1. ACSIA Software Product Description

ACSIA XDR Plus - Automated Cyber Security Intelligence Application is a powerful cyber defense product developed in Europe by Dectar that integrates our Extended Detection and Response (XDR) solution with a powerful Threat Intelligence capability that delivers a real-time predictive, proactive, and remediated cyber defense protection.
If you were to compare ACSIA XDR Plus with traditional cyber security products, it would be described as a cyber security product that incorporates Endpoint Detection and Response (EDR) capabilities with Intrusion Prevention (IPS), Intrusion Detection Systems (IDS), DNS-Shield, Host Insight and End Point Protection (EPP) into a single platform, all of which are supported by our real-time Security Information and Event Management (SIEM) system. Our design takes telemetry data from all monitoring tools into our SIEM for correlation and real-time threat analysis.
ACSIA XDR Plus performs these reactive detection capabilities ruthlessly and in real-time. We also know that a significant number of threats can be proactively protected against before they can manifest themselves at the perimeter security infrastructure or an endpoint device. The traditional approach of a network security device/agent is to block threats once they are detected at the perimeter of a company's infrastructure or when they have penetrated past the perimeter security measures and are detected on an endpoint device.
We augment the Extended Detection and Response functions with a predictive Threat Intelligence feed that bans wrong IP Addresses, anonymous network exit nodes, and sources of malware from accessing the network. Eliminating these sources of threats from being able to get anywhere near your network means that *"if they can't find you, they can't attack you"*.
The ACSIA XDR Plus Threat Intelligence feed is a predictive cyber defense tool DNS Shield blocks requests to malicious domains before the connection is established. This approach helps prevent Phishing or more advanced threats such as Command & Control (C&C) callback on any protocol and port.
Our End Point Protection blocks Portable Executables from being downloaded on the victim's hard drive.
Host Insight continuously monitors digital assets with the capabilities such as compliance assessment and management, vulnerability assessment and management, and finding software misconfiguration. It also provides visibility and a full report of monitored assets relevant to the risk assessment.
We also include an anti-surveillance feature that detects and prevents intelligence-gathering activities from being performed, thereby removing cybersecurity security threats before the surveillance information can be used to plan a cyberattack.
Our highly advanced monitoring and remediation techniques prevent the majority of cyberattacks from being planned or executed, vastly reducing the threat landscape for every organization.

A Force Multiplier for Your Security Operations
By integrating a threat intelligence feed with a pre-attack reconnaissance detection solution, which then also contains endpoint detection, and kernel-level monitoring, with an IDS and IPS, we have consolidated the shared telemetry of these otherwise disparate security tools into a unified SIEM, enabling ACSIA XDR Plus to correlate and remediate threats with forensic levels of accuracy in real-time.
We use Artificial Intelligence and Machine Learning to automate and remedy detected threats.

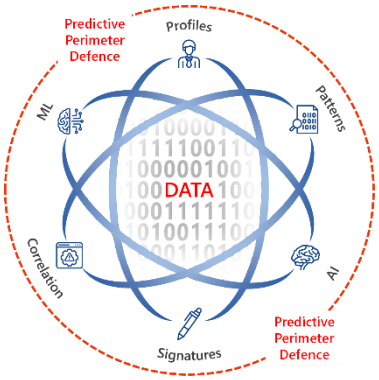
2. Design Objectives

Before exploring the product details, we shall first outline some of the major objectives for ACSIA XDR Plus, which will help explain some of the design decisions and directions taken with the product.

Our company mission is "*to democratize the availability of ACSIA as the next modern cyber defense platform of choice, providing the highest levels of data protection in the market, using open source technology at an affordable price*."

This is a somewhat loaded mission statement that required us to design and build a cyber defense solution from the ground up that was both highly efficacious and targeted blind spots synonymous with other platforms. It was also mandatory for the solution to be scalable, robust, simple to operate, easy to manage and deploy, and affordable. The ACSIA XDR Plus product was created with the following characteristics:

- It is a standalone product built and supported entirely by Dectar using open-source technology and over 150 unique algorithms.
- We use no third-party licensable products.
- Product innovations include highly effective anti-surveillance technology and Kernel & Registry level monitoring for granular accuracy.
- The product infrastructure requirements are minuscule and can be deployed in physical/virtual/cloud or container environments.
- ACSIA XDR Plus can be deployed using an agent on each endpoint or in an agentless deployment model.



ACSIA XDR Plus is designed to help protect against the following attack types:

✓Anonymous Exit Nodes (including Darkweb)	✓Pre-Attack surveillance techniques
✓Malware Signatures	✓Information Gathering
✓Port Scanning	✓Vulnerability Scanning
✓Malicious URLs	✓User and Account Compromise
✓Privilege Escalations	✓File and Data Manipulation
✓SQL Injection Threats	✓Lateral Movements
✓Exploitation & Payloads	✓Men-In-The-Middle Attacks
✓Ransomware Attacks	✓Drive-By-Attacks
✓Cross-Site Scripting	✓Password Attacks
✓Kernel Level Detection	✓Registry Level Detection
✓Zero Day Attacks	✓Kill Malicious Process

✓Kills connection to Cyber Attack Command and Control	✓Automated and Single-click Remediation
✓Regulatory & Compliance	✓Blocks Botnets
✓Management Reporting	✓Forensic Reporting
✓Block Portable Executables Download	✓Blocks Malicious Domains
✓MITRE ATT&CK mapping	✓Complete Host Insight

3. Product Composition

This document explains the composition of the ACSIA XDR Plus product from the client endpoint through the main components of the product logic to the end-user experience and management reports. As shown in fig.2 below, this lifecycle consists of seven separate elements, each of which we will discuss in more detail below.

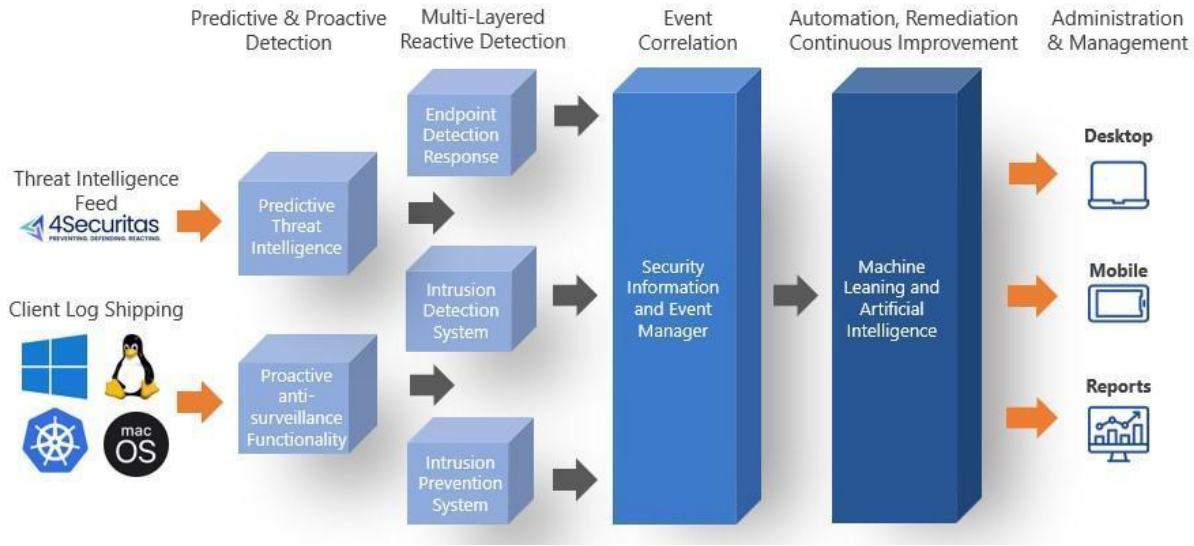


Fig 2. Components of ACSIA XDR Plus cyber defense application.

Clients must be deployed using Agents

ACSIA XDR Plus is a client-server architecture with Agents deployed on all monitored end-points. The application engine has a built-in OpenSearch stack and uses the Beats provided as log shippers.

When deploying the agent, the prerequisites for ports and service user requirements are minimal, i.e., no service user prerequisite exists. The ports are consolidated into unified ports 443 (HTTPS) and 444 (TCP/UDP) and). The agent will work autonomously if the device cannot reach the ACSIA engine/server.

The Client Agent uses Beats to send the following logs to the ACSIA application:

- System Logs
- Web Application Logs
- Audit Logs
- Network Traffic
- Kernel/Registry Logs
- Compliance Related Logs

4. Client Agent

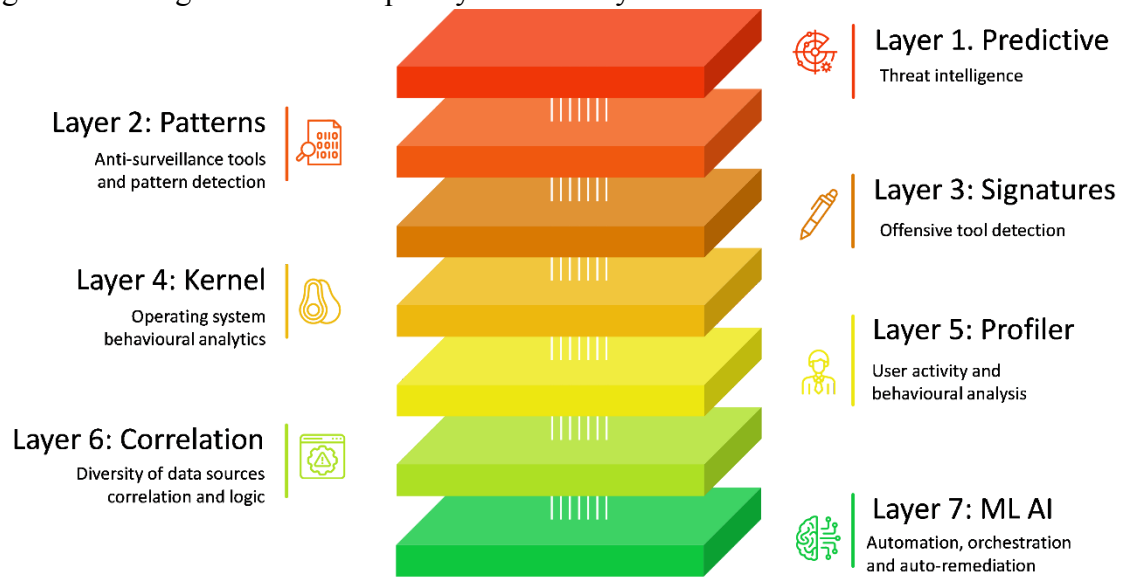
The aforementioned Beats is bundled into a single Client Agent for Windows, Linux, and MAC OS operating systems, and can be downloaded from the ACSIA UI (see the official guide) and will auto-install once the downloaded executable is run. The ACSIA agent consolidates all communication ports into a single port which is 443 (HTTPS) and 444 (TCP/UDP). The agent doesn't require a service user for ACSIA.

5. Log Shipping

OpenSearch provides the Beats as the log shipper to transfer the various log files to the Security Information Event Manager in ACSIA. The data volumes involved are minuscule (measured in kilobits), so there is no performance overhead on the client or network when deploying ACSIA.
All client traffic is encrypted using Transport Layer Security (TLS V1.2 or later) using client-server certificates.

6. Multi-Layered Detection Logic

The detection logic within ACSIA XDR Plus is an advanced multi-layered, high-performance security module containing seven integrated logical components of more than 150 unique algorithms designed and developed by our security architects in Dectar.



The seven logical components in the ACSIA XDR Plus Multi-Layered Defense design use shared telemetry for accurate threat detection and remediation.

7. Predictive and Proactive Cyber Defense

Dectar has developed two proactive Cybersecurity features unique to ACSIA XDR, which is why we call it ACSIA XDR Plus.

- Predictive Threat Intelligence
- Proactive Pre-Attack Anti-surveillance
- The pattern of Offensive tools detection

Predictive Threat Intelligence blocks billions of active threats from gaining any cyber access to your data. Eliminating many of the most prolific and damaging cyber threats from contaminating your IT System - vastly decreasing threat levels to the business.
Proactive Pre-attack and Anti-Surveillance is an active module that provides reconnaissance protection at the periphery of an environment. It captures all requests for information and correlates the tools and exploit techniques to deny complex and obfuscated cyberattack methods from intelligence gathering. Surveillance and information-gathering techniques are necessary steps for cybercriminals to perform in advance of planning an attack. ACSIA will detect and block these activities; the data collected can be used to plan a cyberattack.

8. XDR Protection

The XDR features within ACSIA contain the following key features.

- Offensive tools detection
- Kernel Monitoring
- User Behavioral Analysis

The signatures and behavior of offensive tools used during pre-attack and attack phases are one of the key functionalities in ACSIA XDR Plus to stop threats proactively. It captures offensive tools cybercriminals use to gather intelligence to discover weaknesses in a cyber defense before planning an attack. It will also identify an attacker trying to collect information from within an organization by analyzing their techniques and methods and the data being queried.
The kernel layer analyzes the operating system's core to detect anomalies and threats. It is very efficient in detecting insider threats from legitimate users and malware or rootkit deployments. This security level operates independent of the type/maturity of the threat and therefore has the unique ability to capture previously unknown threats (zero-day attacks)
The UEBA (user entity behavior analysis or Profiler) is used to profile users' day-to-day routine activities to detect unusual changes in the pattern of actions being performed, particularly when internal users or compromised accounts are accessing data or executing routines not associated with their daily activities. This powerful feature is helpful for auditing personnel activities, particularly when determining "who did what" retrospectively.

9. Correlation

We correlate logs from all our data points discussed earlier into our Security Information and Event Management (SIEM) along with the following data sources:

- Endpoint Detection and Response
- Intrusion Detection System
- Intrusion Prevention System

As ACSIA contains an integrated Endpoint Detection and Response (EDR) with an Intrusion Prevention (IPS) and Intrusion Detection Systems (IDS) in a single platform, we capture the logs of these security modules for real-time correlation and analysis using our Security Information and Event Management (SIEM) system.
Consolidating these rich data sources in a SIEM strengthens the ability of ACSIA XDR Plus to identify threats across multiple cyberdefense toolsets.

10. Automation, Remediation & Continuous Improvements

ACSIA XDR Plus utilizes Machine Learning/Artificial Intelligence to automate and continuously improve threat responses and improve the threat intelligence information to detect bad actors better before they can compromise the monitored asset.
Data analyzed by ACSIA Detection Logic is passed onto ML/AI to automatically determine the most appropriate remediation action based on the threat type and severity level. These are automated using Ansible playbooks for the orchestration of remediation actions.

11. Administration and Management

The ACSIA user interface is accessed via a web browser to any standard desktop device or smartphone device. By default, ACSIA generates self-signed SSL certificates for HTTPS browsing, but ACSIA can be deployed with client-specific SSL certificates. Multi-factor authentication or two-factor authentication is used for Administration and Management access.
The notification of alerts is configurable and can be sent via email, Slack messaging system or Microsoft Teams.
The Hosts page contains a table of client hosts monitored by ACSIA and where new clients can be added using a simple wizard.
A Live Notifications page lists all active and pending alerts for review or action.
Insights are where default and custom dashboards are listed. These are particularly useful for forensic investigation and include:

- Access Control Dashboard
- User Activity Dashboard
- General Network Traffic Dashboard
- IP Address Activity Dashboard
- All Traffic Dashboard

The Compliance section is where the analytics and dashboards relating to compliance and regulatory frameworks are available – these include:

- Security Events Dashboard
- Integrity Monitoring Dashboard
- PCI DSS Compliance Dashboard
- GDPR Compliance Dashboard
- NIST 800-53 Framework Dashboard
- Mitre Att&ck® Framework Dashboard
- Vulnerabilities Dashboard
- Policy Monitoring Dashboard
- HIPAA Compliance Dashboard
- System Auditing Dashboard
- Trusted Services Criteria Dashboard

All analytics and dashboards have reporting capabilities that can be exported into major standard formats.
The Policies section contains all actioned events, such as:

- IP Blacklist

- IP Whitelist
- Locked Users
- Muted Notifications
- Location Based Access

The section "Event History" records every activity in ACSIA UI and mitigation responses. For instance, who authorized a user, who locked an account, who banned an IP address and so on; this has been documented to have the complete track of who did what.
A ‘Distribution List’ is used to notify multiple members when an alert is generated. All pending alerts are listed in the ‘Live Notifications’ section, where the end user requires remediation actions.
The “Settings” is where all the UI settings handled:

✓Notifications

✓Integration

✓DNS Shield

✓Log Retention

✓License

✓Users

✓E-mail

✓2FA

✓Software Update

✓Clients Uninstall

12. Key Product Features and Benefits

The product features and benefits below are all core components of our ACSIA product set. They result from years of research and development by our team in Dectar and represent the latest technological and innovative advancements in the cybersecurity market.

Threat Detection	
✓Includes Endpoint Detection Response	✓It contains an industry-leading Kernel analysis function to identify and eliminate abnormal processes
✓Includes an Intrusion Detection System	✓Contains pre-emptive anti-surveillance technology to prevent attacks before they can be planned

✓Includes an Intrusion Prevention System	✓Provides protection for Windows servers and desktops
✓Includes a Security Information and Event Management system	✓Provides protection for Linux servers and desktops
✓Includes cybersecurity remediation for all threats	✓Provides file-level integrity check

Technical Benefits	
✓Compatible across Physical and Virtual servers	✓Scales' to 1000's endpoints
✓Compatible across Container and Cloud environments	✓Small technical footprint requirement (8 cores, 16GB free memory, 200 GB free SSD, 1GB file to download)
✓Compatible across Physical and Virtual servers	✓Contains both web & mobile User Interface
✓Includes Artificial Intelligence and Machine Learning	✓Will operate in an Air-gapped Network
✓Built using Open source technologies	✓Easy Installation (7 minutes)
✓Implements Role Based Access Control (RBAC) for internal users	✓Full visibility on privileged accounts

Commercial & User Benefits	
✓Removes over 99% of false positive alerts	✓Agent deployment
✓Automates and simplifies cybersecurity operations	✓Eliminates the need for daily security updates
✓Commercially competitive and can be implemented as part of a cost reduction plan	✓Contains both web & mobile User Interface
✓All product features listed above are included in the core product – no extras.	✓Product available on an annual subscription basis
✓Provides Management Reporting	✓Provides Forensic Reporting

Related articles

- ACSIA XDR Plus Architecture V6.x.x
- ACSIA XDR Plus Installation and User Administration Guide - v6.x.x
- Uninstall AgentLess Windows
- Release Note v6.x.x
- Product Feature Reference