FLEXINNOVO
flexible innovations

SIEM-Novo

SECURITY INFORMATION AND EVENT MANAGEMENT

Comprehensive security monitoring, threat detection and response solution establishing main component of security operation center.

MODULES

- Event management and correlation
- Incident analytics.
- Anomaly detection.
- Case management.
- Threat intelligence.
- Asset vulnerabilities management.
- Network discovery.
- Flexible and rich. reporting.
- Built-in and user defined dashboards.

SPECIFICATIONS

- Modular components.
- Scalability, clustering and load balancing.
- Automated installation.
- Docker support.
- Easy configuration.
- User friendly.

DIFFERENTIATION

- Flexible and efficient parsers.
- Variety of data sources.
- Agent and agentless.
- Legacy systems.
- Rules and events correlation.
- High through output.
- Flood protected.
- Cross devices and data.
- Instant alerting.

MAIN FEATURES

- File integrity monitoring.
- Integration with MITRE ATT&CK and MISP.
- Regulatory compliance (PCI DSS, GDPR, NIST 53-800, GPG13, TSC SOC2, HIPAA, …).
- Security configuration assessment.
- Built-in vulnerability scanning engines and support for external engines.
- Case management and follow up of suspicious security incidents.
- Multiple security analysers for variety of observables.
- Chart rich reports.
- Exporting reports in multiple formats (csv, pdf and html).
- Intrusion detection and NIDS integration.