HORIZON

aiSIEM™

Horizon Industries, Ltd. aiSIEM powered by Seceon, helps organizations visualize user activities, network traffic flows, anomalous behaviors, and host-based suspicious processes through a single pane of glass while ensuring cyber threats, exploits and attacks are detected early and accurately with automated intelligence, advanced correlation and real-time analytics. The solution empowers SOC analysts to respond to real alerts by cutting out the noise and providing a simplified path to threat containment and risk mitigation.

- Advanced event correlation (on-premise and cloud) and behavioral patterns with AI and Dynamic Threat Models
- Behavior base-lining and profiling for anomaly detection leveraging Machine Learning techniques
- Contextual enrichment with threat intelligence (70+ sources), vulnerability assessment and historical data
- Exhaustive reporting across several key areas - security, compliance, operations, and investigation
- Rules based policy creation, enforcement and notification for appropriate action and governance

Comprehensive Visibility

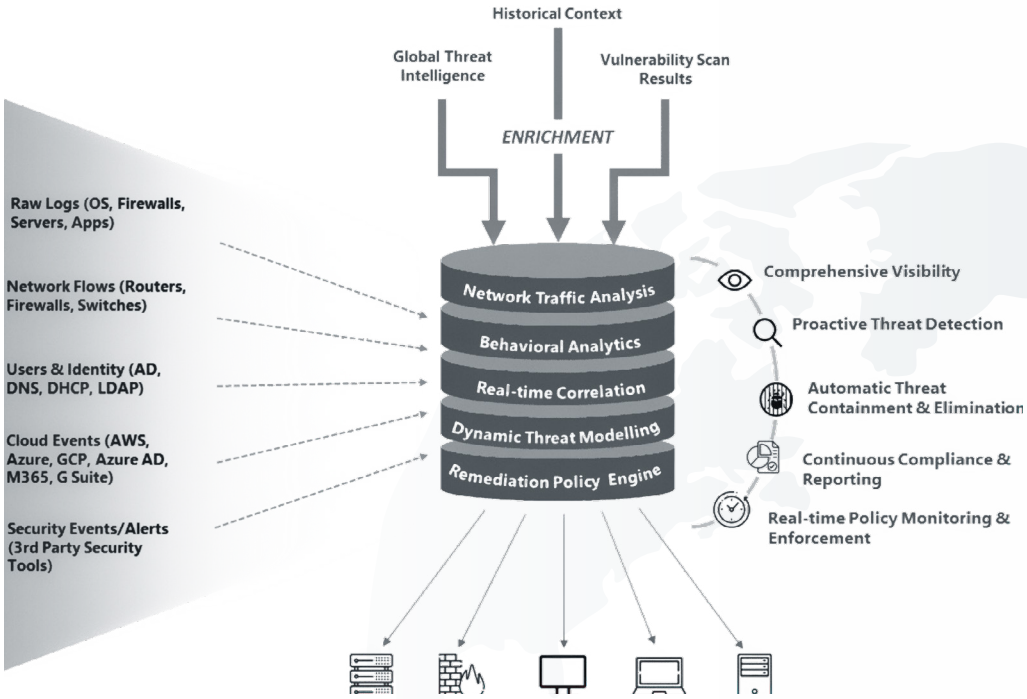
Uncover myriads of threat vectors lurking inside auto- discovered hosts, network, cloud, OT and IoT with 360° inference drawn from events, network traffic, packets, identities, and behavioral patterns.

Mean Time to Identify and Respond

Considerably shorten Mean-Time- To-Identify (MTTI) and Mean- Time-To-Response (MTTR) with automated threat detection and remediation in real-time and near real-time through registered alerts, critical and major.

Reduction in Operational Backlog and Human Error

Significantly reduce operational backlog and human error with Dynamic Threat Models and Advanced Correlation orchestrated through Artificial Intelligence, avoiding weeks of custom correlation, tuning,and human error.



Continuous Compliance

Ensure compliance 24x7 through regulation focused audit and reporting on PCI-DSS, HIPAA, NIST, GDPR and more, in addition to security posture, operations and investigations reporting.

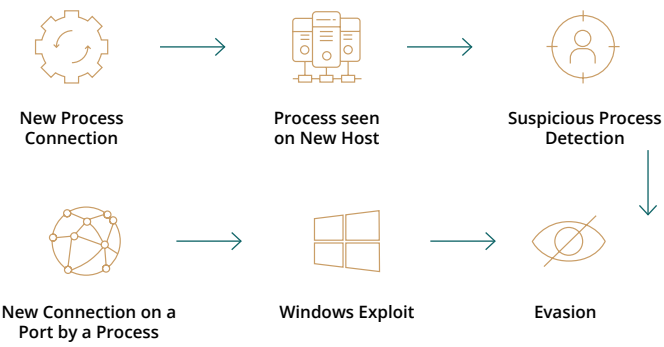
Accuracy and Speed

Gain edge over adversaries and hackers with real-time processing of big/fast data at speed, combined with behavioral anomalies and threat intelligence to arrive at validated threat indicators.

Scalability and Flexibility

Harness the power of flexible deployment through on-premise, cloud or MSP hosted solution spanning multiple sites – data center and branch offices – with multi-tenancy and data segregation at the core of platform architecture.

Malware Threat Detection
Automated with AI based Dynamic Threat Model



System Requirements

CCE: Virtual or Physical Machine with 4 Core CPU, 4 GB RAM, 256 GB HDD, 1 GigE
Network
Interface
APE: Virtual or Physical Machine with 32 Cores CPU, 128 GB DRAM, 2 TB NVMe SSD(30K/10K IOPS)
LTS: 40 TB HDD
CCE can be deployed on-premise (ideally close to the main network switch) or in cloud. APE and LTS are bundled together and hosted on-premise or in cloud.

Array of Use Cases and Threat Vectors Addressed by Horizon aiSIEM

Cyber Crime

Malware <> Ransomware <> Advanced Persistence Threats <> Botnet Detection <> Trojan Activity

Insider Threat

Malicious Insider <> Compromised Credentials <>Privilege Misuse <> Suspicious Login

DDoS

Application Layer <> Volumetric <> SYN-ACK Flooding <> Amplification Attacks

Web Exploits

SQL Injection <> Cross-Site Scripting <> Local File Inclusion <> Directory Traversal <> Remote File Execution <> Cross-Site Request Forgery

Brute-Force

Password Spraying <> Dictionary Attack <>Credential Surfing

Other

Data/IP Exfiltration <> IoT/IIoT Cybersecurity <> OT/ICS Cybersecurity

Key Technology Components of Horizon aiSIEM

Control & Collections Engine (CCE)

The CCE orchestrates collection of events and network flow data across assets deployed within the enterprise and cloud. It applies intelligent detection for enrichment of structured and unstructured data before routing to the OTM core through a secure connection.

Analytics & Processing Engine (APE)

The APE forms the core of aiSIEM, processing high- volume high-velocity data in real-time, while feeding threat intelligence, behavioral anomalies, historical context and vulnerability scan results to dynamic threat models running on AI and ML based engines.

Long Term Storage (LTS)

The LTS compresses, encrypts and stores log data – on- premise or cloud, for archival and compliance (upto 7 years). Forensic search can be conducted through simple queries and Boolean operations.

Dashboard: Get a summary view of Open/ Close Status, Top Alerts by ThreatType, Top Users and Hosts with Critical & Major Alerts.

Behavioral Analytics: Have a quick curate-dunderstanding of your user behavior - ranging from Abnormal Logins and File Access to potential Insider Threat activity and Brute Force attack.

Alerts Analysis: Understand the nature of alerts and underlying threat indicators, including assets and users impacted. Drill down further to look at the event or networkflow attributes (Source IP, Destination IP, Event Type, Timestamp, Process Name, etc.).

Threat Hunting: Dive deeper into threat indicators across various sources - network, host, device and ML - and drill down into the actual event with rich contextual data (Event Type, Source, Host, Destination, User Name etc) presented in easy-to-read format.

MITRE ATT&CK: Get a consolidated view of Tactics and Techniques adopted by adversaries, mapped into sub-techniques and threat indicators - offering granular details on underlying events.

Compliance Reporting & Audit: Stay current and stay informed with regulatory compliance check and balances all the time - PCI-DSS, HIPAA, NIST, GDPR etc - even as your business grows with users, assets and digital footprint.

Auto-Remediation: Define specific criteria for auto-remediation based on severity type,confidence level, security alert type and assetcategory, including action path (Firewall, NAC, EDR) and schedule, causing minimum disruption to business.

Provisioning & Administration: Set up Policy Controls, Application Constructs, Cloud Configuration, Asset Discovery, MFA, Encryption – through unified User Interface.

7 DAYS

Only Alerts that Matter

349,010,831
Events Analyzed

1/20

2,978,381
Threat Indicators Detected

1/5000

7
Critical & Major Alerts