security operations and more effectively respond to potential security incidents and threats
- Access to a team of security experts who have the knowledge and expertise to keep the systems and networks secure
- Have peace of mind knowing that your security is in the hands of experienced and knowledgeable security professionals

Overview

Vulnerability Management is the process of identifying, prioritizing, and mitigating security vulnerabilities in networks and systems. The goal of Vulnerability Management is to reduce the risk of a security breach by proactively identifying and addressing potential weaknesses before they can be exploited by attackers. Hence, Vulnerability Management should be implemented in a sequence of well-organized phases to provide the best results. Effective Vulnerability Management can help organizations prevent security breaches and protect their sensitive information, systems, and infrastructure. It is an important component of an overall cybersecurity strategy and should be performed regularly to stay ahead of new and emerging threats.

The key to successfully managing vulnerabilities lies in the cross-section of:

- Creating a good baseline for vulnerability management, considering the physical and digital assets and prioritizing them to define the risk based on their criticality and value.
- Performing automated scans to reduce the time and effort needed to identify security vulnerabilities and weaknesses in the organization's infrastructure.
- Prioritizing found security issues according to their risk levels.
- Applying mitigation or remediation for detected vulnerabilities in a timely manner to reduce the impact and severity.
- Providing clear and concise reports with actionable insights.
- Verifying security flaw patches to ensure that they work properly and the issues cannot be exploited in the future.
- Monitoring continuously the network and systems to maintain a good security posture.
- Having access to real-time information on emerging threats and maintaining an up-to-date database for well-known and published security issues so that the vulnerabilities can be addressed promptly.
- Integrating with other security tools such as patch management and threat detection to provide a comprehensive security posture.
- Ensuring that every procedure in vulnerability management is executed by cyber security analysts with the necessary expertise and skills.

Key Features

- Gain assurance that your infrastructure and applications are secure
- Discover vulnerability by using fuzzing and our own vulnerability database
- Monitor and alert new issues continuously and automatically
- Test by talented security pentesters from CyStack and over 3000 researchers from our community
- Manage, track, prioritize, and remediate the findings in the CyStack Vulnerability Management Platform
- Receive actionable recommendations to enhance security
- Reduce your risk and improve operational efficiency
- Can integrate the scan with CI/CD and productivity tools
- Export monthly report

How CyStack Helps

The CyStack Audit Team is a group of highly skilled security testers who use a goal-oriented approach to testing, refined through years of experience and extensive testing. Our team members have a unique blend of app development and security testing expertise, enabling them to conduct comprehensive security evaluations that uncover potential risks for organizations. Members of this team are also regular speakers at world-known cyber security conferences and also talented bug hunters who discovered many critical vulnerabilities in the products and are acknowledged in the Hall of Fame of global tech giants such as IBM, HP, Microsoft, Alibaba, Sea Group, etc.

As a leading managed security service provider in Vietnam, with years of experience in designing and implementing network security solutions for many large and small businesses, experts at CyStack have researched and launched a comprehensive and efficient Vulnerability Management solution that can be tailored for businesses of every size and nature. This security model is a model of continuous testing and responding, via a combination of automated asset and vulnerability scans, regular monitoring and real-time alerting, manual analysis from our experts and crowdsourced security, in order to minimize security risks on the system at all times. As a result, businesses can enhance the security of their applications at every stage of development and maintain a stable security posture while rolling out frequent application upgrades without investing time and effort in every procedure of vulnerability management. By working with the development team, CyStack will extend the organization's security capabilities, improve its reputation, and reduce its security backlog.

CyStack's Vulnerability Management service can be understood as an efficient and systematic reorganization of our following services:

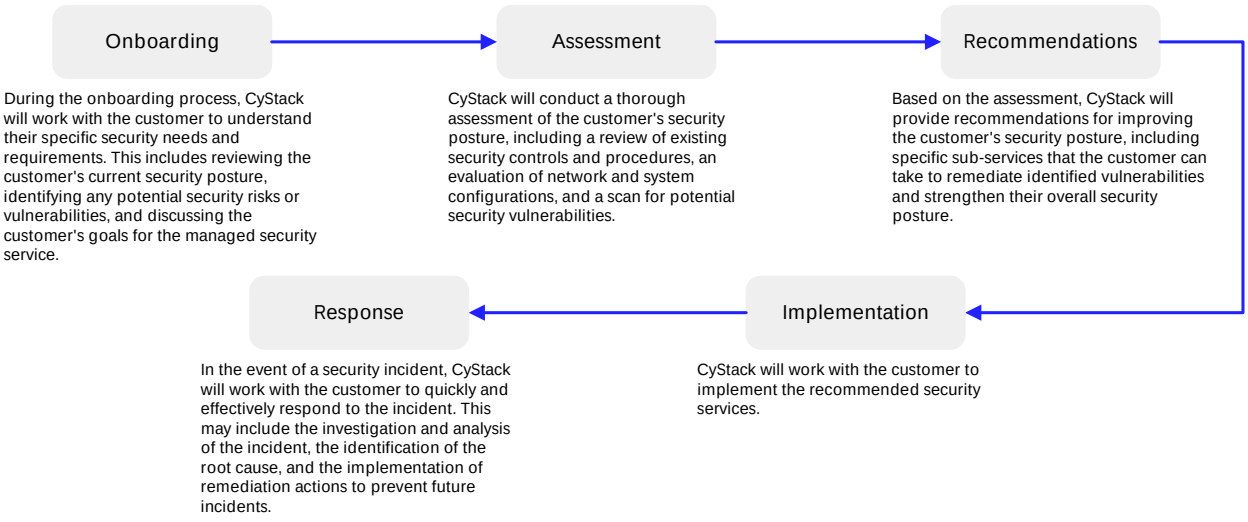
- **Vulnerability Assessment**: To simplify and automate the Vulnerability Assessment, CyStack develops a security vulnerability scanning and monitoring tool for web applications, called CyStack Web Security (CWS). CWS helps organizations scan sub-domains and addresses in the private network, and discover vulnerabilities by using fuzzing and our own vulnerability database. With CWS, new vulnerabilities are monitored continuously and alerted automatically right the moment they are detected. CWS also provides a platform to manage, track, prioritize, and suggest remediations for the findings. Moreover, organizations can integrate CWS with CI/CD and productivity tools. Please refer here for more details.
- **Pentest**: A Pentest, or Penetration Test, is a simulated cyber attack on a computer system, network, or web application in order to identify vulnerabilities that an attacker could exploit. Pentest is performed by security professionals who use a variety of tools and techniques to test the security of the target environment and identify weaknesses that could be attacked. Please refer here for more details.
- **Managed Bug Bounty**: A Bug Bounty program is a type of crowdsourced security that incentivizes individuals or groups, known as "white hat hackers", to identify and report security vulnerabilities in a company's software or systems. Companies offer rewards, such as monetary compensation, swags, or recognition, to ethical hackers who are able to find and report these vulnerabilities. CyStack provides organizations with the first and the biggest crowdsourced security platform in Vietnam called WhiteHub. Please refer here for more details.

Methodology

In general, the methodology of CyStack's Vulnerability Management strictly adheres to the following steps:

1. **Prework**: Defining the scope of vulnerability management, identifying the architecture, components and infrastructure of each in-scope asset, understanding the business processes and the required standard, legal or regulatory compliance, prioritizing the assets based on their criticality and creating an effective and well-organized plan of vulnerability management accordingly.
2. **Discover**: Performing OSINT information gathering, deciding the correct vulnerability scan strategy according to requirements and compliance, running vulnerability scans using tools, and examining the infrastructure security (with documentation if provided).
3. **Evaluate**: Applying the business and technology context to scanner results to point out which the actual vulnerabilities are, filtering false positive results by validating security issues manually, and prioritizing found vulnerabilities based on risk and level of impact.
4. **Report**: Creating a clear and concise report that contains concrete information for each vulnerability, such as title, ID, description, severity score, steps to reproduce, recommendations, etc.
5. **Remediate**: Prioritizing remediation based on risk ranking, informing well-structured action plan to implement recommendation or remediation, reviewing the root cause of vulnerabilities with customers, providing best security mitigation in case of risk acceptance due to the business processes.
6. **Verify**: Rescanning the systems to identify if applied fixes are effective, performing dynamic analysis manually by security analysts to ensure all patches work perfectly, and reviewing the attack surface after vulnerability remediation.
7. **Monitor**: Performing vulnerability scan and assessment periodically, alerting security issues early with threat intelligence and in real time via vulnerability management platform, consulting up-to-date best practices that fit the business, reviewing security policies, procedures and controls regularly.

Flow To Work With Clients



About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net