What Makes ACSIA XDR Plus Different from Existing Technologies

ACSIA XDR Plus is a radically new Cybersecurity product that identifies and eliminates potential exploits before they can threaten your data. It focuses on Predictive and Pre-attack surveillance techniques deployed by modern cybersecurity criminals as well as advanced monitoring of both the compute resources and data to identify any potential compromises within your IT environment.

This approach differs significantly from virtually all current Cybersecurity defense products which attempt to identify hash exploits using a database of known attack identifiers (called signatures - similar to fingerprints). A reference database of this nature requires constant and regular updates in-order to update newly identified cyber exploits, and only works when a cyberattack uses an exact replica of the exploit signature. While these products do detect a large proportion of malware attacks, they only do so after the system has been compromised - so they are totally reactive by design. Whilst this defense model worked reasonably well in the 1990's when cyberattacks were unsophisticated and infrequent, the inherent latency updating the latest security vulnerabilities coupled with weaknesses matching exploit signatures are two of the major reasons these traditional cybersecurity products are unable to keep the pace with modern and constantly evolving cyber-attack strategies.

The number of security and data breaches continues to grow exponentially (see Thales breach index) and the security industry is slowly acknowledging that defense must start at the earlier pre-attack stage where ACSIA XRD Plus is focused (see Lockheed Martin article).

The fact that the majority of existing cybersecurity solutions focus on the Network (or perimeter security) to prevent external cyber-attacks is also problematic. Traffic at the Network layer is encrypted and therefore cyber defense tools are unable to deterministically analyse traffic patterns or content. This requires them to capture vast quantities of data to predict anomalies which may or may not represent a cyber exploit (this is referred to as 'indicators of compromise'). This is both costly in terms of the IT infrastructure required to host the solution and the considerable number of resources required to manage it (running costs). These legacy cyber defense tools generate vast quantities of false positives and vague threat detection results which also requires considerable time and expensive security analysts to investigate and determine the validity of the alert.

By contrast, ACSIA XDR Plus analyses in real-time all pre-attack activities including system activities and user behaviour, correlating and automatically resolve threats immediately using our advanced cyber defense engine. We track actual events to accurately identify real threats to the integrity of your data, and automatically stop and prevent your data from being compromised. Eliminating false positives, ACSIA XDR Plus accurately removes cyber threats without the need for expensive security analysts to investigate vast quantities of vague alerts generated by other solutions.

ACSIA Technical Defense Model - Highlights

Cyber Blind Spots

ACSIA is designed to focus on advanced cyber-attack methodologies that target Cyber Blind Spots which traditional cybersecurity products are incapable of detecting.

- ✓ ACSIA XDR Plus provides a Predictive Threat Intelligence feed that pro-actively blocks billions of real threats from gaining any level of cyber access to your business, eliminating many of the most prolific and ruthless cybercriminals worldwide from accessing to your platforms and applications. This best way to describe this would be to say that your IT environment is invisible to these malicious cybercriminals – you are in stealth mode.
- ✓ ACSIA XDR Plus monitors your digital footprint that is remotely or locally accessible - from web based applications, internet or extranet access points through to local access points by employees or partners
- ✓ ACSIA XDR Plus detects pre-attack attributes (indicators of warnings) at an early stage, offering recommended remediation options with a simple click on a mobile device.
- ✓ ACSIA XDR Plus detects and correlate pre-attack attributes which when combined represent a significant or real and present danger of attack across their full lifecycle
- ✓ All ACSIA XDR Plus monitoring, detection, analysis, remediation and reporting is all performed in real-time

Why have Cyber Blind Spots not been addressed until now

The Network has long been perceived as the weak spot in an organization and most solutions have been designed around a perimeter security model, with data assets surrounded by these technologies (similar to a security fence protecting a building). This one dimensional security model is incapable of protecting your data assets whenever the perimeter security is breached - a major factor in all the increasingly sophisticated successful cyber-attacks. So why is this?

- The most serious challenge for the cybersecurity industry is to detect attack attributes at an early stage (indicators of warnings) and existing solutions use antiquated techniques that are unable to address most Cyber Blind Spots
- Preventive measures are only taken seriously with regulators intervention, and this has been slow and inconsistent across various business sectors (Fintech, Utilities, Government, Manufacturing all conform to different regulations)

ACSIA XDR Plus focuses on accurate detection and remediation of cyber blind spots in real time. Other solutions have varying levels of success informing you that it may have detected malware, which of course means that you have already been compromised and that the last stage/step of an attack has already occurred. The ACSIA XDR Plus product operates at the predictive and pre-attack stage which is 4 steps earlier.

Predictive Threat Intelligence can be described as having the ability to ban known malicious sources (IP addresses, Bad URL's, sources of malware …) from anywhere across the globe, having any level of access to your environment. A complete ban of malicious actors getting access to an environment is a powerful tool in the elimination of cybercriminal activity.

Our Pre-attack prevention capability operates differently as it prevents cyber-criminals from gathering intelligence and working out how and what to use in planning an attack on your data.

ACSIA XDR Plus detects and stops the intelligence gathering activities of an attacker at the earliest stages of their planning activities.

What are the other major Challenges facing tradition Cybersecurity vendors?

- Detection of zero-day attack is where a new and previously undocumented weakness is discovered in software which is exploited by criminals before a fix is available from its creator.
- Reducing the large quantities of false/positive alerts requiring investigation and analysis by security teams

Both challenges can be addressed if Cyber Blind Spots are addressed and eliminated in real time through appropriate cybersecurity defenses. Many vendors use Machine Learning / Artificial Intelligence to improve security remediation outcomes, but this approach is expensive, slow and inaccurate. The best method to detect 0-day attacks is for a solution to focus on cyber blind spots because the Cyber Blind Spot is the method cyber criminals use to prepare an attack.

The ACSIA XDR Plus product is capable of identifying both known and unknown (0-day) attacks using two separate defense modules. The first method uses our proactive Pre-attack capability which detects and prevents potential threats at the information gathering (reconnaissance) process. The second method is a kernel level analysis capability which operates at the core of the operating system. The kernel is at the core of a computer's operating system and maintains complete control over every single operation of the system. It is the portion of the operating system code that is always resident in memory and facilitates interactions between all hardware and software components. Including Kernel monitoring within the ACSIA XRD Plus product enables granular levels of monitoring to be performed and allows malicious activity to be reported and remediated.

Does Machine Learning (ML) and Artificial Intelligence (AI) significantly improve cybersecurity ?
Most cybersecurity defense solutions use ML/AL to ingest all anomalous activities that have been detected and parse them. Anomalies are not necessarily threats and a great majority of them are benign alerts. Because of the volume of alerts and lack of clarity around a threat or a benign alert, ML/AI must be used to reduce the number of security alerts being raised, but despite this, the quantity and quality of these alerts still contains massive numbers of false positives.

As mentioned previously, ML/AI does not assist with 0-day attacks, but neither does ML/AL enable the detection of cyber attacks. ACSIA XDR Plus does not use ML/AI for threat detection as we use our intelligence analysis engine offensively (at the Predictive and pre-attack phase) as well and defensively (if a real-time attack is occurring). ACSIA XDR Plus is designed to use ML/AI for orchestration and to automate remediation. Once it has identified a threat, then there is no need for human intervention as ML/AI will automatically handle the threat.

Other benefits provided by ACSIA XDR Plus
Cyber solutions tend to be very expensive both in terms of subscription and running costs. Today's cybersecurity vendor market is prohibitively expensive at a capital and operational level and are predominantly designed to focus on large organizations with deep pockets. A great number of organizations have also implemented solutions but cannot afford the security teams required to scan the vast quantities of alerts to determine which ones need attention and which are false positives.

ACSIA XDR Plus provides a superior cyber defense solution which is highly scalable, boasting an extremely affordable pricing model to fit the budget constraints of small, medium and large

organizations, without the need to have cybersecurity experts sift through vast quantities of false/positive alerts being generated by existing cybersecurity solutions. Anyone with basic knowledge of IT and the business, can manage ACSIA XDR Plus.

Conclusion

The future of cybersecurity is to have a multi-dimensional security strategy which combines a perimeter defense shield with an internal security capability which defends data assets being compromised for any reason.

That is what we do at 4Securitas, and that is what makes ACSIA XDR Plus different.

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