JOSHUA CYBERISKVISION

Widely spread cyber threats and sophisticated techniques expose organizations to the risk of cyber attacks

CYBER FOOTPRINT

detects and analyzes all digital assets within an enterprise ecosystem, identifies the compromised ones and potential vulnerabilities

Security Postural Assessment

detects, georeferences, and maps external organization assets

Discovery Theft Account

assets potential identity thefts, performed via means of enterprise account compromise

CYBER RISK STATUS

measures and determines the risk level within an enterprise ecosystem

Cyber Risk Scoring

for security incidents and adopted cyber security practices

Supply Chain

extending the Cyber Risk Status Score to subsidiaries, suppliers, and customers

Remediation

identifies types of threats one can be exposed to and possible countermeasures

Market benchmarking

comparing the Cyber Risk Status Score with Third-Parties operating within the same industry

INSIGHT

processes and distributes reports addressing security event issues detected by the network on a global scale

Reports

for intelligence activities including information on threats, vulnerability, and data breach

Special Reports

organized in a well-established layout displaying information on genesys, assessment, and technical features

Opponents

detail description of the main groups of hackers and hacktivists operating at an international level, and their aliases

JOSHUA
CYBERISKVISION

Fighting against violations and reacting to attacks is not enough: you need to know and prevent potential threats

THREAT TRACKER

monitors IoC and tracks the overall level of risk, with a prompt snapshot on the main critical issues and threats

Actionable Intelligence

collects, standardizes, and analyzes in real time all data generated by users, applications, and infrastructures impacting on enterprise security

DATA BREACH DETECTOR

ensures in real time search for, detection, and notification of potential info and data breaches

Infoleak Monitor

monitors OSINT sources to search for and identify potential data leakage

Pasted Monitor

searches through the Deep Web for patterns of interest in order to retrieve information and anticipate potential data breach effects

ADVANCED THREAT HUNTING

sets up custom monitoring mechanisms and tools external to the organization

Underground Attack

creates an information flow on attacks from Dark Net infrastructures

Black Market Monitor

on information within Dark Net networks

Fraudolent Domain Registration

identifies and monitors the activation of profiles created for fraudolent purposes

Attack & Fraud Building Monitor

exchanges messages and extracts information highlighting attack and fraud intents

www.cyberiskvision.com

Almaviva