cyberlevel ins

CYBERONE SIEM

OVERVIEW

Today's networks are more complex than ever before, and protecting them from increasingly malicious and sophisticated attackers is a never-ending task. Organizations seeking to protect their customers' identities, safeguard their intellectual property and avoid business disruption need to proactively monitor their environment so that they can rapidly detect threats and accurately respond before attackers are able to cause material damage. **Security Information and Event Management (SIEM)** is designed to provide security teams with centralized visibility into enterprise-wide security data and actionable insights into the highest priority threats. As a first step, the solution ingests a vast amount of data throughout the enterprise to provide a comprehensive view of activ- ity throughout on-premises and cloud-based environments. As data is ingested, our solution applies real-time, automated security intelligence to quickly and accurately detect and prioritize threats. Actionable alerts provide greater context into potential incidents, enabling security analysts to swiftly respond to limit the attackers' impact. The SIEM agents run on many different platforms, including Windows, Linux, Mac OS X, AIX, Solaris and HP-UX. They can be configured and managed from the Security Operation Center (SOC) server.

HIGHLIGHTS

- Log and events data collection
- File and registry keys integrity monitoring
- Inventory of running processes and installed applications
- Monitoring of open ports and network configuration
- Detection of rootkits or malware artifacts
- Configuration assessment and policy monitoring
- Execution of active responses

PRODUCT FEATURES

SECURITY ANALYTICS

Lev Ins SIEM is used to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats and behavioral anomalies. As cyber threats are becoming more sophisticated, real-time monitoring and security analysis are needed for fast threat detection and remediation. That is why our light-weight agent provides the necessary monitoring and response capabilities, while our server component provides the security intelligence and performs data analysis.

INTRUSION DETECTION

SIEM agents scan the monitored systems looking for malware, rootkits and suspicious anomalies. They can detect hidden files, cloaked processes or unregistered network listeners, as well as inconsistencies in system call responses. In addition to agent capabilities, the server component uses a signature-based approach to intrusion detection, using its regular expression engine to analyze collected log data and look for indicators of compromise.

LOG DATA ANALYSIS

The SIEM agents read operating system and application logs, and securely forward them to a central manager for rule-based analysis and storage.The Cyber One SIEM rules help make you aware of application or system errors, misconfigurations, attempted and/ or successful malicious activities, policy violations and a variety of other security and operational issues.

FILE INTEGRITY MONITORING

Our solution monitors the file system, identifying changes in content, permissions, own- ership, and attributes of files that you need to keep an eye on. In addition, it natively identifies users and applications used to create or modify files. File integrity monitoring capabilities can be used in combination with threat intelligence to identify threats or compromised hosts. In addition, several regulatory compliance standards, such as PCI DSS, require it.

VULNERABILITY DETECTION

The SIEM agents pull software inventory data and send this information to the server, where it is correlated with continuously updated CVE (Common Vulnerabilities and Expo- sure) databases, in order to identify well-known vulnerable software. Automated vulner- ability assessment helps you find the weak spots in your critical assets and take correc- tive action before attackers exploit them to sabotage your business or steal confidential data.

CONFIGURATION ASSESSMENT

Cyber One SIEM monitors system and application configuration settings to ensure they are compliant with your security policies, standards and/or hardening guides. Agents perform periodic scans to detect applications that are known to be vulnerable, unpatched, or insecurely configured.

Additionally, configuration checks can be customized, tailoring them to properly align with your organization. Alerts include recommendations for better configuration, references and mapping with regulatory compliance

INCIDENT RESPONSE

Our product provides out-of-the-box active responses to perform various countermeasures to address active threats, such as blocking access to a system from the threat source when certain criteria are met. In addition, Cyber One SIEM can be used to remotely run commands or system queries, identifying indicators of compromise (IOCs) and helping perform other live forensics or incident response tasks.

REGULATORY COMPLIANCE

SIEM provides some of the necessary security controls to become compliant with industry standards and regulations. These features, combined with its scalability and multi-platform support help organizations meet technical compliance requirements.

CLOUD SECURITY

SIEM solution helps monitoring cloud infrastructure at an API level, using integration modules that are able to pull security data from well known cloud providers, such as Amazon AWS, Azure or Google Cloud. Cyber One SIEM provides rules to assess the configuration of your cloud environment, easily spotting weaknesses. In addition, SIEM lightweight and multi-platform agents are commonly used to monitor cloud environments at the instance level.

CONTAINERS SECURITY

Cyber One SIEM continuously collects and analyzes detailed runtime information. For example, alerting for containers running in privileged mode, vulnerable applications, a shell running in a container, changes to persistent volumes or images, and other possible threats.

ABOUT THE SOC

Our SOC is 100% focused on cybersecurity. In fact, that's all we do. We are fully committed to combating cyber threats to ensure that our customers are fully protected.

Our specialists monitor more than 1,000 cyber threats every day. By investing in the best technology and the brightest geniuses in the industry, we provide effective detection, analysis and response to cyberattacks. This means that we identify the attack as it occurs and take the right steps to eliminate the risk to you and your information systems.

CONTACT DETAILS

If you are interested in learning more about Cyber One SIEM please reach out to us by phone or email and one of our experienced sales people will take the time to answer any questions you may have.

Phone: +359 8999 862 47

Mail: office@cyberlevelins.com