Take charge of your security with ACSIA real-time threat intelligence cyber defense system.

FAQ's

Q1: Why do I need ACSIA, our firm has already invested in security products to protect the perimeter of our IT environments. These products are designed to protect the network and some endpoint devices and include products such as Splunk, Palo Alto, McAfee?

A: The traditional model of network security has been designed around perimeter security. This model i.e. a high fence, while still relevant does not offer full protection as methods of attack have become more refined and ingenious, including social engineering and insider threats.
An emerging requirement is for an extra layer of security monitoring protecting the data itself, typically this data is housed in key assets such as servers (apps, databases backups,storage).
Despite perimeter security products working very well at the external attack surface, their analytical capabilities are limited. The level of refinement with a solution is limited to specific functions - limited with what and how they interpret the security threat.
Whereas when looking at the data layer, a different story emerges. The level of analysis from the data in its own right, yields higher quality data for security analysis.

Value of assets and our dependence on our digital estate has become total, the need for highly focused risk mitigation strategies has also increased. Defense in depth suggests a greater eco system of security products and services.
ACSIA can sit at the core of such an ecosystem.

Most of the significant data breaches of recent years have all occurred where organisations have relied exclusively on a perimeter security model.

ACSIA (Automated Cybersecurity Interactive Application) is a '*post-perimeter*' security tool which complements a traditional perimeter security model. ACSIA resides at the Application or Data layer. These platforms (physical/VM/Cloud/Container) are the ultimate target of every attacker.

Q2: What is the architecture of a standard ACSIA deployment?

A: The ACSIA engine is provided on a subscription basis, and can be deployed on physical/VM/ Cloud/Container platforms. ACSIA supports both windows and linux operating systems. The ACSIA core engine needs to be hosted on a dedicated VM from which it monitors all connected clients. See also, ACSIA Design and Architecture Overview document.

Q3: How long does it take to deploy ACSIA in a typical installation?

A: The ACSIA engine deploys in under 15 minutes on physical/VM/Cloud/Container platforms. ACSIA is simple to deploy and does not require any complex tuning or input of rules or policies.

Q4: Is ACSIA a SIEM product?

A: In order for ACSIA to analyze server logs in real-time it has to have all logs centralized in one place and therefore it needs a SIEM. Therefore ACSIA comes with its own SIEM however ACSIA is not primarily designed as a SIEM product.

ACSIA utilises multiple threat intelligence and detection features. These include log analysis, signature recognition, patterns types, machine learning, Artificial Intelligence, UEBA, correlation and profiling algorithms - a different design concept to existing solutions.

Q5: What Operating systems are ACSIA compatible for monitoring?

A: ACSIA can monitor Windows and Linux as well as Containers.

Q6: Our company already uses X Technology to collect logs. Can we use ACSIA alongside this?

A: ACSIA can be used as an add to your existing cyber security suite or as a standalone product.

Q7: What format of log files does ACSIA accept?

A: ACSIA reads standard system and the most popular web application logs.

It could be the case that a client has developed a custom webapp with a custom log format. For this to be monitored by ACSIA we can provide support to integrate the log ingestion - within a very short time.

Q8: We have a lot of servers/platforms - 1000's - all over the world. Can ACSIA scale to this degree?

A: Yes - one of ACSIAs core strengths is scalability. As a rule of thumb, one ACSIA deployment can support up to 200 physical, virtual, cloud or container infrastructures. ACSIA can scale beyond 200 servers, 4Securitas professional services will engage with organisations where specific configurations are required.

Q9: Will ACSIA interfere with my existing systems and network performance?

A: No, ACSIA does not interrupt or imbalance in any way with any systems/processes or infrastructure. The network performance impact is virtually zero.

Q10: Will ACSIA make decisions and disrupt my business based on false positives/ negatives?

Until ACSIA is 100% sure that what has been detected is an actual threat it will not automate a response. Instead it will dispatch a notification requiring user input to make that call.

Q11.Will ACSIA generate a lot of notifications that require user input?

Typically the split between automatically actioned threats to user input is 95% : 5%.
This 5% also reduces every time the user input occurs and the engine refines its detection capabilities.

Q12: If I receive an ACSIA alert, what should I do next?

A: Uniquely ACSIA monitors for anomalous behaviour and will provide detailed guidance on the nature of the threat - what it means, where it came from and how to deal with it - all in real time.

Q13: Does ACSIA offer the ability to take immediate action on attacks?

Yes, ACSIA gives your full visibility on incidents not automatically handled by ACSIA to take action and enables the most appropriate remediation action to be taken in real time.

Q14: Does ACSIA offer me the ability to take immediate action on specific user accounts?

Yes, if the incident involves an internal legitimate user account and the account has been used to perform some unauthorised activity, ACSIA admin upon notification can avail of so-called immediate actions and block that specific user.

This can even be done from remote connected devices which is a big plus for busy security teams and on-call engineers.

If an ACSIA user wishes to block a specific user account without having received a notification that is possible too.

Q15: Can ACSIA itself be hacked by the hackers? Will that make me more vulnerable?

A: ACSIA cannot itself be hacked - it does not form part of the attack surface that this exposed on a network, it will be foolish to expose any security product to everyone. However, ACSIA comes with security by design and security by default, it is a well hardened system. ACSIA monitors itself with no exceptions. When ACSIA is installed it automatically becomes its own first client.

Q16: Why have you chosen to focus on servers?

A: We are in a post perimeter security world. It is no longer sufficient to exclusively focus on perimeter security. Employees work from anywhere in the world and their devices access corporate data from the cloud outside of traditional security protections. Securing data in the post-perimeter world requires organizations to move critical security capabilities to where applications are hosted and data is stored. This is the fundamental design methodology of ACSIA.

Q17: Don't you need to monitor the health of the endpoint while the user is connected to servers?

A: There are many solutions for monitoring endpoints. ACSIA is designed for server systems because this is where the data is held.

Q18: It sounds like ACSIA needs to be deployed with other solutions in order to deliver comprehensive security?

A: We work with all perimeter security products and would be happy to advise on particular use cases.

Q19: What is the ACSIA support model and what levels of support are there and where are they provided from?

A: Level 1 and 2 support are provided by ACSIA resellers.

The ACSIA Standard Support Subscription provides customer support between 08:00 and 17:00 BST (09:00 and 18:00 CET). Support is provided from our Dublin and Milan offices and is provided via emails where the customers can send a support request to support[at]acsia.io. Support is provided by web conferencing tools as well where our team remotely assists the customer by sharing their screens. A current ACSIA annual Support subscription includes ACSIA related support calls.

Q20 How can partners and clients influence product direction?

We have a customer feedback channel where we encourage partners and customers to help us identify new needs and thereby influence our product roadmap.

4Securitas

65 Ivy Exchange, Parnell Street D01 AW68 Dublin Registered in Ireland

CRO: 598914 VAT Number: 3463752OH

Contact: info@4securitas.com