

Core Product Features

Proactive Anti-Surveillance

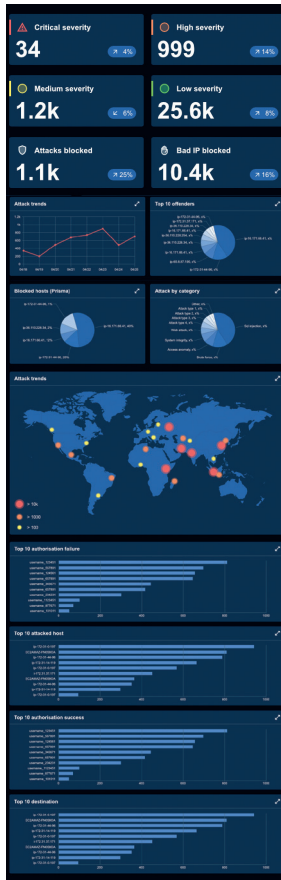
- Blocks information gathering tools
- Prevents port scanning
- Stops vulnerability scanning
- Identifies and blocks pre-attack techniques

Predictive Threat Intelligence

- Real-time threat intelligence feed
- Blocks anonymous network
- Blocks malware signatures
- Blocks malicious URLs (command & control, etc.)
- Blocks malicious IP using reputation scoring

Full XDR Features

- Centralized EDR, IDS, IPS & SIEM
- Real-time correlation of all logs
- Kernel-level monitoring
- File integrity monitoring
- Account Compromise and User Profiler for anomalous behavior



Key Operational Features

- 1 Simple Installation**
Supports Linux, Mac and Windows end-points.
- 2 Environments**
Available for on-premises and cloud infrastructure with physical, virtual and container deployments.
- 3 Accuracy**
Consolidation and logs across predictive, proactive and XDR features provides massive improvements in threat correlation that provided forensic level accuracy.
- 4 Clients**
Available with client agent and in agentless client mode.
- 5 Remediation**
One-click remediation using AI & ML to web and mobile devices.
- 6 Footprint**
Very small footprint - a typical ACSIA server platform for monitoring 100 servers is:
 - ▶ 2 CPU cores
 - ▶ 8GB memory
 - ▶ 100GB storage
 (Simply scale size for larger environments to be monitored.)



ACSIA XDR Plus, from 4Securitas, is an Extended Detection and Response (XDR) solution with a powerful threat intelligence capability, that delivers a real-time predictive, proactive and remediated cyberdefense protection.

KEY BENEFITS

Simple to operate - with excellent accuracy which reduces 'Alert Fatigue'

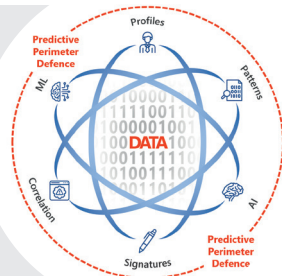
Heterogeneous - monitors servers and desktops whether physical, virtual or containerized in Kubernetes, with Linux, Mac and Windows support from a single platform

Automation - tunable levels of automation

Affordable - best ROI in the market

"If they can't find you, they can't attack you either."

Automated Cyber Security Intelligence Application (ACSIA) Extended Detection and Response (XDR) Plus



Contact 4Securitas to get in touch with your **country manager**



+353 85 720 4124



sales@4securitas.com
4securitas.com



Scan me to arrange a demo



ACSIA XDR Plus Predictive/ Proactive/Reactive Cyberdefense System























Types of Cyberattack

Cyberattack Methodologies

Combined Proactive/Reactive ACSIA Cyberdefenses

Reactive ACSIA Cyberdefenses

Predictive & Proactive ACSIA XDR Plus Cyberdefenses

<ul style="list-style-type: none"> Malicious URL Blocking Malicious IP Blocking Block Anonymous access Block sources of Malware 	 1. Predictive Protective Shield 	<ul style="list-style-type: none"> Anonymous Network Attacks Command and Control Ransomware Attacks
<ul style="list-style-type: none"> Bespoke ACSIA Algorithms Offensive Tool Detection Patterns & Technique Detection Correlation & ML/AI 	 2. Information Gathering & Reconnaissance 	<ul style="list-style-type: none"> Fingerprinting Port Scanning Vulnerability Scanning
<ul style="list-style-type: none"> Bespoke ACSIA Algorithms Offensive Tool Detection Kernel Level Analysis Pattern & Technique Detection Correlation & ML 	 3. Men-In-The-Middle 	<ul style="list-style-type: none"> Session Hi-jacking DNS/IP Spoofing Network Sniffing
<ul style="list-style-type: none"> Bespoke Algorithms User Profiler Patterns Detection Correlation & ML/AI 	 4. Password Attacks 	<ul style="list-style-type: none"> Brute Force Attacks Dictionary Attack Social Engineering
<ul style="list-style-type: none"> Bespoke ACSIA Algorithms User Profiler Patterns & Technique Detection Kernel Level Analysis Correlation & ML/AI 	 5. Drive-By-Attack 	<ul style="list-style-type: none"> Code Injection Redirect Iframe Malware Injection
<ul style="list-style-type: none"> Database Manipulation Database Dump Database Compromise 	 6. SQL Injection Threat 	<ul style="list-style-type: none"> Database Manipulation Database Dump Database Compromise
<ul style="list-style-type: none"> Bespoke Algorithms Correlation & ML Offensive Tools Detection Pattern & Technique Detection 	 7. Malware 	<ul style="list-style-type: none"> Whale Phishing Spear Attack Pharming
<ul style="list-style-type: none"> Bespoke ACSIA Algorithms Kernel Level Analysis Correlation & ML/AI 	 8. Ransomware Attack 	<ul style="list-style-type: none"> Malicious Software Data Encryption Deception
<ul style="list-style-type: none"> Bespoke ACSIA Algorithms Kernel Level Analysis Correlation & ML/AI 	 9. Eavesdropping Attacks 	<ul style="list-style-type: none"> Sniffing Snooping Traffic Hijack
<ul style="list-style-type: none"> Bespoke Algorithms User Profiler Offensive Tool Detection Patterns & Technique Detection Kernel Level Analysis Correlation & ML/AI 	 10. AI-Powered Attacks 	<ul style="list-style-type: none"> BotNet with AI/ML Adversary ML/AI Social Engineering
<ul style="list-style-type: none"> Bespoke Algorithms Offensive Tools Detection Pattern & Technique Detection Correlation & ML 	 11. Cross Site Scripting (XSS) 	<ul style="list-style-type: none"> Malicious Script Injection Malicious Code Injection Bypass Control