Features of Zeron

EDR Features

Real time endpoint data collection agent for log-based data	✓
Automated Response and Ticketing system for alerts and response management	✓
Analytics and Response coordination and notification	✓
Forensics and Endpoint security for host and network-based architectures	✓
Security audit response in scalable architectures and incidents	✓
Remote management dashboard to easy monitor statistics and aspects	✓
Patch management and scheduling for hosts and network systems, workstations and appliances	✓
Intrusion Detection and Mitigation solution in scalable environments	✓
File Integrity Monitoring	✓
Configuration assessment for endpoints, workstations and networks	✓
Host based Intrusion Detection System	✓
Integrated Network based Intrusion Detection and Prevention System	✓
Integrated Aggressive and Advance Scans methods with home-built tool Sayonara	✓
OWASP Top 10 monitoring for web-based environments	✓
Data Leakage crawling for business asset storage and manipulation services	✓

Tactical Exploitation in domains of solutions and methods of business architecture	✓
Adversary Simulations for all round protection from potential threats and monitoring security	✓

SIEM Features

Log Collection, Monitoring and Analysis with Integrated display dashboard	✓
Log data management and retention with standard checks for adversarial behaviour	✓
Threat Hunting and anomaly detection	✓
Asset ownership and manipulation tracking for end user and management	✓
Incident monitoring, response and ticketing system	✓
User and Entity Behavioural analysis	✓
Automated threat alert ticketing with monitoring dashboard implementation for internal audit	✓
Defensive AI suggesting defensive measures against trained intrusions	✓
Compliance tracking for company integrated policies	✓
Health Monitoring - systems, endpoints, workstations and network	✓
Asset value and Business fallout tracking for recorded assets	✓
Visualization of security scores and company standpoints	✓
Security Event Correlation for ITOps and event management	✓
Incident timelines and recording	✓

Compliance Module

Compliance asset management for controls as per company	✓
Business revenue fallout tracking for PCI, PHI and PII asset control violation	✓

ISO 27001	✓
HIPAA	✓
PCI DSS	✓
NIST	✓
GDPR	✓

Attack Module

Automated Scanning Modules for Network vulnerability measure	✓
Adaptive data monitoring and scaling for small and large scale companies	✓
Web environment scan methods for security standard maintenance	✓
Crawling and simulation for information audit	✓
Flaw identity for vulnerability identification, mitigation and audit	✓
Adversary identification	✓
Activity monitoring as interactive real time dashboard statistics	✓
Source reporting	✓

Defence Module

Advance analytics and visualization solution for intrusion and activity	✓
Adaptive Defence methodologies for threat mitigation	✓
File activity monitoring and anomaly detection	✓
Updates and Patch monitoring with customization and scheduling	✓
Artefact recovery and forensics for assets and log data	✓

Integrated security for 3rd party integration and security upgradation	✓
Zero Trust Initiative as security standard for global approach	✓

Global Support & Service Offerings

Technical support by phone, web, and email	**Included**
In-product resource centre / Support portal access	**Included**
Standard 9x5 Support	**Included**
Enterprise Support 24x7x365	Available
Designated Technical Account Manager + Enterprise Support	Available
Vigilance Managed Detection & Response (MDR) Subscription	Available
Vigilance PRO MDR + DFIR Subscription	Available
ZERON Readiness Deployment	**Included**

We aim to make security simplified and available to all sections of the industry, starting from start-ups to enterprises.