

Open Source Intelligence (OSINT) Strengthens Your Security Posture

Protecting your company's assets goes beyond physical and cyber security. A critical component of risk protection is detecting threats beyond the perimeter. To secure your company's digital and physical assets, and to protect your external attack surface, you must integrate Al-powered Open-Source Intelligence (OSINT) into your company's security strategy. OSINT helps deconstruct complexities in data to expose threats before they impact your brand. Here's six ways OSINT protects corporate assets.



Roughly 200,000 phishing sites

BRAND PROTECTION

are created monthly. Phishing sites, ransomware actors and bogus profiles imitate a brand's look and feel. These sites are used for malicious gain that can cause substantial harm to your organization and your customers. Using Al-powered OSINT tools,

investigate attempts to impersonate your brand, mitigating any negative impact of phishing to your customers. OSINT helps identify and investigate brandjacking through site takeovers, spoofing, phishing and impersonations online.



According to an analysis performed by

DATA BREACHES

breach is \$3.92 million and the average time to identify a data breach inside an organization is 206 days. To prevent damaging leaks of sensitive internal information, corporations must

DataProt¹, the average cost of a data

leverage Al-powered OSINT information to secure their digital attack surface. Because attack vectors are fluid and change continuously, OSINT tools can help businesses identify the earliest signals of high-impact events.



According to Jack L Hayes International LLC, for every \$1 recovered by companies \$33.15

was lost to retail theft.

LOSS PREVENTION

Al-powered OSINT quickly identifies thefts and fraud, identifying hidden relations to recover stolen goods and stop organized retail theft. Coupling this data with digital marketplace

information and the dark web,

companies can recover merchandise, and break up large, organized theft rings to reduce your company's losses. **EXECUTIVE PROTECTION**

For every \$1 recovered by companies



executives are 12 times more likely to be victims of social engineering incidents. Leverage AI-powered OSINT tools to

investigate compromised executive

information (doxing), credential theft, physical threats, and social engineering

According to Verizon's 2020 Data Breach Investigation Report², senior

incidents to quickly identify personal and brand risk, saving investigators hours of manual investigative work.

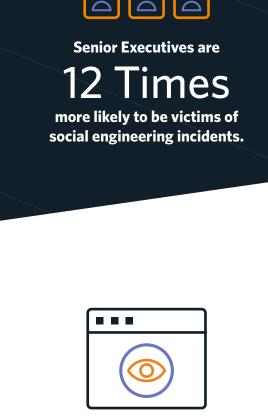
INSIDER THREAT Insiders often have elevated access privileges to sensitive data and

applications. This position of trust can be compromised through malicious intent or inattention, and 60%³ of

companies found it to be increasingly

difficult detect these activities.

before reputational damage occurs or intellectual property is compromised.



AI-Powered OSINT can uncover threats from inside and outside of a company to detect malicious sharing of information

DUE DILIGENCE

supply chain disruptions can cause a massive 62% loss in finances. Third-party risk is a huge factor for companies, regardless of size or location. Disruptions not only effect logistics and financials, but also brand reputation and customer retention as

According to the Zappia website⁴,

well. Integration of OSINT data ensures proper due diligence and vetting of vendors and suppliers. Continuous monitoring can also be used to provide early warning signs and realtime updates for various security threats

like natural disasters, geopolitical risks,



of companies found it to

be increasingly difficult to

detect malicious activity.

Supply chain disruptions

can cause a massive

loss in finances

or targeted threats. To discover how your organization can benefit

> from Cobwebs Web Intelligence Platform contact us today.

> > Book a Demo >

Cobwebs Technologies

Cobwebs Technologies is a worldwide leader in web intelligence. Our innovative solutions are tailored to the operational needs of national security agencies and the private sector, identifying threats with just one click. Cobwebs solutions were designed by our intelligence and security experts as vital tools for the collection and analysis of data from all web layers: social media, open, deep and dark

web. Our web intelligence platform monitors these vast sources of data to reveal hidden leads and generate insights. Our exclusive technology extracts targeted intelligence from big data using the latest

machine learning algorithms, automatically generating intelligent insights.

¹Dataprot.net