



KryptoKloud

SECURITY MADE SIMPLE

Industries which benefit from KryptoSOC 360

Largescale enterprises around the world, including global industry leaders, count on the KryptoSOC 360 advanced threat detection and response platform to protect their most valuable assets. Industries include:

- Banking / Finance
- Insurance
- Healthcare
- Retail / Real Estate
- Industry
- Critical Infrastructure
- Government
- Education
- Legal

About KryptoKloud

KryptoKloud is a UK-based company delivering security solutions to companies of all types and sizes. KryptoKloud simplifies security by providing KryptoSOC 360, a scalable, easily deployable cyber protection platform that delivers prevention, precise findings and automated response to advanced threats with near-zero false positives, shortening the time from detection to resolution and limiting damage to an organisation.

To learn more contact us at: cic@kryptokloud.com

KryptoSOC's key differentiators

- Covers tens of thousands of endpoints in as little as 2 hours
- Heuristic analysis engine identifies anomalous behaviour and protects against insider threats
- Cross correlation across networks, users, files and endpoints means full visibility across the network
- Enables creation of rules for automated remediation and automated Incident Response
- Provides a complete solution for organisation cyber security including anti-malware, anti-ransomware, and anti-exploitation capabilities.
- "Eyes-on-glass" Incident Response team with you every day, 24/7



KryptoKloud

SECURITY MADE SIMPLE

KryptoSOC 360: Security Made Simple

In today's rapidly evolving threat landscape, an organisation's security practices are as important as their product or service.







In the effort to protect their assets, organisations employ multiple security solutions, trying to anticipate potential threats and plug vulnerabilities before they happen.

At the same time, the success and efficiency of organisational cyber security is affected by factors such as budget and prioritisation of needs. Organisations frequently find themselves scrambling to keep their assets safe as new threats arise, and fighting to get their security needs met as funding priorities change. Regardless of the reason, solution purchases, manpower and other resources frequently end up on the cutting board.

Under these circumstances, as organisations strive to establish a secure cyber environment, IT security teams often find themselves using a variety of different security solutions to meet their detection, protection and response needs. Security analysts spend hours integrating between the mass of information coming at them from multiple security solutions not 'speaking the same language.' It is easy to see how visibility is lost as the real threats end up hidden in a mountain of false positives.



KEY BENEFITS

-  **24/7 Threat Response**
With KryptoSOC, threats are detected and dealt with 24/7 ensuring your organisation is always protected.
-  **Automated Ransomware Isolation**
Infected endpoints are instantly isolated from the network to ensure no malware propagates across the organisation.
-  **Lower Risk**
Helps prevent data breaches from those with access to critical business assets and information.
-  **Reduce Costs**
Various resilience capabilities provided in a single agent provide a more cost-effective and integrated solution.
-  **GDPR Alignment**
Implementing KryptoSOC will help ensure you have the right measures in place for GDPR compliance.
-  **Protects In Minutes**
Setup of KryptoSOC is quick and easy, ensuring no business down time.

The KryptoSOC 360 Platform

The KryptoSOC 360 advanced threat detection and response platform simplifies enterprise security by providing a holistic answer to all the organisation's protection and prevention needs. KryptoSOC 360 reduces security spend by providing multiple capabilities in a single solution, while putting less demand on organisational resources, manpower and budget. Additionally, the KryptoSOC 360 platform provides the highest level of enterprise security by correlating indicators across systems, thus increasing visibility and accuracy of detection throughout the organisation, without the need for multiple cyber security solutions.



How Do We Do It

With no installation necessary, the KryptoSOC 360 platform can be launched across tens of thousands of endpoints in as little as 2 hours. Once in place, the KryptoSOC 360 platform begins analysing and correlating indicators across the network, files, users and endpoints, issuing risk rankings for potentially anomalous behaviour, ensuring lowest false positives and achieving a clear picture of attack operations over time. KryptoSOC 360's machine learning and automated remediation capabilities mean that processes are streamlined, putting less strain on IT security staff.



The KryptoSOC 360 Capabilities

The KryptoSOC 360 advanced threat detection and response platform provides a comprehensive suite of enterprise security capabilities to organisations that require the highest level of protection and prevention across thousands of endpoints.



Endpoint Monitoring & Detection

The KryptoSOC 360 platform rapidly deploys and detects threats across endpoints in under 2 hours. As part of a comprehensive solution, KryptoSOC 360 correlates indicators and provides network visibility.



Threat Intelligence

The KryptoSOC 360 platform utilises the latest Threat Intelligence information. This provides organisations with an extra layer of protection against suspicious and malicious activities.



Network Analytics

The KryptoSOC 360 platform provides full visibility into and analysis of network traffic and activity across the organisation.



User & Entity Behaviour Analytics

The KryptoSOC 360 platform's UEBA capabilities help IT security teams identify rogue insiders, compromised accounts and targeted attacks before the damage is done.



24/7 Breach Response

KryptoSOC 360 provides 24/7 Cyber Breach Monitoring Capability in order to respond to detected breaches and threats in real-time.



Firewall Security

The KryptoSOC 360 platform has a full firewall capability that can be easily configured and optimized. This can replace an operating system's firewall or sit on top as an additional layer of protection.



Folder Monitoring

With the KryptoSOC 360 platform, files can be marked for close monitoring, triggering alerts if someone attempts to move or access without clearance, giving visibility into user activity around critical assets.



Patch Management

The KryptoSOC 360 platform can perform patch management on all installed endpoints, providing updates for a broad range of vendors as well as critical operating system patches.



Forensics

KryptoSOC 360's cyber team can perform deep-dive investigations, to rapidly identify and investigate suspicious incidents before they escalate.

Managed Detection & Response: KryptoKloud's Proactive Solution

Due to the ever-changing nature of our current cyber landscape, a reactive solution is no longer sufficient to protect an organisation from attack. In order to stay on top of the new threats and vulnerabilities coming to light each day, it is essential to adopt a proactive solution such as a Managed Detection & Response (MDR) service.

With an MDR service, heuristic AI-driven analysis cuts down the false positives and provides instant response to detected threats. This approach is critical in order to respond to issues as they arrive in real-time as it allows organisations to focus their attention and resources on genuine verified threats. Traditional cyber protection from Managed Security Service Providers is becoming increasingly antiquated since the analysis and response time is delayed from hours to days due to the slow and cumbersome nature of manual analysis.

In addition, this manual type of analysis and response lacks the effective auto-containment capabilities of an MDR solution which can isolate an infected machine from the network, preventing any malware or cyber attacker from being able to spread across the organisation. Whereas, with the complex automation built into MDR solutions like KryptoSOC 360, thousands of devices and files can be scanned and analysed in minutes allowing for action to be taken in real-time before an attack can propagate across a network.