CyStack

DATA SHEET

Security Monitoring

Always on the lookout, securing your digital assets

Why Monitoring?

Security Monitoring is a critical aspect of modern business operations, as it helps organizations protect their digital assets and ensure the security of their networks and systems.

Today, businesses rely on digital data to run their operations, and this data is often highly sensitive in nature. This data can include confidential business information, financial records, and personal data of customers and employees. Organizations face an ever-increasing threat landscape, with cyber attackers leveraging a growing array of tactics, techniques, and procedures to compromise systems and steal data. By implementing Security Monitoring, organizations can detect and respond to these attacks, limiting their impact and helping to prevent data breaches.

Compliance with industry regulations and standards is another important reason why Security Monitoring is so important for businesses. Many industries and countries have regulations that require businesses to implement and maintain robust security measures, including Security Monitoring. These regulations may include data protection laws, such as the European Union's General Data Protection Regulation (GDPR), or payment card industry standards, such as PCI DSS. Organizations that fail to comply with these regulations can face significant financial penalties and damage to their reputation.

Additionally, Security Monitoring can provide organizations with the visibility they need to assess their security posture, identify areas for improvement, and implement best practices to reduce the risk of future attacks.

Customer Benefits

- Improve security posture through continuous monitoring and analysis
- Compliance with regulations
- Continuous improvement with latest technologies
- Have peace of mind knowing that the systems and data are protected against security incidents
- Access to a team of security experts who have the knowledge and expertise to keep the systems and networks secure

How CyStack Helps

The CyStack team is a highly skilled group of security experts with extensive experience in security operations. With a deep understanding of the latest security threats and technologies, we are well-equipped to help businesses in their Security Monitoring efforts.

CyStack provides a comprehensive solution including security incident response and ongoing Security Monitoring services via cutting-edge tools and methodologies thus helping businesses stay ahead of the curve in terms of their security posture. Our approach is designed to be flexible and scalable, ensuring that we can meet the needs of businesses of all sizes, regardless of their security requirements.

Methodology

The CyStack methodology in Security Monitoring is a comprehensive, multi-step approach that is designed to help businesses protect their digital assets and ensure the security of their networks and systems. This methodology includes the following steps:

1. **Assessment**: During the assessment, the CyStack team reviews the business's current security posture, including the existing security infrastructure, network configuration, and information security policies and procedures. This step provides valuable insights into the business's current security posture and helps identify any gaps that need to be addressed.
2. **Design**: Based on the assessment, we design a Security Monitoring plan that is tailored to the specific needs of the business. This includes selecting the appropriate security technologies, such as firewalls, intrusion detection systems, and log management solutions. The monitoring schedule and reporting requirements are also established during this step.
3. **Deployment**: The CyStack team deploys the security technologies and implements the monitoring plan. This includes installing security sensors, configuring log management solutions, and setting up real-time monitoring. The team also establishes communication protocols to ensure an effective and efficient incident response.
4. **Monitoring**: We provide ongoing monitoring of the business's network and systems, using a variety of tools and techniques to detect and respond to security incidents in a timely manner. This includes real-time monitoring, log analysis, and threat intelligence. The team also reviews security reports and updates the Security Monitoring plan as necessary to address new and emerging security threats.
5. **Incident Response**: In the event of a security incident, we will quickly identify the root cause of the incident, contain the incident, and resolve the issue. The team also communicates with the business to provide regular updates on the status of the incident and to ensure that the appropriate steps are taken to prevent similar incidents from occurring in the future.
6. **Reporting**: Experts from CyStack provide regular security reports to the business, which detail the security incidents that have been detected, the actions that have been taken to resolve them, and the overall security posture of the business. These reports help the client understand the security posture of their systems and provide valuable insights into the effectiveness of their security infrastructure.
7. **Continuous Improvement**: The CyStack team is committed to continuous improvement, regularly updates their Security Monitoring plan and incorporates the latest security technologies to ensure that they are able to deliver the highest level of managed Security Monitoring services. The team also provides training and support to the business to help them stay informed about the latest security threats and best practices.

Key Features

- Comprehensive assessment
- Tailored monitoring plan
- Deployment of best-in-class security technologies
- Real-time monitoring and log analysis
- Threat intelligence
- Incident response

Types Of Security Monitoring

CyStack supports the following types of Security Monitoring:

- **Network Security Monitoring**: This involves monitoring the network infrastructure, including servers, routers, switches, and firewalls. It is designed to detect and prevent security incidents, such as network intrusions, unauthorized access, and data breaches. To achieve this, Network Security Monitoring uses a range of technologies, including network intrusion detection systems (NIDS), network intrusion prevention systems (NIPS), firewalls, and others.
- **Endpoint Security Monitoring**: This involves monitoring individual endpoints, such as laptops, desktops, and mobile devices. It is designed to detect and prevent security incidents, such as malware infections, unauthorized access, and data breaches. To achieve this, Endpoint Security Monitoring uses a range of technologies, including antivirus software, firewalls, and others.
- **Application Security Monitoring**: This involves monitoring applications and software systems. It is designed to detect and prevent security incidents, such as software vulnerabilities, unauthorized access, and data breaches. To achieve this, Application Security Monitoring uses a range of technologies, including web application firewalls (WAF), vulnerability scanners, and others.
- **Cloud Security Monitoring**: This involves monitoring cloud-based infrastructure and applications. It is designed to detect and prevent security incidents, such as unauthorized access, data breaches, and misconfigurations. To achieve this, Cloud Security Monitoring uses a range of technologies, including cloud security posture management (CSPM), security information and event management (SIEM), and others.
- **Database Security Monitoring**: This involves monitoring databases and data stores. It is designed to detect and prevent security incidents, such as unauthorized access, data breaches, and data theft. To achieve this, Database Security Monitoring uses a range of technologies, including database activity monitoring (DAM), database security information and event management (SIEM), and others.
- **Compliance Monitoring**: This involves ensuring that the organization is in compliance with relevant security regulations and standards, such as PCI DSS, HIPAA, and others. To achieve this, Compliance Monitoring uses a range of technologies, including security information and event management (SIEM), vulnerability scanners, and others.
- **Insider Threat Monitoring**: This involves detecting and preventing security incidents caused by insiders, such as employees, contractors, and partners. To achieve this, Insider Threat Monitoring uses a range of technologies, including security information and event management (SIEM), user behaviour analytics (UBA), and others.

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