

ACSIA OVERVIEW

This document provides an **overview** of ACSIA, its main features and the benefits to use it compared to other market products in the security area.

Overview

ACSIA implements a **real-time** all-in-one solution that **cut down on costs** but at the same time transforms your digital asset in a **safer environment**.

Even though it is hard to categorize ACSIA as it position itself between next generation cybersecurity solutions, formally it can be defined as a combinations of SIEM, IDS and IPS but in reality it is much more than that - ACSIA includes an automated interactive cyber security monitoring and cyber defence system.

But what does it mean?

- **SIEM Like:** it incorporates the Elastic stack log collector.
- **Automated:** the sort of work to investigate a threat or anomaly, dig into logs in deep search and remediate actions are fully automated by ACSIA.
- **Interactive:** it enables organizations to challenge malicious users by tracking them down, kicking them out and eventually banning them on a permanent basis.
- **Cyber defense:** it enables organisations to perform a security assessment on their IT assets and helps to reveal vulnerabilities in order to improve their security posture.
- **Cyber security monitoring:** it monitors your IT assets by capturing anomalies with its analytical engine and algorithms.

The implementation of our algorithms are based on Signature, Technique, Machine Learning and Artificial Intelligence concept that makes ACSIA a self-learning product.

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

Key Features

- Assess and prioritize 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
- **No disruption** to your business network or systems
- **Ease of deployment** in 3 simple steps
- **Email notifications** - with embedded remediation actions
- Free your systems from **botnets**
- **Optimize** cybersecurity posture
- Immediate notifications and reporting to enable **GDPR compliance**
- **Simple UI** - Deploy non-tech staff with basic training

ACSIA provides/offers:

- OS and app level **intrusion detection** for legit and non-legit access attempts
- OS and app level **intrusion prevention** for legit and non-legit access attempts
- **Real-time intrusion detection** using the log analysis and geo-location (no product can deliver this as of today)
- **Kernel level** anomalies detection
- **Fully container (LXC)** aware i.e. docker infrastructures
- **User activity analysis** (UBA) with machine learning and artificial intelligence
- **0-day vulnerability** through its unique log analysis mechanism that intelligently monitor and cross checks on multiple data sources
- Distinguishes compromised accounts with legitimate accesses and **notifies accordingly**
- **Kill connections** - this option allows you to shutdown/kill the malicious users during their attempt, before they succeed or do anything harmful
- **File integrity check**

- **Automated hardening** for each server environment and generation of a report/alert with recommendations and fixes (no product can deliver this as of today)
- **User session player** for internal auditing systems (the majority of hacks are actually internal data leaks) and constant monitoring

Benefits

- Addresses core Cybersecurity **issues**
- **Real time monitoring, control and analysis in one product**
- Combines many competitor product features in **one package**
- ACSIA allows customers to manage risk with **fewer specialist staff**, achieve better security and **save money**
- Does not disrupt business operations or buffer/slow your network
- **Simplifies Security** - alleviates 'alert fatigue' and reduces time wasted by IT team investigating false positives

ACSIA vs Competitors:

ACSIA distinguishes itself from other products as it is **real-time**, reduces false positives (>90% accuracy), detecting both manual and automated attacks, detecting account compromises and most importantly enables the user (owner) to mitigate, meaning, **fight back** and respond to a malicious user/attacker with its interactive future that **requires no particular skills**.

The features like “Kernel level analysis”, “User session player attached to notifications for internal users”, “User profiling” and “Automated event handling for the majority of incidents” are unique, just to list a few. Another unique aspect worth to mention is the one that identifies hacking techniques through our unique patterns designed in algorithms, where ACSIA does not need to have a database to compare but it has the ability to recognize hacking techniques prior to knowledge (without having a database of techniques).

Current cyber defence/threat solutions are analyzing every type of logs and traffic, this requires time and lots of dedicated resources (both human and equipment). ACSIA analyses specific security related logs and knows what to look for, therefore, it can analyse with more accuracy and efficiency with no additional resources and in timely manner.

ACCSIA monitors and captures anomalies with auxiliary of algorithms that recognises from the simplest to most advanced intrusion/exploitation techniques. These anomalies are profiled via it's reinforced learning machine concept and ultimately trigger alerts and dispatches notifications by severity level (decision making) thanks to its AI principle based algorithms.

Alerts and notifications are transmitted in plain english to receivers where within the email alert it gives the ability to interact, therefore challenge back the malicious user (attacker) via it's so called immediate actions.

Support and Licensing:

Platform supported:

ACCSIA supports Linux systems predominantly but it also has windows implementation as clients to be connected and the details provided within user administration and installation guide.

Support:

We operate in continuous development mode, our product is **continually updated** so that all users can benefit from the latest improvements and upgrades.

Our team is available to support our Enterprise Clients, with full multi-lingual support from our headquarters in Dublin, the Silicon Valley of Europe.

Licensing:

Our software is sold on a 1 year/annual renewable licence. Full support for 1 year is included.

With an active community, free documentation and plenty of video training and educational courses available, 4Securitas.com offers resources to help you make the most of your ACSIA license.

Visit <https://4securitas.com> main site for details and pricing, the main blog where we publish some use cases at <https://blog.acsia.io> and the media web site <https://media.acsia.io> where you can find some videos introducing ACSIA.