ACSIA Product Features Overview

Overview

ACSIA is designed with a view of both offensive and defensive strategies, using the mentality and modus operandi of hacker methodologies and tools that can compromise security.

ACSIA offers an innovative approach to preventing cyber-attacks for enterprises. The product is a data-centric endpoint detection and response (EDR) system with predictive analytics powered by machine learning (ML) and artificial intelligence (AI).

It helps enterprises identify and repel cyber-attacks in real-time through its ability to detect offensive tools, pattern identification technology, and advanced correlation engine. It can detect hacking techniques in their very early stages, long before they become an offensive attack.

Moreover, it is user friendly, simple to deploy and intuitive to operate. It requires only basic IT skills.

What it does

- Assess and prioritise threats in Real-Time
- Analyse deep level log signals from within your infrastructure with our specialist algorithms which pick up the most advanced hacking techniques
- Send notifications through email or instant messaging solutions
- Simplify workflow associated with remediation actions
- Protect your systems against threats and automated botnets
- User behaviour analytics to protect from compromised identity and insider threats
- Detect and capture external threats and automatically mitigate
- Monitor system and application behaviour to capture malware and other malicious software
- Provides comprehensive feedback to users where an incident can be mitigated instantly
- Covers major compliances and regulations requirements

- Operates across distributed environments such as AWS, GCP, Azure and On-Prem...

Benefits

- Enhanced security detection and analysis capabilities
- Real time monitoring, control and analysis in one product
- Provides combined functionality previously only available through multiple solutions
- Enables enterprises to manage risk with fewer specialist staff, achieve better security outcomes and save money
- Does not disrupt business operations or degrade your network performance
- Simplifies workflows and alleviates “alert fatigue” and reduces time consumed by IT teams investigating false positives
- Simple UI - Deploy non-tech staff with basic training
- Immediate notifications and reporting to enable GDPR compliance
- Easy setup and deployment

For full details about ACSIA administration and Usage please refer to ACSIA Administration Guide or contact us at support@4securitas.com

4Securitas
65 Ivy Exchange, Parnell Street D01 AW68 Dublin
Registered in Ireland
CRO: 598914 VAT Number: 3463752OH
Contact: info@4securitas.com