CLONE SYSTEMS®

1.800.414.0321 CLONE-SYSTEMS.COM

Conduct real-time analysis of threats by correlating log data from your network and security devices with **Clone Systems'** Security Information and Event Management (SIEM) with Endpoint Detection and Response (EDR)

SECURITY INFORMATION AND EVENT MANAGEMENT

POWERING CLONE GUARD® SECURITY PROTECTION

Optimizes your security intelligence to help prioritize security team resources so they can focus on unique threat patterns that could negatively impact your security posture

- Correlating historical and real-time security information and events to identify patterns and trends to help prevent emerging threats before they occur
- Analyzing correlated events to investigate suspicious activity and determine the level of potential risk to the business
- Active threat intelligence consistently updated from multiple internal/external security sources
- Security Analytics collects, aggregates, indexes and analyzes security data, helping the SOC detect intrusions, threats and, behavioral anomalies
- Cloud Security monitors 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. In addition, rules are set up to assess the configuration of your cloud environment, easily spotting weaknesses
- Containers Security provides security visibility into your Docker hosts and containers, monitoring their behavior and detecting threats, vulnerabilities, and anomalies. It also continuously collects and analyzes detailed runtime information

Maximizes your team's visibility of correlated events by providing additional insights and expertise that facilitates a deeper level of troubleshooting and resolution

- Monitoring and alerting to identify events that require additional investigation by your team in collaboration with our security experts
- Security Operation Center monitoring and analyzing your correlated events to identify and triage event patterns, and provide guidance and escalation 24/7/365
- Unified reporting of correlated security events occurring on your network
- Intrusion Detection the EDR agent scans the monitored systems looking for malware, rootkits, and suspicious anomalies. It can detect hidden files, cloaked processes or unregistered network listeners, as well as inconsistencies in system call responses

1.800.414.0321 CLONE-SYSTEMS.COM

Conduct real-time analysis of threats by correlating log data from your network and security devices with **Clone Systems'** Security Information and Event Management (SIEM) with Endpoint Detection and Response (EDR)

Aggregate and quickly analyze your essential security logs with Endpoint Detection and Response

- Log collection and storage with powerful parsing, classifying, and categorizing capabilities to allow you to easily identify vulnerabilities in your environment and capable of scaling as you grow
- File Integrity Monitoring the EDR agent monitors the file system, identifying changes in content, permissions, ownership, 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
- Vulnerability Detection the EDR agents pull software inventory data and send this information to the SIEM, where it is correlated with continuously updated CVE (Common Vulnerabilities and Exposure) databases, in order to identify well-known vulnerable software and operating system issues
- Real-time search and analysis capabilities streamlining your ability to troubleshoot and perform postmortem analysis and forensic investigations

With enhanced visibility and access to relevant log information, you can expedite troubleshooting, remediation, compliance, and audit requirements

- Maintain compliance with industry standards and regulations
- Detailed reporting of all security related logs for any device and endpoint on your network