Cybersecurity & Safety of >200M Residents

Across All Major Metros and Thousands of Critical Locations

Objective: Monitoring & Remediation of any safety and security issues for citizens across thousands of critical locations

State leadership has a vision of providing safety and security to its hundreds of millions of residents and visitors to its top metros and thousands of locations visited by thousands of people each day. Execution of a project like this requires the right combination of infrastructure and platform, one that scales and offers high availability and seamless failover. Seceon aiSIEM and aiXDR platforms were selected to bring modern cybersecurity to this project for the following reasons:

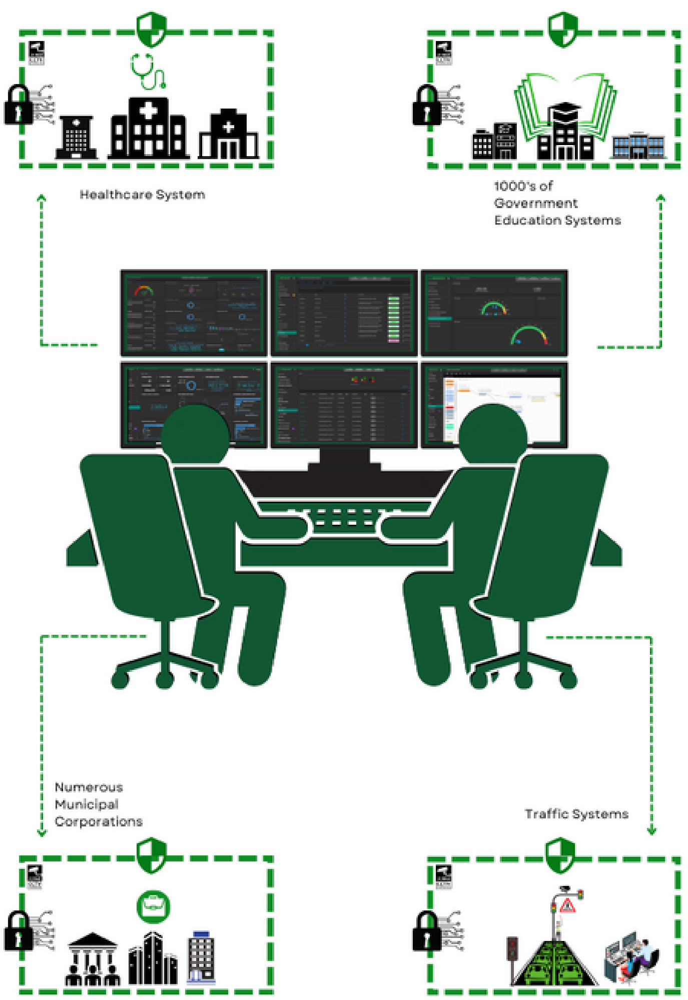
- Monitoring all activities across thousands of locations in real-time
- Visibility of all activities across all locations
- Using context and situational awareness to detect threats and breaches to take actions in real-time
- Single source of truth for all the activities and auto-correlation of data collected from different sources offering logs, flows, and identities
- Detect the threats and malicious activities in their early stages and take automated as well as playbook-based actions to eliminate the threats
- Platform with all the evidence for compliance and forensic analysis

Cybersecurity with aiSIEM and aiXDR

Unlike NG-SIEM (Next Generation SIEM) solutions, Seceon's aiSIEM relies on behavioral anomaly detection, dynamic threat models, and AI to detect threats in the early stage of an attack and provides automatic or playbook-driven responses for remediation to keep the organization safe from data breaches.

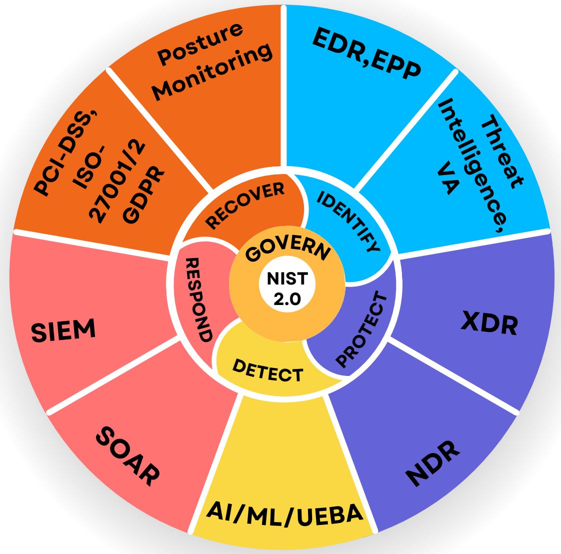
- Seceon aiSIEM and aiXDR solutions eliminated the need for silos and point-solutions like NG-SIEM, SOAR, NDR, UEBA, NBAD, IDS, EDR, NG-AV, DLP, etc., and a single platform offered "Modernization of Cybersecurity for the Digital-Era" and cybersecurity EFFICACY and EFFICIENCY when dealing with billions of events daily to surface meaningful alerts.
- aiXDR raw telemetry correlation in aiSIEM provides options to perform threat hunting across thousands of locations automatically and eliminate malicious activities and actions quickly.
- Network control policies and UDA were added to ensure suspicious activities are either eliminated or tracked over time.
- Playbooks are enabled for threat mitigation as well as threat hunting.
- Training of teams for playbook creation, threat hunting, compliance monitoring.

State Cybersecurity Monitored with Seceon aiSIEM & Seceon aiXDR


Healthcare System
1000's of Government Education Systems
Numerous Municipal Corporations
Traffic Systems

Mordernizing Cybersecurity with Seceon aiSIEM & aiXDR

1. Cybersecurity monitoring across thousands of locations with a single platform eliminates the need for 20+ silos and point solutions and their associated complexity and lack of common context.
2. Significantly reduced the risk of data manipulation, and improved public safety by quarantining suspicious users and hosts
3. Reduced unnecessary alerts (false positives) to a manageable number of alerts for detection and remediation.
4. Served as a deterrent for potentially malicious insiders and careless users.
5. Notifies SOC Analysts and IT Management instantly upon policy violations to take action, including education of the workforce, and third-party contractors.
6. Full transparency is provided for every alert and threat indicator with the flexibility to add organizational intelligence.
7. Significantly lowers TCO



As one of the project leaders noted – "We were presented to by multiple global leading vendors that to meet our requirement, we need multiple products and one year of integrations and showed us that all of our requirements can professional consulting engagements. Seceon team and its partner handled with a single platform and implementation happened within a week with operations going live within 2 weeks.
Our reaction was "no way possible because others asked for 6 months to a year." After a reference check, we selected Seceon and we are happy that we made that choice because Seceon delivered more than what was promised."

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 400 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 7,600 clients.

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/