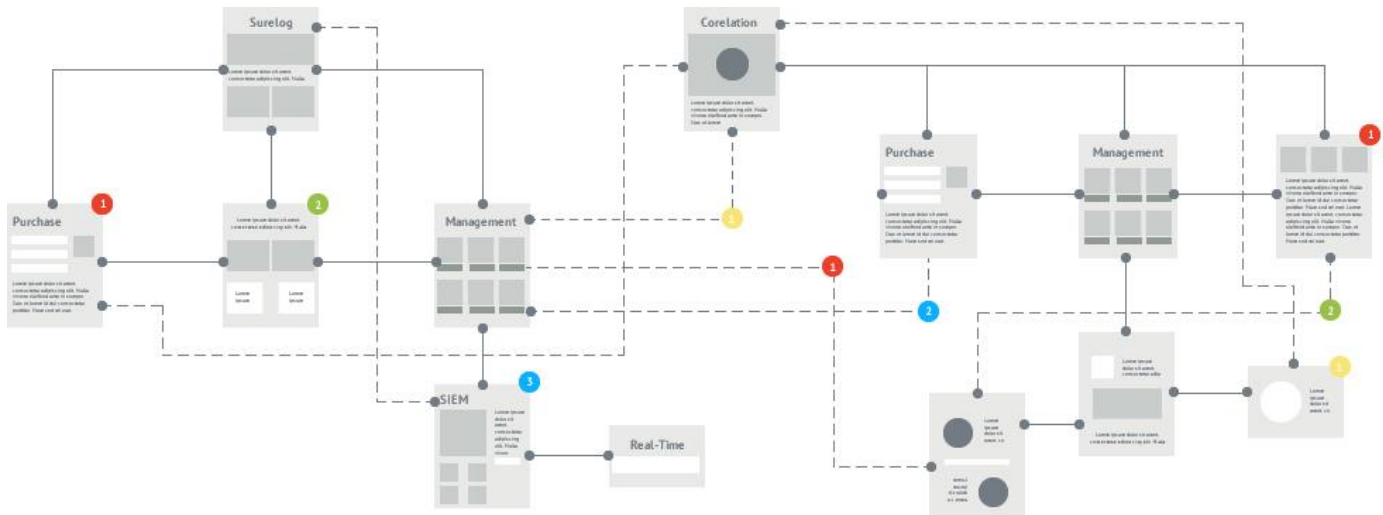


# Surelog Details



- Cost-effective Security Information and Event Management (SIEM) software
- Real-Time Event Correlation
- Log Search
- Real-time Alerting
- Dashboard and User based Views
- Automates the entire process of managing terabytes of machine-generated logs
- Agent-less log analytics software for network security devices
- Collects, archives, and analyzes security device logs and generates forensic reports from a central console
- Provides end-point security monitoring and analysis, employee Internet monitoring, and bandwidth monitoring
- Supports capacity planning, policy enforcement, security, and compliance audit reporting
- Works with open source and commercial network firewalls (Check Point, Cisco, Juniper, Fortinet, Snort, and more) and IDS/IPS
- Supports VPNs, proxies, and related security devices
- Collects, analyzes, searches, reports, and archives from a central location
- Reports on user activity, regulatory compliance, historical trends, and more
- Conducts log forensics analysis, monitors privileged users, and ensures compliance with regulatory bodies
- Agent-less Log Collection
- Agent based Log Collection
- Log Search
- Log Analysis
- Log Archiving
- Log Forensics
- Importing Event Logs
- User Authentication
- Ready-built EventLog Reports
- Custom EventLog Reports
- Microsoft Internet Information Services (MS IIS) Server Log Reports
- VMware Server Log Management Reports
- Active Directory Log Reports
- Privilege User Monitoring (PUMA) Reports
- User Session Monitoring
- Event Log Reports
- Historical Event Trends
- Advanced Search Result as Report Profile
- Microsoft IIS Web server application
- Microsoft IIS FTP server application
- DHCP Windows application
- DHCP Linux application
- MS SQL database application
- Oracle database application (Audit)
- Apache web server application
- Print server application
- Windows Terminal Server Log Monitoring
- Custom Reports
- Scheduled Reports

