JOSHUA
CYBERISKVISION

Minacce sempre più diffuse e tecniche sofisticate lasciano le organizzazioni esposte al rischio di cyber attack

CYBER FOOTPRINT

rileva e analizza tutti i digital asset di un ecosistema aziendale, individua quelli compromessi e le potenziali vulnerabilità

Security Postural Assessment

rileva, geolocalizza e mappa gli asset organizzativi esterni al perimetro

Discovery Theft Account

verifica i potenziali furti d'identità, realizzati tramite la compromissione di account aziendali

CYBER RISK STATUS

misura e determina il livello di rischio di un ecosistema aziendale

Cyber Risk Scoring

per gli incidenti di sicurezza e le pratiche di cyber security adottate

Supply Chain

per estendere il Cyber Risk Status Score a controllate, fornitori e clienti

Remediation

identifica le tipologie di minacce a cui si è esposti e le relative contromisure

Benchmarking di Comparto

per confrontare il Cyber Risk Status Score con i soggetti operanti nello stesso settore merceologico

INSIGHT

elabora e distribuisce report specialistici sugli eventi di sicurezza su scala globale rilevati dalla rete

Report

di intelligence contenenti informazioni su minacce, vulnerabilità e data breach

Report Speciali

caratterizzati da una struttura consolidata con informazioni su genesi, assessment e dettagli tecnici

Opponent

descrizione di dettaglio sui principali gruppi di hacker e hacktivisti attivi a livello internazionale e loro alias

JOSHUA
CYBERISKVISION

Respingere violazioni e reagire agli attacchi non basta: è necessario conoscere e prevenire le potenziali minacce

THREAT TRACKER

monitora gli IoC e traccia il livello di rischio complessivo, con una visione immediata delle principali criticità e minacce

Actionable Intelligence

raccoglie, normalizza e analizza in tempo reale i dati generati da utenti, applicazioni e infrastrutture che incidono sulla sicurezza aziendale

DATA BREACH DETECTOR

garantisce in tempo reale la ricerca, la rilevazione e la notifica di possibili info leak e data breach

Infoleak Monitor

monitora le fonti OSINT per ricercare e identificare eventuali leakage di dati

Pasted Monitor

ricerca nel Deep Web i pattern d'interesse con lo scopo di reperire informazioni e anticipare gli effetti di potenziali data breach

ADVANCED THREAT HUNTING

stabilisce meccanismi e strumenti di monitoraggio personalizzati esterni al perimetro aziendale

Underground Attack

crea un flusso informativo sugli attacchi provenienti dalle infrastrutture della Dark Net

Black Market Monitor

sulle informazioni all'interno di reti nella Dark Net

Fraudolent Domain Registration

individua e monitora l'attivazione di profili creati a scopo fraudolento

Attack & Fraud Building Monitor

scambia messaggi ed estrapola informazioni che evidenziano la volontà di attacchi e frodi

www.cyberiskvision.com

AlmavivA