AI-Powered Security Incident Analysis

Find the needle in the haystack — even when you don't know what you're looking for.





THE CHALLENGE: A SEA OF COMPLEX DATA

In the wake of a security breach, organizations consistently face three critical barriers to effective incident response.



VOLUME & COMPLEXITY

100+ GB of deeply nested JSON logs cannot be reviewed manually. Traditional approaches collapse under the weight of modern forensic datasets.



UNKNOWN INDICATORS

You often lack the specific IoCs needed for effective search queries. It's like looking for a needle without knowing what the needle looks like.



TIME PRESSURE

Every hour of uncertainty prolongs risk exposure, jeopardizes compliance, and erodes customer confidence. Speed is critical.

OUR SOLUTION: Intelligent, AI-Driven Investigation

THE TRANSFORMATION PROCESS

CyberSolace transforms hundreds of gigabytes of raw log data into a precise, chronological account of exactly what happened—rapidly and accurately.

- Powered by proprietary analytical tools
- Advanced AI engines
- Operating within the MITRE ATT&CK framework



DYNAMIC INTERROGATION

Rather than relying on rigid queries, our AI agents dynamically interrogate log data the way an expert human analyst would, only faster, without fatigue, and without losing context.

How It Works: Our Core Capabilities

Contextual Schema Mapping



The system automatically ingests and understands complex log schemas, mapping relationships across disparate data sources without manual configuration.

Heuristic Threat Hunting



Instructed to find anomalous behaviors, our AI forms hypotheses, tests them against the data, and follows digital breadcrumbs iteratively through the dataset.

Structured & Unstructured Data Fusion



Our tools bridge the gap between structured log fields and unstructured payload data, correlating events that traditional SIEM platforms would miss.

Expert Analyst Review



All AI findings are validated and contextualized by our experienced security consultants, ensuring accuracy, a professional narrative, and actionable output.

Proven Impact: A Real-World Case Study

Financial Services Provider

100+ GB

of JSON logs analyzed

Second-by-Second

attack timeline delivered

Zero Prior IoCs

required to identify the attack

When a financial services provider faced a suspected breach with over 100 GB of data and no indicators of compromise, our AI-powered investigation uncovered lateral movement hidden within legitimate traffic. We delivered a definitive, second-by-second timeline of the threat actor's activities, enabling a highly targeted remediation.

Key Business Benefits



Identify & Mitigate Threats

Proactively detect and resolve risks before impact.



Accelerate Efficiency

Streamline workflows and speed up time-to-market.



Scale Operations Seamlessly

Expand capacity and performance effortlessly.



Optimize Costs & Secure Value

Maximize savings while ensuring financial protection.

NEVER GET LEFT IN THE DARK

Incident Response & Clarity When It Matters Most.



When a breach occurs and the data is overwhelming, we ensure you can respond with **SPEED** and **CONFIDENCE.**

Contact us today to discuss how we can support your incident response capability.

www.cybersolace.co.uk