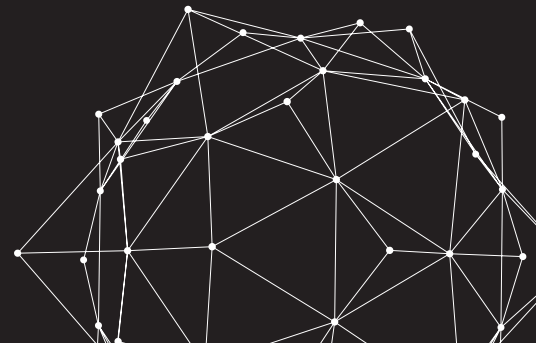
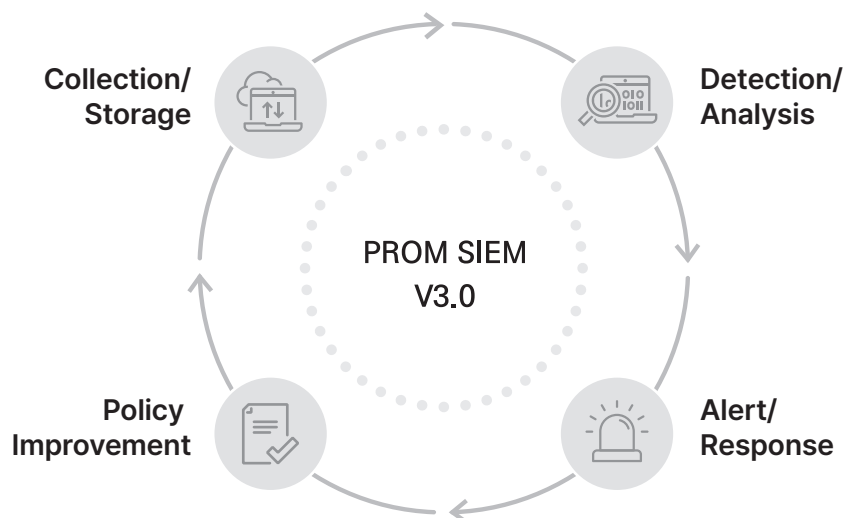


PROM SIEM V3.0



Product Overview

PROM SIEM V3.0 is an important security product designed to enable companies to effectively monitor, analyze, and respond to security alerts. PROM SIEM V3.0 plays a role in collecting and analyzing various IT assets and security data to detect and alert security threats in real-time. PROM SIEM V3.0 plays an essential role in protecting the organization's IT infrastructure and simplifies threat management in complex security environments.



Special Features



Optimized Integrated Security Management

- Unified Management of Diverse Security Systems and IT Assets
- Structured/Unstructured Data Management



CEP Analysis and Big Data Processing

- Real-Time Event Detection
- Big Data Processing with NoSQL Integration



User-Centered UI

- Customizable User Dashboard
- Intuitive Log Search Interface with Simplified Queries



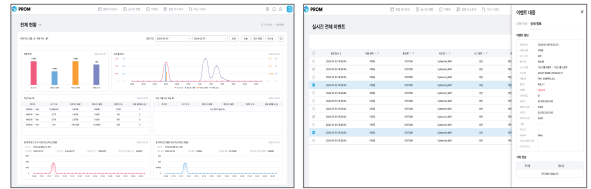
Efficient Log Management

- Logs Compressed by Over 70%
- Log Lifecycle Management from Collection to Deletion

Main Functions

Real-Time Event Detection

- Applying an In-Memory-Based Real-Time Event Detection Engine
- Scenario-Based Correlated Event Detection



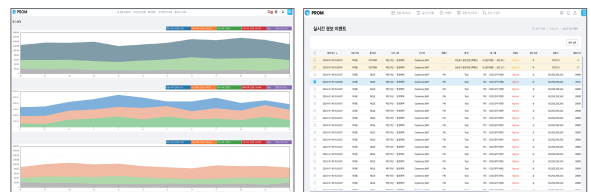
Threat Analysis Dashboard

- Security Threat Landscape Categorized by Attack Types
- Attack Map Based on GeoIP
- Customized Dashboard Based on Customer Environment



Various Analysis Functions

- Trend Charts/Single Analysis /Composite Analysis
- Time Series Analysis Function



Implementation Effects

PROM SIEM is a product designed to provide specialized monitoring services based on CyberOne's accumulated operational experience, offering an optimized functional framework. Through the introduction of PROM SIEM, organizations can swiftly respond to cybersecurity threats and comprehensively enhance their cybersecurity stance.



Threat Detection and Response

- Collects and analyzes security events and log data in real-time
- Detects threats in advance by identifying not only known threats but also abnormal behavioral patterns



Compliance and Regulation Adherence

- Automatically collects and archives necessary logs through SIEM to support audit readiness for regulatory compliance
- Simplifies incident investigations and reports processes based on logs and records through SIM when security incidents occur



Cost Reduction

- Cost savings possible through effective threat detection and response via SIEM
- Cost savings in labor and other associated expenses through automation and efficiency improvements



Efficient Security Operations

- Reduces manual workload through automated alerting and reporting functions
- Provides immediate situational awareness with various dashboards