⊃TACT
Purpose. Mission. Impact.

DTACT Raven for SOC/SIEM

Regain control of your data. Cut software license costs, grant vendor flexibility and increase quality of insights. DTACT Raven significantly reduces your data footprint flowing through your SOC or SIEM system.

Raven is a powerful data streaming platform with a modular, brick framework to build your data infrastructure to generate, retrieve and distribute actionable insights when you need them most.

Initially developed for and implemented with the police and the military, Raven provides critical insights from large amounts of data locked in corporate and functional silos to significantly reduce costs and complexity.

CURRENT PAIN POINTS

Exponentially Increasing Costs

Are you under pressure to reduce costs relating to SIEM systems, L1 to L3 SOC personnel and project implementation?

Myopic Risk Mitigation

Something could be already happening and impact your organisation in the near future. Current security measures in place to prevent, protect, detect, respond and recover from attacks are not adequate. Do you have visibility over what you don't know?

Limited Resources

How do you best allocate your resources to deal with overwhelming amounts of data, data silos, a lack of cybersecurity experts, non-integrated systems and integration problems?

Every organization has data lying dormant across a wide range of sources. Organisations have to aggregate this data to a central point before performing any analysis, but existing systems are not designed to be interoperable and not all data gets integrated. Some, if not most, crash at high volumes resulting in downtimes across your data pipeline.

After aggregation, high data processing license fees put pressure on organisations as they pay for processing sheer amounts of data that often contain a lot of noise.

Aggregate, clean and enrich your organisation's data with DTACT Raven before distribution to other data analysis and storage tools.

Raven is a fast, multipurpose and scalable open data streaming platform.

Easily aggregate large amounts of data from a big range of endpoints before sending them to external storage or other data analysis tools easily with no loss of records.

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

As Raven is complementary and tool agnostic, you won't have to run it at the expense of any of your existing and future vendor tools. In fact, Raven will do most of the heavy lifting for you so that your data will be flowing as quickly as at the snap of a finger. Do you want to spend hours and days rather than weeks and months on data integration?

Raven can generate a cost reduction of up to 40% for any usage-based license costs of your existing software products.

1. CONNECT & CACHE DATA

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

Data flows out

open source initiative

Data flows in

3. TRANSFORM & EXPORT

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

2. MANAGE & ORCHESTRATE

The Raven brick handles infrastructure orchestration to run workloads. It manages scheduling, monitoring and error handling.
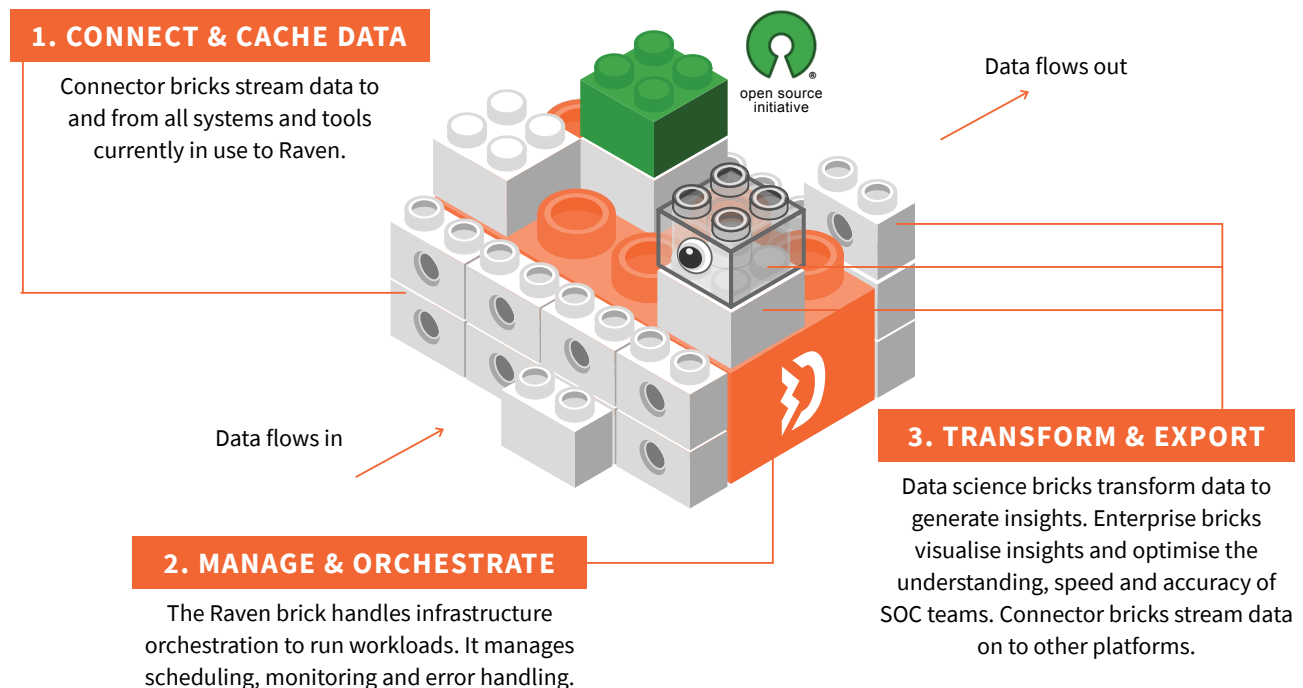
Fig 1. The Raven Brick and our other bricks illustrated to demonstrate the inflow of data from the left, analysis and outflow on the right, to other tools or storage.

EFFECTIVE RISK MITIGATION

Increase visibility across your organisation as you have complete data records from a single dashboard and you now know what you didn't previously.

BETTER UTILISATION OF RESOURCES

The speed and ease of implementation of the platform allow you to perform analysis and right away. Reduce dependence on scarce cybersecurity experts and completely eradicate data silos.

REDUCE COSTS

Reduce license fees of your SIEM systems and project implementation costs. Free up capacity as you rely less on L1 to L3 SOC personnel.

ARRANGE A DEMO

WHERE DATA FLOWS

Learn more at dtact.com

With vendor lock-ins and high data processing licensing costs impacting most organisations, Raven is a better, agnostic alternative that ensures that all your data is properly integrated, cleaned, analysed and sent to other analysis or storage tools. Available on-premise or SaaS.

Our suite of bricks can be used in conjunction with Raven to support a wide range of use cases. The platform also allows you to build your own bricks wherever necessary.