Core Product Features

Proactive XDR Anti-Surveillance

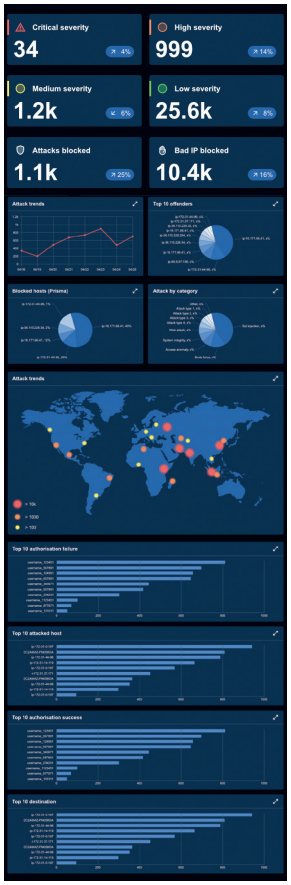
- Blocks information gathering tools
- Prevents port scanning
- Stops vulnerability scanning
- Identifies and blocks pre-attack techniques

Predictive XDR Threat Intelligence

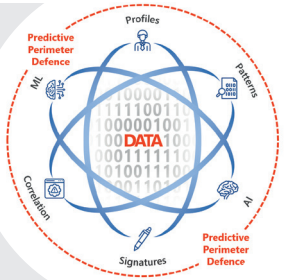
- Real-time threat intelligence feed
- Blocks anonymous network
- Blocks portable executables
- Blocks malicious URLs (command & control, etc.)
- Blocks malicious IP using reputation scoring

Reactive XDR Features

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



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



Key Operational Features

1 **Simple Installation**
Supports Linux, Mac and Windows end-points.

2 **Environments**
Available for on-premises and cloud infrastructure with physical and virtual 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**
Exceptionally lightweight client agent.

5 **Remediation**
One-click remediation from web and mobile devices.

6 **ACSIA Engine Footprint**
Very small footprint - a typical ACSIA server platform for monitoring 100 servers is:

- *8 CPU cores*
- *16GB memory*
- *200GB storage*

(Simply scale size for larger environments to be monitored.)

Technology brief Technology brief Technology brief Technology brief

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

+353 85 720 4124

sales@4securitas.com
4securitas.com

4Securitas
PREVENTING. DEFENDING. REACTING.

ACSIA
XDR PLUS

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 or virtual, with Linux, Mac and Windows support from a single platform

Consolidation - combines the functionality of multiple cyber defense products

Automation - tunable levels of automation

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

Scan me to arrange a demo

ACSIA XDR Plus Predictive/ Proactive/Reactive Cyberdefense System	Types of Cyberattack	Cyberattack Methodologies
• Malicious URL Blocking • Malicious IP Blocking • Block Anonymous access • Block sources of Malware	**1. Predictive Protective Shield**	• Anonymous Network Attacks • Command and Control **Botnet**
• Bespoke ACSIA Algorithms • Offensive Tool Detection • Patterns & Technique Detection • Correlation & ML/AI	**2. Information Gathering & Reconnaissance**	• Fingerprinting • Port Scanning • Vulnerability Scanning
• Bespoke ACSIA Algorithms • Offensive Tool Detection • Kernel Level Analysis • Pattern & Technique Detection • Correlation & ML	**3. Men-In-The-Middle**	• Session Hi-jacking • DNS/IP Spoofing • Network Sniffing on Promiscuous Mode
• Bespoke Algorithms • User Profiler • Patterns Detection • Correlation & ML/AI	**4. Password Attacks**	• Brute Force Attacks • Dictionary Attack
• Bespoke ACSIA Algorithms • User Profiler • Patterns & Technique Detection • Kernel Level Analysis • Correlation & ML/AI	**5. Drive-By-Attack**	• Code Injection • Redirect Iframe • Malware Injection
• Database Manipulation • Database Dump • Database Compromise	**6. SQL Injection Threat**	• Database Manipulation • Database Dump • Database Compromise
• Bespoke Algorithms • Correlation & ML • Offensive Tools Detection • Pattern & Technique Detection	**7. Phishing**	• Whale Phishing • Spear Attack • Pharming
• Bespoke ACSIA Algorithms • Kernel Level Analysis • Correlation & ML/AI	**8. Ransomware Attack**	• Malicious Software • Data Encryption • API Integration
• Bespoke ACSIA Algorithms • Kernel Level Analysis • Correlation & ML/AI	**9. Identity Attacks**	• User Profiling Sniffing • Snooping • Traffic Hijack
• Bespoke Algorithms • User Profiler • Offensive Tool Detection • Patterns & Technique Detection • Kernel Level Analysis • Correlation & ML/AI	**10. AI-Powered Attacks**	• BotNet with AI/ML • Adversary ML/AI
• Bespoke Algorithms • Offensive Tools Detection • Pattern & Technique Detection • Correlation & ML	**11. Cross Site Scripting (XSS)**	• Malicious Script Injection • Malicious Code Injection • Bypass Control

Predictive & Proactive ASCIA XDR Plus Cyberdefenses

Reactive ASCIA Cyberdefenses

Combined Proactive/Reactive ASCIA Cyberdefenses