

ACSIA SOS – Redefining Cyber Defense: Endpoint, Perimeter, Mobile and AI Without Boundaries

Prevent. Defend. React. – Your Security, Simplified

Dectar's Mission: Dectar's mission is to revolutionize cybersecurity with a defense model that stops attacks before they occur. ACSIA SOS delivers advanced and accessible protection for everyone — from SMEs to large enterprises — overcoming the limits of traditional systems.

"If cybercriminals cannot gather the vital information from your systems that are needed to prepare an attack, they have no way to strike. This is the power of prevention-based defense."

The Danger of a Complex Ecosystem: Too Many Tools, Less Security

Many companies believe that stacking security tools (EDR, XDR, NDR, MDR, SIEM) means having complete protection. In theory, it should strengthen defenses — but in practice, it often produces the opposite effect.

- **Skills shortage:** the global market suffers from a severe lack of cybersecurity professionals. Having too many solutions offered by the current market brings an excessive amount of workload to manage the same. Therefore as a result this leads to the opposite effect of what is intended.
- **Alert overload:** every solution generates notifications, which together create an unmanageable flow. Among thousands of alerts, the risk of a real attack going unnoticed is extremely high.
- **Poor integration:** different tools create 'information silos,' preventing a unified view and slowing down response capabilities.
- **Complex management:** each system requires specific expertise, increasing the workload of already pressured IT teams.
- **Unsustainable costs:** multiple licenses, ongoing training, and internal management drive expenses up without guaranteeing a real increase in security.
- **False sense of security:** adopting multiple tools can create the illusion of protection, while leaving real vulnerabilities exposed.

ACSIA SOS is the answer to this complexity. It provides all-in-one incorporated functionalities, avoiding the risks of poorly managing too many products.

ACSIA SOS: ACSIA SOS: A Unified Security Platform

ACSIA SOS positions itself a unified all-in-one cybersecurity platform incorporating the typical functionalities of SIEM, EDR, XDR, NDR and many other tools, but with a unified and simplified approach. Unlike specialized solutions focused on a single domain (such as antimalware, antivirus, intrusion detection and prevention systems, network detection response and so on), ACSIA SOS offers a centralized platform that emphasizes prevention — preventing cybercriminals from gaining deep knowledge of digital assets — combined with ease of use and significantly lower costs compared to managing a fragmented cybersecurity solutions industry.

The **ACSIA SOS platform** stands out for its ability to deliver 360-degree cybersecurity across the entire infrastructure. While its operation begins with the installation of an agent on endpoints, its plug-and-play architecture enables seamless integration, extending security to the perimeter through integration with firewalls, existing solutions, as well as mobile devices. As a result, ACSIA SOS is not limited to being a simple endpoint protection system but extends its coverage to the entire IT domain.

Key Benefits of ACSIA SOS

- **Consolidated Platform:** The ACSIA SOS platform consolidates the functionalities of multiple cybersecurity solutions into a single platform. This provides a unified view of threats, **reducing management complexity** and the need to install and maintain numerous separate tools. Thanks to this **holistic approach**, security management becomes more efficient and streamlined.
- **Firewall Integration:** Through integration with firewalls, **ACSIA SOS** extends security to the perimeter. **It provides umbrella-model security coverage for network devices where the agent cannot be installed** (e.g., embedded systems, IoT, OT, telephony, telecameras etc.), integrating with existing firewalls to ensure visibility and immediate threat blocking in the event of anomalies.

- **Suitable for Organizations Without Dedicated Resources:** Ideal for SMEs as well as large organizations that cannot invest in high-end dedicated tools or do not have specialized security teams.
 - **Asset Inventory Area:** ACSIA SOS amongst its numerous functionalities it functions as an **Asset Inventory management** as well. Once the agent is installed, the system ensures complete visibility across all endpoints and integrated devices. It can deliver detailed information on critical elements for cybersecurity, including installed software, running processes, open ports, established connections, and patch levels. This detailed visibility is essential for an effective security strategy.
 - **Extended Protection for Android and iOS Mobile Devices:** With ACSIA SOS, protection goes everywhere—not just within the corporate network, but also on smartphones, tablets, and laptops on the move. Leveraging the predictive and proactive threat-blocking via threat sharing capabilities and extending it to mobile devices. Whether it's an iPhone or Android or a tablet used for remote work, security remains active: malicious URLs, the primary threats targeting mobile devices, are blocked for monitored devices. All of this is controlled through a centralized management system with our unique open detection engine. In this way, ACSIA SOS ensures that every endpoint—fixed or mobile, inside or outside the corporate perimeter—is always protected, simplifying management and reducing risks associated with the increasing mobility of work.
 - **Artificial Intelligence** is reshaping every industry, and cybersecurity is no exception. In a world where threats evolve faster every day than human response capabilities, AI becomes a critical ally: it accelerates processes, reduces operational complexity, and makes tasks accessible that were previously reserved for experts. ACSIA SOS brings this revolution directly into the hands of its users. Thanks to the AI Sigma Rule Generator component, anyone can create additional threat detection and response capabilities wherever the platform's coverage may fall short. Users gain capabilities that traditionally only a vendor could provide and they can do this so by using their natural language. With the AI component, ACSIA SOS is no longer just an integrated security platform; it becomes an intelligent defense ecosystem, capable of adapting to and responding to threats in real time, without requiring specialized technical resources.
-

2. ACSIA SOS's Unique 3-Stage Open Engine

The detection engine of **ACSIA SOS** is unique. Unlike any other cybersecurity solutions, it enables users to create instantly and autonomously their own detection and remediation rules. This engine operates on three distinct levels to provide comprehensive, multiphase layered protection.

- **First Stage (Standard Threats – Automatic Detection – Predictive Phase)**

The first stage is designed to automatically detect and block standard, known threats. This process leverages real-time **Threat Intelligence**, providing the platform with constantly updated information on threats and malicious actors. Thanks to this predictive layer, the system acts proactively and autonomously, without requiring user intervention or manual analysis. Threat Intelligence feeds are already vetted and deemed 100% malicious and therefore blocked as soon as they interact with the monitored assets, ensuring immediate protection.

- **Second Stage (Custom Rules – Operational Flexibility – Proactive Phase)**

This crucial stage enables the detection and blocking of threats based on custom rules, such as **Sigma Rules**. These user-loaded rules provide **exceptional flexibility**, tailoring the platform to the specific detection and response needs of each organization. The custom rules are in addition to the default set of rules that are primarily implemented to detect threats at their early stage, i.e. performing reconnaissance activity or profiling the target.

- **Third Stage (Advanced Analysis and Sophisticated Threat Containment – Reactive Phase):**

It performs in-depth analysis to reconstruct the entire attack sequence (the "full kill chain"), providing a comprehensive understanding of the incident context. This enables the identification and blocking of even the most sophisticated, advanced, and unconventional threats.

3. The Predictive and Proactive Functions of ACSIA SOS

ACSIA SOS doesn't just react—it anticipates and acts against threats, following the principle of “**Prevention First**.”

- **Predictive defense:**

- **Behavioral Analysis:** Continuously monitors endpoint data and network patterns, searching for anomalies that could indicate suspicious activity before they materialize into actual attacks.
- **Threat Intelligence:** Integrates real-time global threat feeds, constantly updating the platform to recognize new threat actors, techniques and vulnerabilities. Malicious actors are immediately blocked upon first contact with monitored systems without waiting for them to perform something malicious. This thanks to the threat intelligence data being vetted and deemed in advance as 100% malicious.
- **Goal of the “Predictive” Stage:** Detect latent threats and prevent them, effectively stopping attacks before they become a proper threat.

- **Proactive defense:**

- **Automated Response, Rule-Based Automation, and Remediation:** When a threat is detected, the system executes immediate, automated actions (e.g., IP blocking, endpoint isolation, malicious file reporting) without any human intervention, significantly reducing workload and the response times.
- **Continuous Monitoring:** ACSIA SOS implements constant checks to ensure security is not compromised, alerting or intervening in case of anomalies (e.g., disabled firewall).
- **Extended Network Control:** Its proactive nature extends to perimeter control, allowing, through integration with existing firewalls, “umbrella” style protection and blocking threats at network level devices without having agents installed.
- **Goal of the “Proactive” Stage:** For anyone to plan a cyber attack it is fundamental to perform first reconnaissance and profiling activity on the target. The main objective of the proactive defense is to get the actors while they are performing such activities, so way before an attack occurs.

Note: The entire process of detection and remediation actions within the predictive and proactive layers is completely automatic and the ratio of false positives in here is equal to zero.

Why choose ACSIA SOS?

Dectar's ACSIA SOS is the answer to modern cybersecurity challenges. In a world where tool complexity and the shortage of skilled personnel are real issues, ACSIA SOS provides a solution:

- **Integrated and Simplified:** Reduces complexity and alert fatigue caused by too many tools.
- **Cost Reduction:** ACSIA SOS is a consolidated platform that often requires no additional integrations, lowering overall business costs.
- **Primary Focus on Prevention:** Blocks up to 98% of threats before they cause harm—not just detecting, but anticipating them.
- **Zero False Positives:** In its preventive functions (predictive and proactive against external threats), the false positive ratio is zero.
- **Budget-Friendly:** Highly competitive and accessible for both SMEs and large enterprises.
- **Flexible and Customizable:** Thanks to its unique engine and customizable Sigma Rules, it adapts perfectly to the specific needs of your organization.
- **Comprehensive and Managed:** Delivers robust coverage and a centralized solution, eliminating the need for dedicated in-house expertise.
- **AI assistant:** functionality which enables every user to create their own threat defense mechanisms and extend capabilities beyond vendor control.

Choosing ACSIA SOS means investing in prevention, resilience, and peace of mind for your business.