DTACT Raven for Anti-phishing

Move swiftly and proactively against cybercriminals. Discover, trace and timestamp cybercriminals' activity and have the evidence ready at your fingertips to join forces with law enforcement agencies and the threat intelligence community.

Raven is a powerful data streaming platform with a modular, brick framework that perform analysis on data aggregate from a big range of endpoints to generate, distribute and retrieve actionable insights when you need them most, and when they matter most.

91% of all cyberattacks start with a phishing message. Phishing is one of the oldest cyberattacks in the book, dating all the way back to 1990 and the industry still doesn't have a fast and effective solution for it. Cybercriminals rely on social engineering and deceptive techniques to trick users into giving away their personal information or account credentials. Think malicious weblinks or attachments and fraudulent data entry forms on fake websites.

Cybercriminals are also getting smarter, being able to bypass new technologies meant to protect organisations' data and systems. SOC teams have two main responsibilities – maintaining security monitoring tools and investigating suspicious activity. However, many existing tools that SOC teams currently use do not integrate seamlessly with one another. Time is wasted on implementation and integration errors rather than analysing the data.

DTACT Raven is a powerful and scalable data streaming and analytics platform that prepares everything needed for automated takedowns of phishing websites.

Phishing is a holistic data problem for all industries and sectors. The sheer amount of data that requires analysis to accurately pinpoint suspicious activity is time-consuming and requires tedious and manual work. The cybersecurity industry and law enforcement agencies need a better solution that is built for cross-functional collaboration to take up legal action against cybercriminals.

CURRENT PAIN POINTS

TEDIOUS & INEFFICIENT ANALYSIS

SOC teams struggle with identifying and dissecting phishing activity creating an accurate timeline of events correlated to an incident with little effort and time. Existing tools are not able to integrate seamlessly or easily with one another and it is currently a long and manual process where analysts go over records individually.

UNABLE TO EFFECTIVELY CREATE CASES FOR LEGAL FOLLOW UP

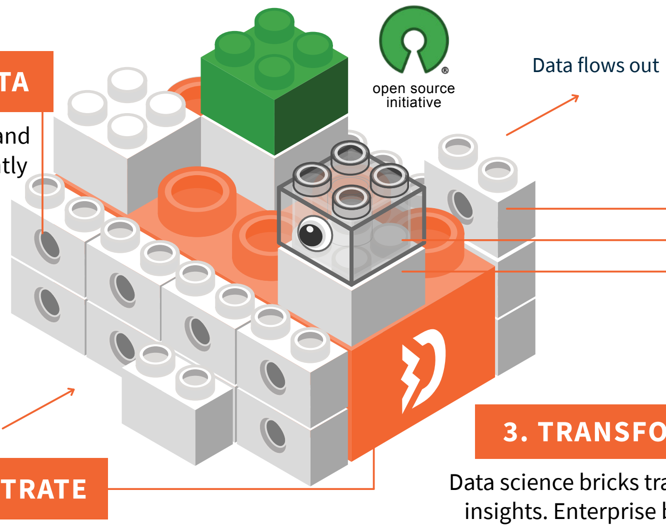
Without an accurate and timely analysis of incidents, SOC teams have difficultly creating comprehensive reports of incidents that include all necessary evidence to build legal cases for recourse to relevant law enforcement agencies.

CYBERCRIMINALS ESCAPE PROSECUTION

Without conclusive supporting evidence to bring cybercriminals to justice, organisations are unable to seek the appropriate legal action undertaken by local law enforcement agencies and continue to plague organisations.

DTACT Raven is a fast, multipurpose open data streaming platform.

DTACT
Purpose. Mission. Impact.



1. CONNECT & CACHE DATA

Connector bricks stream data to and from all systems and tools currently in use to Raven.

2. MANAGE & ORCHESTRATE

The Raven brick handles infrastructure orchestration to run workloads. It manages scheduling, monitoring and error handling.

3. TRANSFORM & EXPORT

Data science bricks transform data to generate insights. Enterprise bricks visualise insights and optimise the understanding, speed and accuracy of threat hunting teams. Connector bricks stream data on to other platforms.

Fig 1. The Raven Brick and our other bricks illustrated to demonstrate the inflow of data from the left, analysis and outflow on the right, to other tools or storage.

KEY BENEFITS

AUTOMATION WITHIN SECONDS

Raven is built to do all the heavy lifting for you so that you don't have to. Where other products take hours to automate, we do it in seconds.

FASTER & BETTER DATA ANALYSIS

Raven is complementary and tool agnostic. Any data source like certificate authorities, domain registers, Spam traps and social media are effortlessly integrated to perform comprehensive analysis and visualise information in graphs and timelines.

COMPREHENSIVE CASE BUILDING FOR LEGAL RECOURSE

Raven provides a complete timeline of the attacker's tracks. Specific snapshots at specific times show the continuous flow of the attackers' environments, allowing organisations to build strong cases against them and take legal action swiftly.

BETTER THREAT INTEL

Raven allows you to easily distribute data to any tool or storage system. Share your findings with other organisations to aid in detecting similar attacks and sync up on defence strategies against cybercriminals.

Initially developed for the national security industry, Raven provides the best critical insights from the large amounts of data locked in corporate and functional silos. It is fast, scalable, and can perform analysis on data aggregate from a big range of endpoints. We prepare everything needed for an automated takedown.

YOUR PARTNER WITH INSIGHTS

Raven is an agile, agnostic and dynamic solution that can be integrated with open source, in-house developed and/or third-party software.

Time is of the essence to act fast and prevent your customers from being manipulated by cybercriminals through phishing websites. Raven provides a proactive approach that easily integrates open source threat intelligence to provide better visibility of your phishing threat horizon.

Raven does all the heavy lifting for you, so that you can dedicate less time and resources to hunting down phishing sites on your own. Focus on meeting your customers' needs, all while knowing that risks to your brand reputation and trust are being mitigated.

ARRANGE A DEMO

Learn more at dtact.com