GRAMAX
CYBERSEC
A GAR AERO SERVICES INITIATIVE

CASE STUDY

AI/ML Based Behaviour Anomaly Detection

EXECUTIVE SUMMARY

GRAMAX Cybersec is one of the leading cybersecurity services providers in the market and works with global customers across industries ranging from BFSI, healthcare and education to aviation, energy & utilities, defence, etc. The company was recently contacted by an organization actively working in the critical infrastructure sector, who was looking to devise innovative strategies and solutions, and swiftly detect & respond to real-time information security anomalies and events. The customer wanted to build an effective security mechanism that can detect threats arising from suspicious behaviour or patterns.

CHALLENGES FACED BY THE CLIENT

01 Shortage of the right talent

02 Too many false security alerts

03 Lack of comprehensive visibility

04 Lack of automation & integration

05 Lack of proactive threat detection capability and auto containment of any threats in real-time

HOW GRAMAX CYBERSEC HELPED

GRAMAX recommended the organization to go with Seceon aiSIEM solution that addresses all the pain points and offers comprehensive threat detection. Seceon aiSIEM platform is unique as it combines traditional SIEM functionality with user, application, host and network behavioural analysis, Threat Intelligence (TI) and Vulnerability Assessment (VA) results, leveraging Machine Learning (ML) algorithms and Artificial Intelligence (AI) techniques to automate threat detection, alerting and response in a single powerful platform.

ABOUT THE SOLUTION – SECEON AISIEM

Seceon's aiSIEM can be broken down into three core components, all of which run on Linux CentOS

01 Collection and Control Engine (CCE)

02 Analytics and Policy Engine (APE)

03 Long Term Storage (LTS)

aiSIEM is designed to ingest feed from logs, network flows, Windows events and a variety of other sources. User behaviour and global threat intelligence is applied to build dynamic threat models, leveraging ML/AI to arrive at the final outcome - intelligent decision making, actionable threat indicators and compliance checks and balances. The final decision is then executed as described in the Decision Flow Architecture. The solution also stores the raw logs in the LTS

"Seceon aiSIEM threat intelligence feeds" constitute more than 70 different highly trusted, reliable and reputed sources. We have thoroughly vetted these threat feeds to ensure the accuracy and reliability of information they provide. The threat feeds are produced by NSA (United States National Security Agency), highly reputed Honeypots, and industry shared intelligence. Seceon's Theat Intelligence Service refreshes threat feeds once every few hours and delivers latest updates to Seceon aiSIEM platform to enrich the security posture of customers. Insights drawn from such information can relate to URL Reputation, Bad Domain, Geo Location, Suspicious BotNet channel etc.

It also ensures that the feeds are filtered, de-duplicated, and reputation scores are assigned to each entry in the threat feed using our proprietary algorithm. Reputation score assigned to each item in the threat feed plays a significant role in estimating the alert confidence score and severity.

Apart from standard threat intelligence, Seceon's aiSIEM also offers the ability to integrate with 3rd Party Threat Intelligence sources using STIX/TAXII protocol. Subsequently, events associated with these sources can be identified.

Key benefits of this platform include:

01 Reduces Mean-Time-To-Response (MTTR) with Automatic Threat Remediation in Real-time

Seceon aiSIEM performs automatic threat containment and elimination in real-time. It also provides clear actionable steps to eliminate the threats that can either be prompted automatically by the system or manually by the security expert post-analysis.

02 Reduces Mean-Time-To-Identify (MTTI) with Proactive Threat Detection

Seceon aiSIEM proactively manages threats in real-time without an agent or alert fatigue. It performs threat management across the cloud, on-premises, and hybrid environments for MSSPs and Enterprises.

03 Continuous Compliance and Monitoring (Security Analytics)

Seceon aiSIEM provides continuous compliance and scheduled or on-demand reporting for HIPAA, PCI-DSS, GDPR, NIST, ISO and many other similar regulations.

04 Comprehensive Visibility of all assets, flows, applications and their interactions

Ingests raw streaming data (Logs, Packets, Flows, Identities), enriches and extracts meaningful features to provide real-time view of all assets (users, hosts, servers, applications, traffic) that are on premise, cloud or hybrid. The solution provides a single pane of glass view for all events and incidents across the organization and provides real-time analysis and reporting.

05 Automatically discovers and reports on new assets in the environment

Automatically discovers new assets introduced in the environment, such as laptops, PDAs, mobile devices, lots etc. These are automatically monitored without any human intervention to ensure the comprehensive security of all assets in the environment. This not only helps the typical commercial environments but is extremely critical for university, sports arena, public places such as train stations and airports.

06 Flexible and Flexible and Scalable Deployment in Bare Metal, Cloud or HybridScalable Deployment in Bare Metal, Cloud or

The solution, wrapped in containers and database, can scale horizontally to accommodate growing requirements (EPS, hosts, servers, firewalls etc) of the customer and can be deployed on-premise (bare metal or virtual machine), in-cloud or hybrid using hardened Operating Systems. Initial sizing allows for 1.5 times the estimated data volume, thus allowing for increased events (beyond EPS limits). All data in transit is encrypted for safe storage and tamper prevention.

07 Reduces CAPEX / OPEX as licensing is based on the number of assets

Licensing is based on the number of critical and non-critical assets as opposed to the amount of data being ingested which enables low, fixed CAPEX/OPEX expenses.

08 Eliminates need for silo solutions (such as, UEBA, DLP, IDS, IPS, WASF)

Seceon aiSIEM platform assimilates events, network traffic data, environment information, user identity, process intelligence and 3rd party intelligence/alerts to process, correlate and apply behavioral analytics (ML based) along with dynamic threat models (AI guided), thus bolstering an organization's security posture comprehensively and eliminating the need to rely on siloed solutions.