A Leading Global Financial Institution Case Study

A prominent BFSI leader, part of a global entity operating in 64 countries, with a team of over 184,000 professionals worldwide.

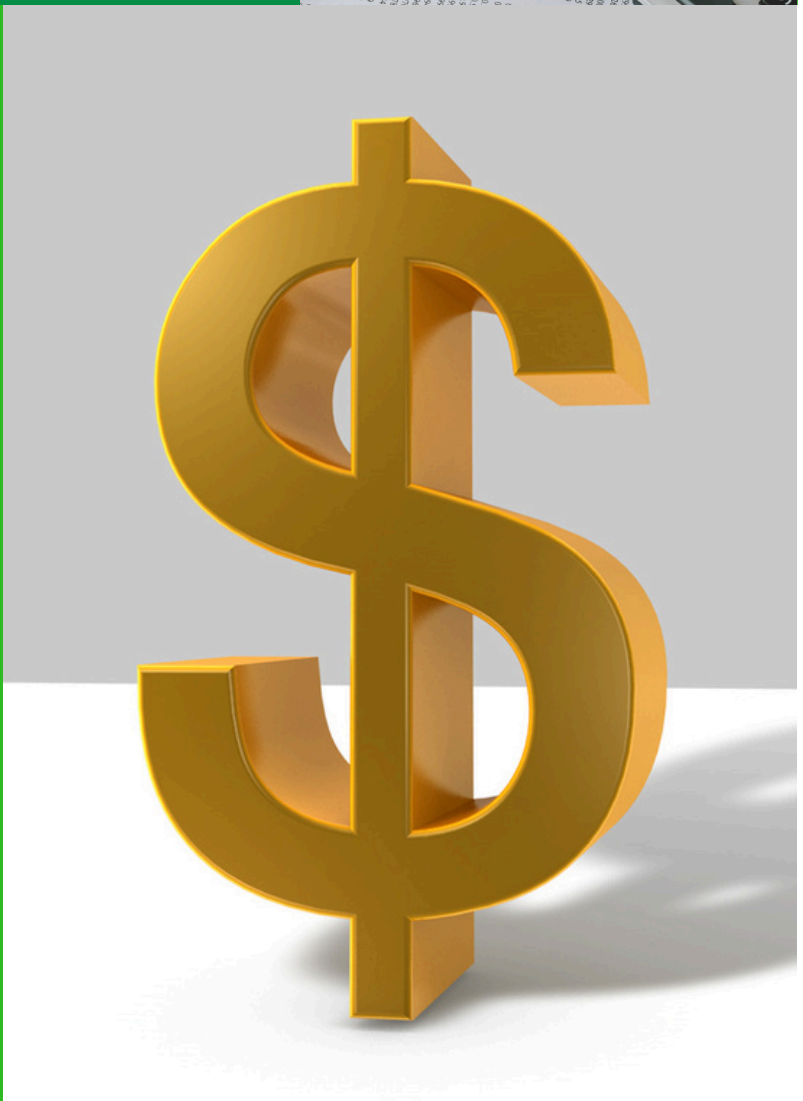
Present Scenario: Financial Institution using OpenText™ ArcSight™ Enterprise Security Manager (ESM) SIEM tool.

Limitations:

1. Limited functionality/capability
2. Limited automation and AI capability
3. Lack of context and situational awareness
4. Numerous manual processes
5. Limited third-party asset integration capability
6. Steep learning curve
7. Resource intensive
8. High cost
9. Performance issues

Impact: Affects overall efficiency and cost-effectiveness, especially in environments with limited resources or expertise.

Decision: Move from a technology-based approach to a platform-based approach/advanced aiSIEM with detection, remediation, contextual awareness, automation, and ROI. Customer evaluated Seceon Platform, Rapid7, Splunk, Securonix & Palo Alto XSIAM.



Objective:

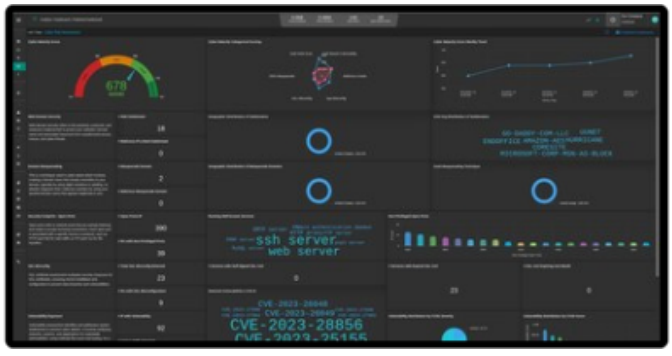
Secure critical assets and entire infrastructure, meet Compliance and Regulatory framework for Cyber Security, Cyber Resilience compliance and Incident response and intellectual property.

1. Transitioning from the current ArcSight SIEM to cutting-edge technologies or a new AI SIEM platform
2. Insufficient contextual information and the inability of analysts to maintain situational awareness significantly prolong both the mean-time-to-detection (MTTD) and mean-time-to-response (MTTR) for cyber threats.
3. Outdated cybersecurity point solutions were limited in scope, addressing only fragments of the issue, while lacking comprehensive context and correlation capabilities creating too much noise and false alerts.
4. Organizational expansion, transformation initiatives, and partner system access the potential for access privilege misuse as well as cyber threats.
5. To meet the Securities Exchange Board of India compliance requirements

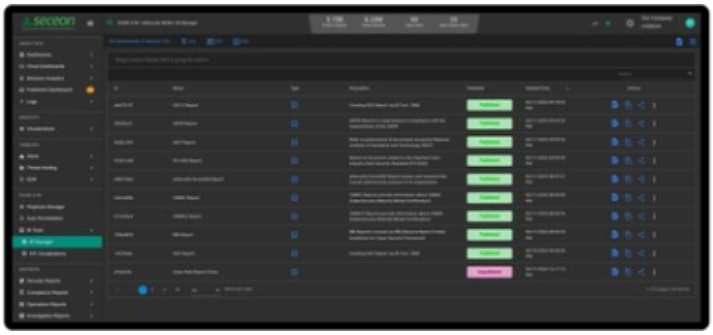
Seceon solution with aiSIEM and aiSecurity BI360

Unlike NG-SIEM (Next Generation SIEM) solutions, Seceon's aiSIEM leverages behavioral anomaly detection, dynamic threat models, and AI to identify threats at the nascent stages of an attack. It provides automated or playbook-driven responses with remediation to safeguard the organization from data breaches. Post-deployment, the machine learning algorithms required a few weeks to establish a baseline pattern, which subsequently auto-tuned the detection models.

1. Following implementation, Seceon identified numerous hygiene issues, misconfigured critical assets, and pre-existing incidents. These were swiftly addressed by the networking, IT, and security teams, significantly enhancing the organization's cybersecurity posture shortly after deployment
2. The Seceon aiSIEM platform was configured for auto-remediation on several critical attack vectors, with alerts established to proactively safeguard the organization against data breaches and malicious activity.
3. Network control policies and custom alerts are configured based on customer-specific conditions.
4. Multiple compliance monitoring reports were created to ensure continuous compliance management and reporting.
5. aiSecurity BI360 enables customers to ascertain their organization's current security score by evaluating critical factors such as dark web scans, CVE vulnerabilities, malicious assets, application misconfigurations, SSL misconfigurations, and DNS masquerading.
6. Faster MTTD and MTTR.



Seceon aiSecurity Score360 Dashboard



Seceon aiSecurity BI360 Report List

Noticeable Gains with Seceon aiSIEM

1. Achieve comprehensive cybersecurity across the entire organization with a unified platform, eliminating the complexity and contextual gaps associated with multiple point solutions.
2. Multilayered detection capabilities enable the team to monitor activities on a single screen, facilitating intelligent and actionable insights.
3. Substantially mitigated the risk of data breaches, operational disruptions, and downtime.
4. Automated Threat Hunting and Investigation: The Seceon platform helps threat hunting team by automating the process, alleviating the workload on security analysts. It seamlessly correlates data, prioritizes alerts, and delivers actionable insights, thereby streamlining incident investigation
5. Highly mature Artificial Intelligence, Machine Learning, and behavioral analytics empower us to identify critical activities and uncover additional insights that were not evident in many competitive technologies we have evaluated
6. Minimized false positives, streamlining alerts to a manageable volume for effective detection and remediation.
7. Functioned as a strong deterrent against malicious insiders and negligent users.
8. Notifies SOC Analysts and IT Management instantly upon policy violations to act, including education of the workforce, third-party contractors, and partners.
9. Complete transparency is ensured for every alert and threat indicator, with the added flexibility to incorporate your organization's proprietary intelligence
10. Substantially reduces total cost of ownership (TCO) while deploying a state-of-the-art cybersecurity program.

Customer Voice:

1. Thousands of assets were onboarded within a week with the platform showing comprehensive visibility of all the assets and making multi-layer security a reality with correlations across all the telemetries. Playbook has already been deployed for multiple types of alerts and use cases and continuous compliance is seen in actions.

2. **Saving 82.30% of CAPEX and OPEX and realizing of "Modernization of Cybersecurity for the Digital Era"**

3. Innovation roadmap and continuous process improvement in place to continue driving security posture improvement and risk reduction.

About Seceon

Seceon enables MSPs, MSSPs, and IT teams 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 augments and automates MSP, MSSP, and IT security services with an AI and ML-powered aiSIEM and aiXDR platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time with threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 624 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 8,200 clients.

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/