ACSIA CRA Product Description

Description of the CRA service

The ACSIA CRA cyber risk assessment service performs a comprehensive analysis of a company's cyberposture, focusing on the external exposure of the services and information that may be vulnerable to cyberattack.

The CRA analysis starts with the manual input of a limited number of Assets, usually the Company's internet domains, from which a map of all publicly connected exposed Assets is generated.

The entire attack surface is then thoroughly checked for critical situations/weak points and specific vulnerabilities for each type of Asset.

After the individual evaluation of each Asset, a proprietary algorithm is activated. The algorithm calculates the overall risk rating, ranging from 0 to 100, by correlating the data of Assets, their connections, and the topology and posture of the Company's internet systems.

A score of 0 represents the worst situation with maximum exposure, while 100 represents the best situation with minimum exposure.

The NIST (National Institute of Standards and Technology) Framework also feeds its information into the service, making the whole process an objective and truly data-driven assessment.

Detected and Monitored Asset Types

CRA detects and monitors a variety of assets, including:

Internet domains

On this Asset type, CRA detects registration information, DNS information, similar domains and Cyber Threat Intelligence information related to what is found on the darkweb.

E-mail

CRA collects information about the number and configuration of email servers and the DNS information related to anti-spam and anti-fraud policies for this Asset type.

DNS

On this Asset type, CRA records information about the configuration of DNS servers and the zones.

Website

CRA detects the software in use to create the website and potentially versions in use on this Asset type, dividing the assets into client libraries, server systems, and external services.

IP

On this Asset type, CRA detects the main open ports and the underlying software and version for each port.

Network

On this Asset type, CRA detects the methods of network announcement, the presence on public databases, and interconnections with other networks.

Autonomous System

For this Asset type, CRA detects information on public databases and interconnections with other autonomous systems and the use of exchanges.

Hosts

This Asset type is mainly used as a link between other Assets. The resulting topology is an important element for assessing the company's posture.

Attack Surface Detection Algorithm

Each Asset-type has its own algorithm for creating derivative Assets. For instance, multiple Asset-types can derive from a Domain, as well as Email, DNS, and IP-type Assets. Meanwhile, the IPs can create a Network-type Asset and potentially further Host-type Assets.

The algorithm for detecting the entire Attack Surface is continuously improving and changing. **The CRA algorithm has been found to successfully detect all Assets exposed on the internet in over 98% of cases.**

If necessary, the user is also able to add additional Assets manually, and CRA will perform further discovery operations on them.

Vulnerability Detection Algorithm

CRA tries to detect potentially dangerous anomalous situations, software versions, and configurations on all Assets detected in the Attack Surface, based on their type.

All detections are done in "passive" mode, without unauthorized access attempts, vulnerability exploitation attempts, credentials or Denial of Service tests.

Each potential vulnerability and dangerous configuration is evaluated and linked to any common Vulnerabilities and exposures (CVE), allowing the user to receive comprehensive information for reporting the vulnerability and fixing it.

Ratings

Following the analysis of each detected Asset, a proprietary algorithm calculates all the information and generates an overall evaluation of the company's cyberposture.

This rating is expressed as a number from 0 (very bad) to 100 (excellent), divided into five categories indicated by color as follows:

0-30	Bad - Intolerable Risk
30-50	Poor - High Risk
50-70	Fair - Medium Risk
70-90	Good - Low Risk
90-100	Excellent - Very Low Risk

A rating higher than 90 is considered very good, a rating lower than 70 means that action needs to be taken. A rating lower than 50 indicates an urgent need to address and fix obvious vulnerabilities.

Where do I access 4Securitas documentation? (manuals, release notes, etc.)

ACSIA documentation can be accessed in the Resources section of this website.

More information on the ACSIA CRA product can be found **Here**

How can I sign up for the ACSIA CRA Service?

If you are not a current 4Securitas customer, please contact- sales@4securitas.com or a local partner to request a call or schedule a demo of the CRA platform.

For more information on ACSIA Cyber Solutions

please use the following link: ACSIA documentation