krome

SOC

MANAGED SECURITY OPERATIONS CENTRE

A NEW ERA OF CYBER SECURITY

With the constant rise of sophisticated threats, a new era of cyber protection is required.

Having the right IT security strategy and the most advanced security solutions in place can ensure that you control and secure your data from malicious changes, deletions or even from accidental or unauthorised disclosure.

IT security, or data security is not just about protection from hackers, although cyber security protection should certainly be included in your overall security strategy. IT security solutions are used to protect organisations from inside and outside threats.

Organisations rely on their information systems to support their business activities, this intrinsically makes them more attractive to cybercriminals, threats from viruses, or even their own staff, albeit malicious or not. Ensuring the sovereignty of your data can make the difference between failure and success for your business.

Your IT security should include the endpoints, network security, cyber security, on-premise and cloud-based systems, as well as your physical data, it should protect your entire infrastructure from risk. Having a comprehensive IT security strategy ensures that all your company information is always protected, preventing unauthorised access, misuse, corruption or deletion of data.

INCREASE IN CYBER CRIME

In this era of sophisticated threats, with offensive AI tactics exacerbating attacks, it is critical for organisations to embrace new technologies which can adapt to attackers' advanced techniques.

Cyber Threat & Ransomware Increases

- In 2022, 71% of companies worldwide were affected by ransomware, with 493.33 million ransomware attacks detected.
- 39% of UK businesses reported suffering a cyber attack in 2022.
- The average cost for UK organisations to rectify the impacts of ransomware attacks was £1.08 million, 13% of UK organisations ending up paying the ransom demanded.
- In 2022, internet users worldwide discovered over 25 thousand new common IT security vulnerabilities and exposures (CVEs), the highest reported annual figure to date.
- Global ransomware damage costs are predicted to exceed $265 billion By 2031.

The total number of Internet connected devices worldwide is projected to amount to 30.9 billion units, by 2025. Without the correct technologies and processes to protect our businesses, we are unnecessarily exposing ourselves to risk.

It is critical that we take control of our threat vectors, but managing a system that encompasses all elements of IT security can be onerous. Cybercrime does not work on a 9 to 5 schedule and ensuring that your systems are constantly monitored can be costly and time consuming. Attacks are often planned at targeted times, outside of operational hours, when cybercriminals know they will have time to execute and gain control over your systems and data. It is difficult to always monitor everything, but it is not impossible.

WHAT IS A SOC?

A Security Operations Centre enables you to monitor all elements of your network on a constant basis, 24/7/365, reacting in real time to threats and stopping malicious behaviours in their tracks.

A Security Operation Centre (SOC) is a centralised operation within a business that utilises a mixture of people, processes, and technology to monitor an organisation's security position, while detecting, preventing, analysing, and responding to any cyber security attacks.

The key aims of a SOC are:

- To detect and respond to threats, analysing pertinent information to ensure the security of your network and the integrity of your data.
- To increase resilience by analysing the ever-evolving threat landscape of both malicious and non-malicious, internal and external threats.
- To identify and address negligent or criminal behaviours by analysing and comparing behaviours and trends in order to stop nefarious activity before a critical event can occur.
- To respond swiftly and effectively to incidents to minimise the disruption that attacks can cause.
- To produce clear and understandable management information detailing the threat landscape, leading to strategic improvements of your environment to further enhance your security standards.

Standing up and running an internal SOC however is a significant investment, which is why for most enterprises, outsourcing your SOC requirement to a trusted partner is the most commercially effective solution.

KROME'S MANAGED SOC

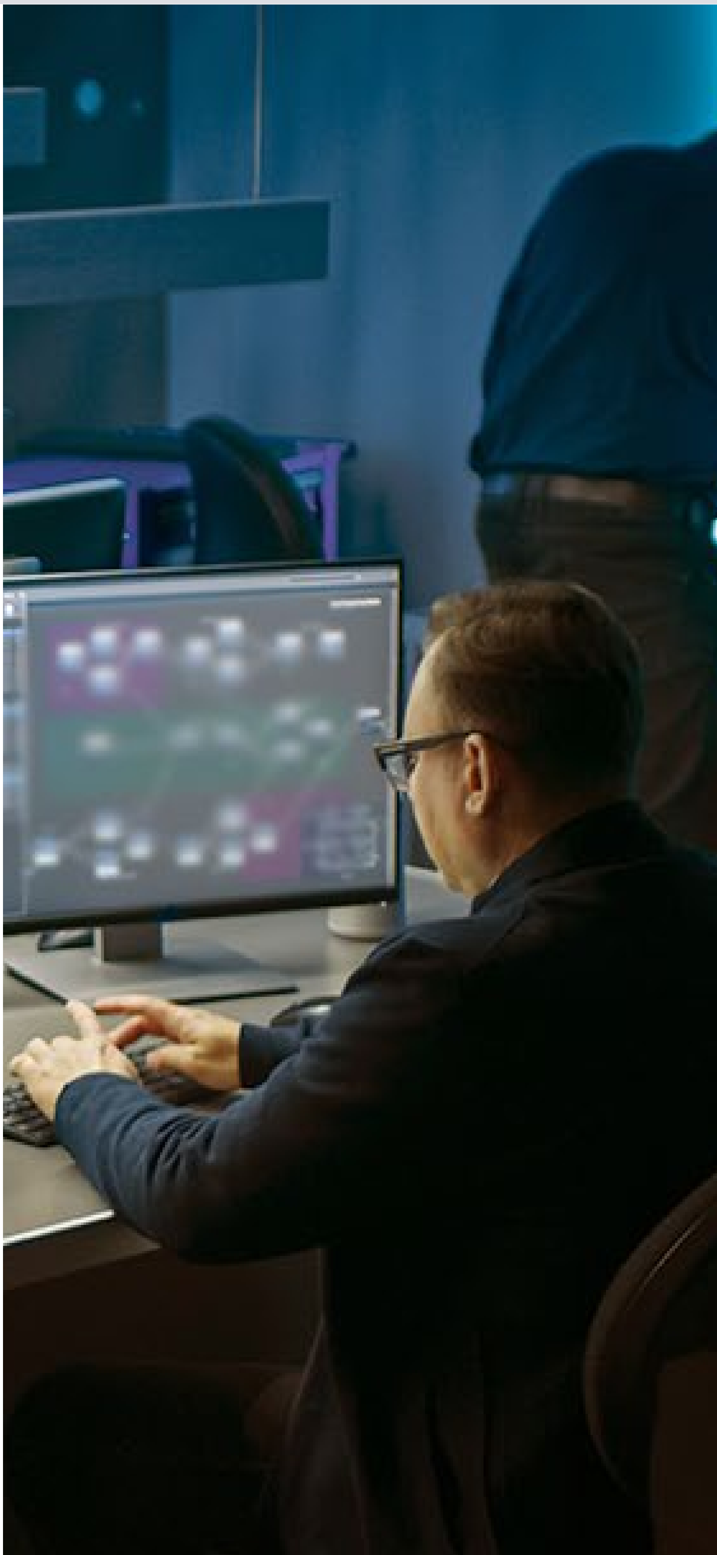
Our Security Operations Centre (SOC) is built on industry leading cybersecurity solutions and manned 24/7 , with a human response team monitoring and responding to threats in real-time.

Our dedicated team of security consultants utilise industry leading technologies, from Vendors such as Darktrace, Palo Alto Networks and Microsoft, to take feeds from your Enterprise, looking for any and all anomalous behaviours that need to be addressed.

Our SOC is manned 24/7 and is monitored in real time with threats responded to as they occur. We work with you to define what your threat response needs to be, putting in place the correct procedures to compliment your security strategy.

Our response can range from highlighting potential threats and informing the relevant contacts at our client's sites (known as MDR – manage, detect and response) through to proactively neutralising the threat at source by taking control of your systems and shutting down services as necessary (how Krome view MDRR – manage, detect, respond and remediate).

Our ability to remediate security breaches is an uplift on what pure MDR providers can provide, giving you extra levels of assurance that your enterprise is subject to the highest levels of threat prevention available.



COMPONENTS OF THE SOC

SIEM / SOAR: Microsoft Sentinel

Built on the Microsoft Azure platform, Sentinel is a capacity licensed SIEM/SOAR solution. Sentinel collects data from devices, users, apps and servers, on any cloud. It uses the power of AI to ensure that real threats are identified quickly.

Perimeter Protection: Palo Alto Networks PA Series

Industry wide acceptance as the best firewalls available, Palo Alto Networks next-generation firewalls detect known and unknown threats. Krome were one of the first Palo Alto Networks partners in the UK, with over 10 years experience.

Endpoint Protection: Microsoft Defender/PAN Cortex XDR

Modern detection and response technology for endpoint protection delivered by Palo Alto Networks Cortex XDR or by Microsoft Defender, quickly finding and stopping targeted attacks, insider abuse and compromised endpoints.

Network & Cloud Protection: Darktrace Enterprise Immune System

The Enterprise Immune System harnesses scalable, self-learning AI to understand the digital DNA of an organisation and illuminate unpredictable cyber-threats.

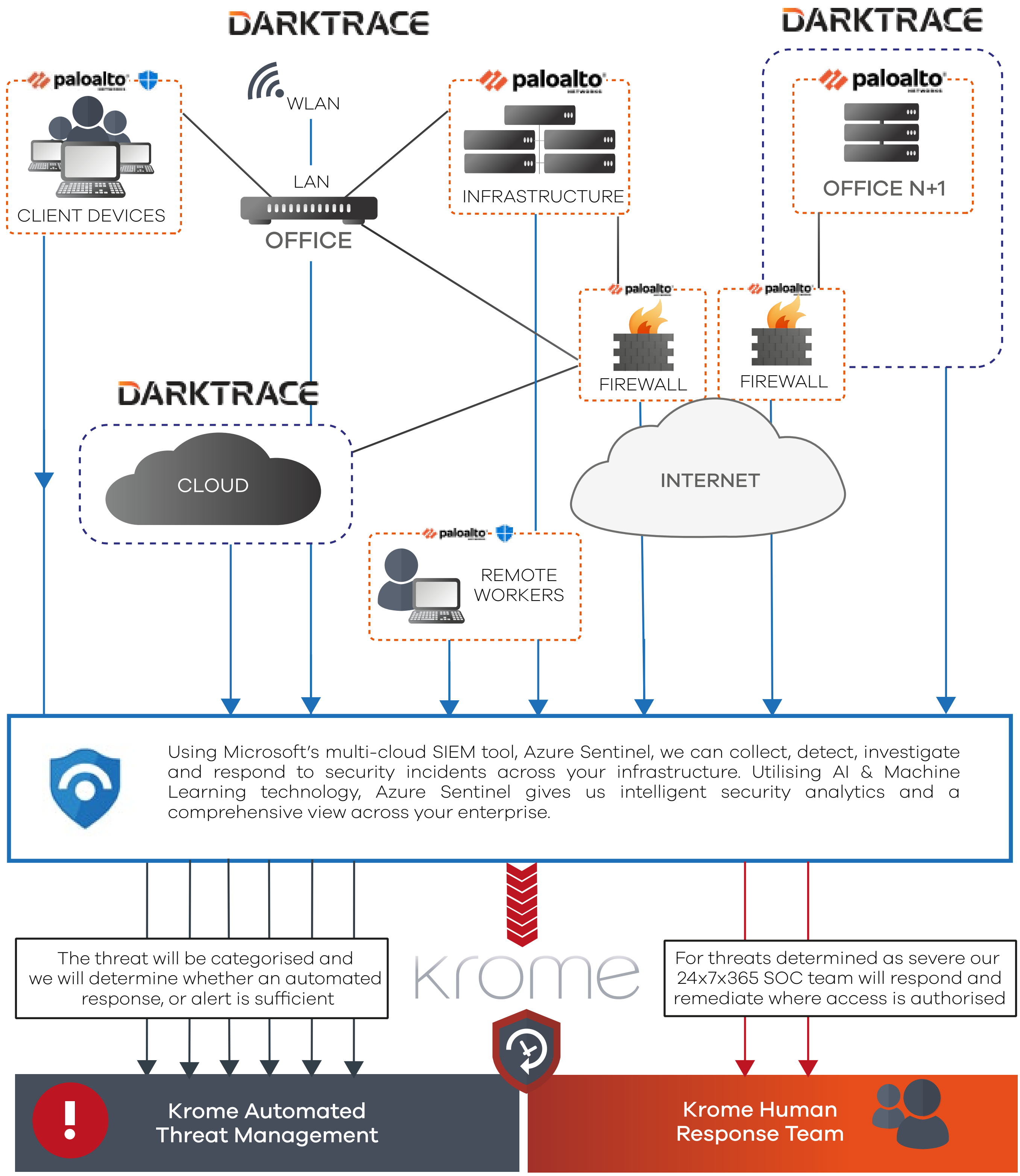
Human Monitoring and Response: Krome Technologies

Our SOC is manned 24/7 by an experienced team of technologists, monitoring and responding to threats in real-time, as they occur. For threats determined as severe our SOC team will respond and remediate where access is authorised.

Reporting: Microsoft Power BI

Using Power BI's native integration with Sentinel we provide data visualisations and real-time reporting on the overall performance of the service.

HOW DOES THE SOC WORK?



DARKTRACE

CLIENT DEVICES

WLAN

LAN

OFFICE

INFRASTRUCTURE

DARKTRACE

OFFICE N+1

FIREWALL

FIREWALL

DARKTRACE

CLOUD

INTERNET

REMOTE WORKERS

Using Microsoft's multi-cloud SIEM tool, Azure Sentinel, we can collect, detect, investigate and respond to security incidents across your infrastructure. Utilising AI & Machine Learning technology, Azure Sentinel gives us intelligent security analytics and a comprehensive view across your enterprise.

The threat will be categorised and we will determine whether an automated response, or alert is sufficient

krome

For threats determined as severe our 24x7x365 SOC team will respond and remediate where access is authorised

Krome Automated Threat Management

Krome Human Response Team

KROME TECHNOLOGIES

Fully Leverage the Power of Advanced Cyber Security Solutions with Krome Technologies

We believe that every organisations IT security strategy should be aligned to the individual needs of the business. Our team of specialist security consultants can advise you on all aspects of implementing an effective IT security strategy; minimising risk, maintaining the integrity and confidentiality of sensitive information, meeting compliance regulations, blocking access and preventing successful cyber-attacks on your organisation.

Krome's specialist security solutions team consists of a number of highly experienced security professionals who can help you to leverage the power of advanced cyber security solutions from the initial design, through to the delivery support and management.

Krome Technologies work with small, medium and enterprise companies; assessing business objectives and implementing technology solutions that will help achieve them; by designing and implementing innovative solutions and providing the highest quality technology based services Krome Technologies will help meet our client's technology and overall business goals.

Krome Technologies' overall objective is to deliver clients with the highest level of service and technical ability across each area of our business. To speak to a member of the Krome team about your cyber security requirements please contact us on 01932 232345.