

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Powered by Clone Guard®

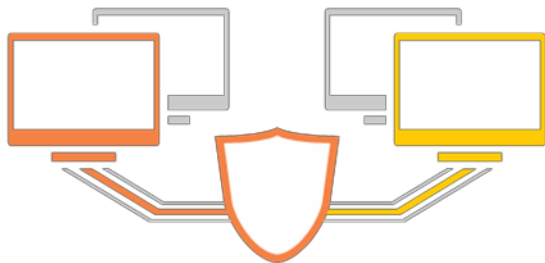


Security Information
and Event Management

Conduct real-time analysis of threats by correlating log data from your network and security devices with CNI's **Security Information and Event Management (SIEM)**

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



Maximizes your teams 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

*Requires Log Management

Call CNI Inc at 610-584-8040