CyStack

DATA SHEET

Managed Security Service

Your Trusted Partner in Cybersecurity

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 who are 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. They can also provide training to employees on how to recognize and respond to security threats. 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

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, CyStack can help businesses protect their networks and data by providing a range of services that are specifically designed to mitigate cyber risks. Our solutions focus on security auditing, hardening, monitoring, training, and responding to threats. Our goal is to help businesses keep their entire systems secure while they just focus on developing their products and their business.

Key Features

- Vulnerability Management
- Security Hardening
- Security Monitoring
- Security Training
- Incident Response
- All-in-one security platform

Methodology

CyStack, as a Managed Security Service Provider (MSSP), offers a range of services that can be tailored to meet the specific needs of each customer. Customers have the flexibility to choose the services that best suit the organization's needs and budget. This can include any combination of the following services:

Service	Main solutions
Vulnerability Management (VM)	Vulnerability Assessment + Pentest + Managed Bug Bounty
Security Hardening (SH)	Configuration Review + Access Control + Software Updates
Security Monitoring (SM)	Event Logging + Threat Detection + Anomaly Detection
Managed Bug Bounty (MMB)	WhiteHub Bug Bounty Platform

Vulnerability Management

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. 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.

CyStack's Vulnerability Management service includes:

- **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.

Security Hardening

Security Hardening is the process of securing networks and systems by implementing best practices and security controls to make them more resistant to attacks. The goals of Security Hardening are to improve the overall security posture of a system or network, reduce the risk of a successful cyber attack, and enhance the confidentiality, integrity, and availability of sensitive data and resources. Security Hardening is an ongoing process that requires continuous evaluation and adjustment to stay ahead of new and evolving threats.

CyStack's Security Hardening service includes:

- **Configuration Review**: Reviewing the security settings and configurations of your organization's systems and applications, and looking for any misconfigurations or vulnerabilities that could be exploited.
- **Access Control**: Assessing the effectiveness of the organization's access controls, such as authentication and authorization mechanisms, and identifying any potential weaknesses.
- **Software Updates**: Updating and patching software and firmware to address known vulnerabilities and security flaws.

CyStack consults and decides with clients on tailored Security Hardening services for organizations, depending on their infrastructure architecture, technologies, and specific requirements. We also have other services that refer to Security Hardening, which are Internal Network Audit, Cloud Security Audit, and DevSecOps.

Security Monitoring

Security Monitoring is the process of continuously monitoring networks and systems for potential security incidents, threats, and anomalies. The primary goal of Security Monitoring is to identify and respond to security incidents in a timely manner before they cause significant harm, in order to minimize the potential impact and prevent further damage to the organization from a security breach. Security Monitoring typically involves the use of security technologies such as firewalls, intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM) systems, and antivirus software. It may also involve the use of manual monitoring and analysis by security professionals.

CyStack's Security Monitoring service includes:

- **Event Logging**: Recording and storing detailed information about events that occur on a system or network, in order to monitor and analyze security-related activity.
- **Threat Detection**: Identifying and analyzing potential security threats and attacks on an organization's systems and networks, which involves the use of security monitoring tools and techniques, and manual analysis by security professionals.
- **Anomaly Detection**: Identifying and alerting on deviations from normal or expected behaviour within a system or network, which might include identifying unusual login activity, unexpected network traffic, or unusual file access patterns.

Please refer here for more details.

Managed Bug Bounty

In the context of Internet users increasingly imposing high standards on the products they use, businesses are inadvertently pushed into the race to develop products fast enough, good enough, and still be safe in the operation. The more frequently the software is updated, the more likely it is to have security flaws.

The solution to this problem is that developers must be faster than hackers in finding and fixing vulnerabilities in their products. An advanced approach here is to use crowdsourced security. Basically, this is an extended version of traditional security testing in terms of human resources. Instead of working with a team of 2-5 security testers, companies now can have a security researcher community of thousands of people who will help them to find out security issues.

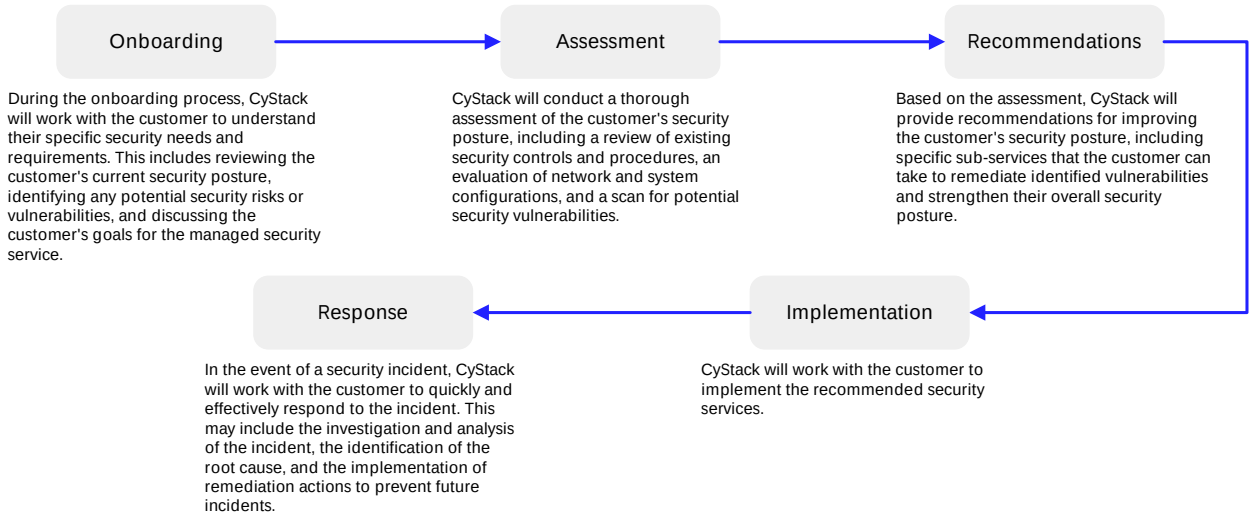
CyStack supports businesses in launching and managing bug bounty programs in WhiteHub, the 1st and the biggest crowdsourced security platform developed by CyStack in Vietnam.

A bug bounty program aims to identify and address security vulnerabilities in a timely and efficient manner, while also providing a safe and secure environment for ethical hackers to report vulnerabilities. This can help organizations to improve their security posture and reduce the risk of cyber-attacks and data breaches.

Please refer here for more details.

Flow To Work With Clients

The flow for working with customers in a managed security service typically includes the following steps:



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