Automated Cybersecurity Intelligence Application

Software Product Description Document

Document: ACSIA XDR Plus Software Product Description V4.01
Release Date: June 2022

Contents

ACSIA Product Description

ACSIA XDR Plus - Automated Cyber Security Intelligence Application is a powerful cyberdefense product developed in Europe by 4Securitas 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.

The ACSIA XDR Plus product incorporates Endpoint Detection and Response (EDR) capabilities with Intrusion Prevention (IPS) and Intrusion Detection Systems (IDS) into a single platform, all of which are supported by our real-time Security Information and Event Management (SIEM) system.

We have then enhanced this Extended Detection and Response (XDR) by including a predictive Threat Intelligence feed that bans bad IP Addresses, anonymous exit nodes, and sources of malware from accessing the network. Eliminating these sources of threats from being able to even view your network, so ***"if they can't find you, they can't attack you"***.

We also include anti-surveillance feature which detects and prevents intelligence gathering activities 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 prevents 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, 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 for the automation and remediation of detected threats.

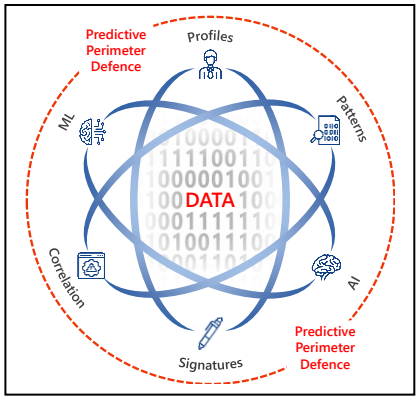
Design Objectives

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

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

This is a fairly loaded mission statement which required us to design and build a cyberdefense solution from the ground up that was both highly efficacious and addressed 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 to be affordable. The ACSIA XDR Plus product therefore has the following characteristics:

- It is a standalone product built and supported entirely by 4Securitas 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 level 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

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.

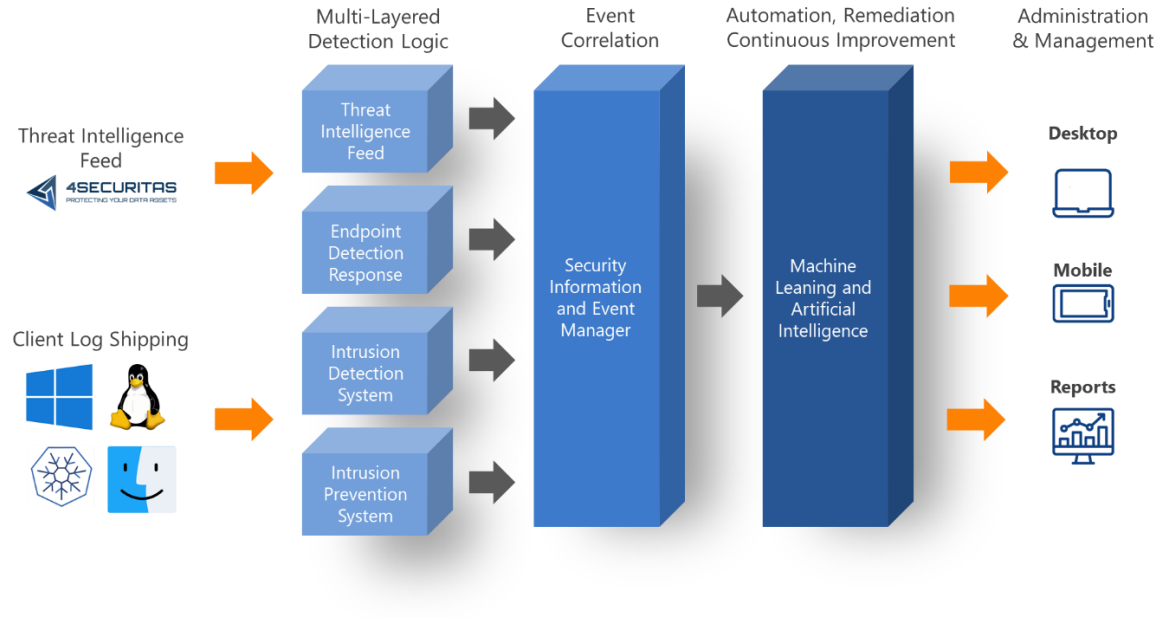


Fig 2. Components of ACSIA XDR Plus cyber defense application.

Clients can be deployed using Agents or in Agentless mode

ACSIA XDR Plus is a client server architecture and can be deployed using an Agent or in an Agentless mode. The application engine itself has a built-in Elastic stack (Elasticsearch, Logstash and Kibana) and uses Beats provided by Elasticsearch as log shippers.

What is the difference between operating with an agent or an agentless client?

When deploying the agent, the prerequisites in terms of ports and service user requirements are minimal, i.e. there is no service user prerequisite and the ports are consolidated into unified port 443 (https) and 444 (TCP/UDP). Furthermore, the agent will work autonomously in case the device is not able to reach the ACSIA engine/server.

Another difference is that the agentless deployment requires multiple ports to be opened on the firewalls (both inbound and outbound), as well as the creation of a service user with privileges on connected devices.

Whether deploying ACSIA XDR Plus with an Agent or operating in Agentless mode, the function of the Beats is to send the following logs to the ACSIA application:

- System Logs
- Web Application Logs
- Network Traffic
- Kernel/Registry Logs

- Audit Logs
- Compliance Related Logs

Both Agent and Agentless modes of operation are described below:

Agentless Clients Deployment

The only occurrence where ACSIA XDR Plus interacts with a connected client is when the application wants to ban a malicious IP address or when the end user selects a remediation option provided with the alerts (immediate actions). This is done by ACSIA via its service account (SSH or RDP) so there is no agent required on the client end to perform such action.

Operations such as banning an IP are performed using playbooks within ACSIA which are orchestrated through the Ansible configuration management system.

Client Agent

A client agent is available starting from v4 of ACSIA XDR Plus. With the agent mode deployment, the aforementioned Beats are bundled into a single package for Windows, Linux and MAC OS operating systems. The bundles can be downloaded from ACSIA UI (see the official guide for details)and will auto-install once the downloaded executable is run. Unlike the agentless mode, 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.

Log Shipping

Beats provided by Elastic search are used as the log shipper to transfer the various log files to the Security Information Event Manager in ACSIA. The data volumes involved are miniscule (being 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.

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 4Securitas.

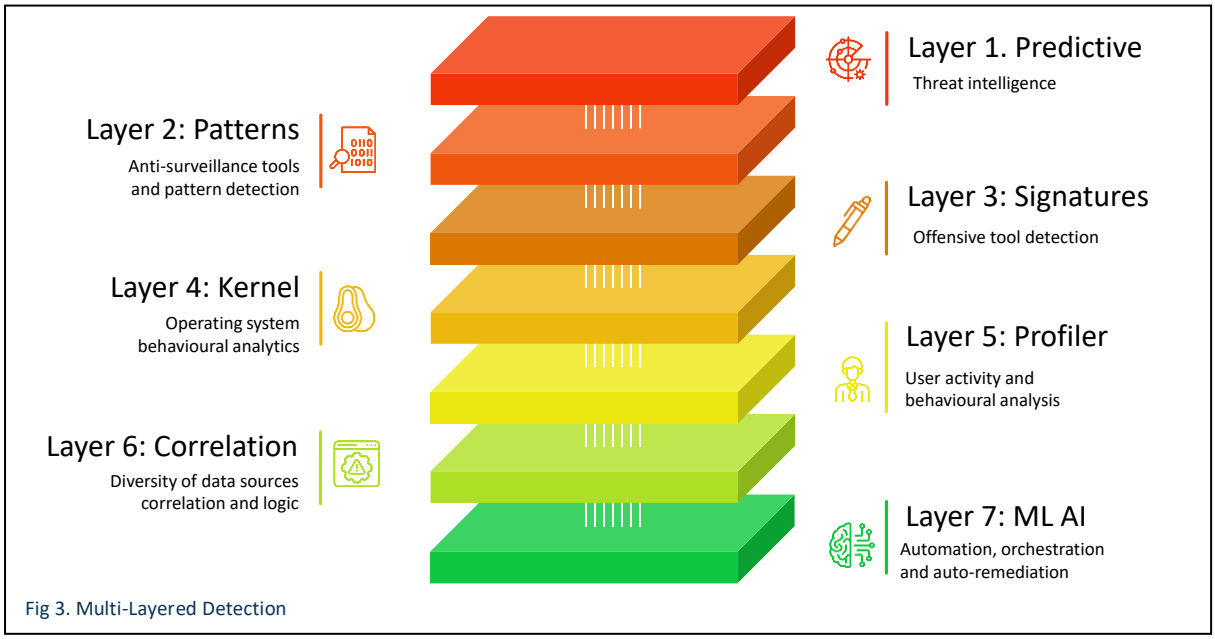


Fig 3. Multi-Layered Detection

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

Predictive and Proactive Cyber Defense

4Securitas has developed two proactive Cybersecurity features that are unique to ACSIA XDR which is why we call it ACSIA XDR Plus.

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

Predictive Threat Intelligence blocks billions of active threats from gaining **any** level of cyber access to your business. Eliminating many of the most prolific and ruthless cybercriminals worldwide from getting anywhere close to your platforms - 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 more 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 these activities and block them before they can be used to plan a cyberattack.

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 is one of the key functionalities of ACSIA XDR Plus to proactively stop potential threats. It captures offensive tools that are used by cybercriminals to gather intelligence and discover weaknesses in a cyberdefense prior to planning an attack but will also identify an attacker trying to collect information from within an organization. This is done by analyzing the techniques and methods being deployed, as well as the data being queried.

The kernel layer analyzes the core of the operating system to detect anomalies and threats. It is very efficient when it comes to insider (legitimate users) threats and/or any type of malware and rootkit deployments. This security level operates independent of the type/maturity of the threat, and therefore has the unique ability to capture threats that are currently unknown.

The UEBA (user entity behavior analysis or Profiler) is used to profile users' day-to-day routine activities so that it can 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 dailty routine. This powerful feature is also used for auditing the activities of personnel, particularly when determining 'who did what' retrospectively.

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 sources of data together in a SIEM, strengthens the ability of ACSIA XDR Plus to identify threats across multiple cyberdefense toolsets.

Automation, Remediation & Continuous Improvements

ACSIA XDR Plus utilizes Machine Learning/Artificial Intelligence to automate and continuously improve threat responses, as well as improving threat intelligence information to better detect bad entities prior to infiltrating 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 playbooks using Ansible for the orchestration of remediation actions.

Administration and Management

The ACSIA user interface is accessed via a web browser to any standard desktop device or via a 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 that are monitored by ACSIA and where new clients can be added using a simple wizard.

A Live Notifications page is where all active and pending alerts are listed for review or action.

Insights is 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 Attack 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’ is where every single activity in ACSIA UI and mitigation responses are recorded. For instance, who authorized a user, who locked an account, who banned an IP address and so on, this has been recorded to have the track of who did what.

A 'Distribution List' is used where multiple members will be notified when an alert is generated. All pending alerts are listed in the 'Live Notifications' section where remediation actions are required by the end user.

The "Settings" is where all the UI settings handled:

✓ Log Retention	✓ Users
✓ Integration	✓ Notifications
✓ Update	✓ License
✓ Install	✓ Email configuration
✓ 2FA	

Key Product Features and Benefits

The product features and benefits below are all core components of our ACSIA product set. They are the result of years of research and development by our team in 4Securitas and represent the latest technological and innovative advancement in cybersecurity in the market.

Threat Detection	
✓ Includes Endpoint Detection Response	✓ Contains 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 of endpoints
✓ Compatible across Container and Cloud environments	✓ Small technical footprint requirement (2 cores, 16GB memory, 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
✓ Implements Role Based Access Control (RBAC) for internal users	✓ Will operate in an Air-gapped Network

Commercial & User Benefits

✓ Removes over 99% of false positive alerts	✓ Agent or Agentless Clients deployment
✓ Automates and simplifies cybersecurity operations	✓ Eliminates need for daily security updates
✓ Commercially competitive and can be implemented as part of a cost reduction plan	✓ Contains both web & mobile device 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

More information on ACSIA can be found using the following link: ACSIA documentation
Contact us: email sales@4securitas.com, www.4securitas.com