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 2024 Ransomware attacks in the UK increased by 70%.
- The UK was the second-most targeted country in the world for cyber-attacks, after the US.
- Half of UK businesses (50%) and around a third of charities (32%) report having experienced some form of cyber security breach or attack in the last 12 months.
- Cybercrime cost UK businesses an estimated £21 billion per year.
- The average cost of a cyber-attack to a UK business was £10,830.
- 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 40 billion units, by 2030.

Without the correct technologies and processes to protect our businesses, we are unnecessarily exposing ourselves to risk.

It's critical to maintain control over your threat vectors, but managing a comprehensive IT security system can be demanding.

Cybercrime doesn't follow a 9–5 schedule, and ensuring around-the-clock monitoring is both costly and time-consuming. Attacks are often timed outside operational hours, when criminals know they have more opportunity to gain access. Continuous monitoring is challenging, but achievable with the right approach.

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

Krome's Managed SOC operates 24x7x365 to protect your critical infrastructure, data, and users.

We use Microsoft Sentinel as our SIEM and SOAR platform, coupled with Microsoft Defender for Endpoint, Identity, Office 365, and Cloud Apps to provide extended detection and response (XDR) capabilities.

Our SOC is staffed by experienced analysts who continuously monitor environments, investigate alerts, respond to incidents, and proactively hunt for threats using Microsoft's security tools.

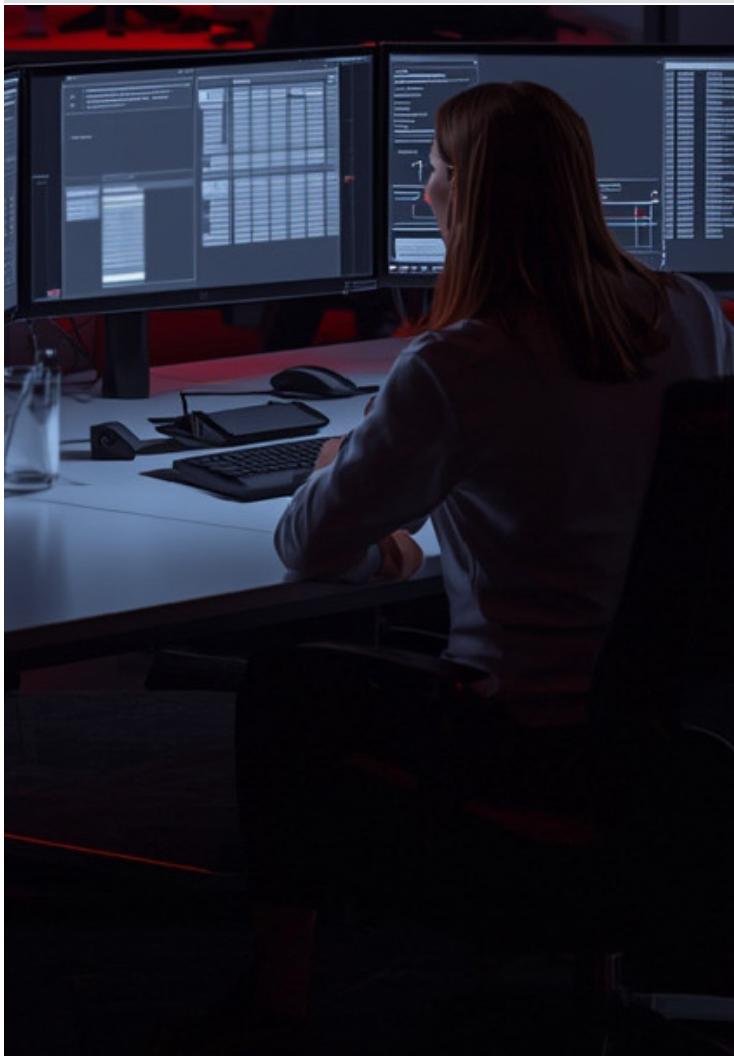
MDR Vs MDRR: Going Beyond Detection

Krome's SOC does more than just notify you of threats - we take action.

- **MDR (Managed Detection & Response)**: Identifies and alerts you to potential threats.
- **MDRR (Managed Detection, Response & Remediation):** Goes further by containing, neutralising, and recovering from incidents on your behalf.

This uplift on traditional MDR gives our clients the highest assurance that their enterprise is subject to the strongest levels of protection.

Krome's Security Operations Centre (SOC) is built on Microsoft Security solutions and manned 24x7x365, with a human response team that monitor and respond to threats in real-time.



RESPOND. REMEDIATE. REPORT.

24x7 Monitoring & Human Response

Our UK-based SOC team operates around the clock, providing real-time monitoring, analysis, and intervention. Using Microsoft Sentinel, we apply correlation rules and automation to detect both known and unknown threats across the environment.

When a threat is identified:

- **Automated responses** can neutralise low-level incidents at speed.
- **Human analysts** investigate and respond to more complex threats in real-time.
- **Remediation** can be executed where authorised, ensuring incidents are fully contained.

Reporting & Service Reviews

Using Microsoft Sentinel's Power BI integration, we deliver visual dashboards and monthly reports on SOC performance, incident activity, and threat trends. These are delivered by your Krome Client Success Manager in a dedicated monthly service review meeting.

The review process ensures:

- **Continuous improvement** in detection and response.
- **Visibility of security posture** against business objectives.
- **Strategic guidance** to reduce long-term risk.

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. Whilst our preferred Firewall vendor is Palo, we are able to support other firewall vendors should you use them.

Endpoint Protection: Microsoft Defender for Endpoint

Modern detection and response technology for endpoint protection delivered by Microsoft Defender for Endpoint, quickly finding and stopping targeted attacks, insider abuse and compromised endpoints.

Cloud Protection: Microsoft Defender for Cloud

Microsoft Defender for Cloud, provides continuous security posture management and threat detection across hybrid and multi-cloud environments. Identifies misconfigurations and detecting active attacks to safeguard workloads and data.

Identity Protection: Microsoft Defender for Identity

Advanced identity threat detection with Microsoft Defender for Identity, monitoring user behaviour and Active Directory activity to detect compromised accounts, lateral movement, and insider threats.

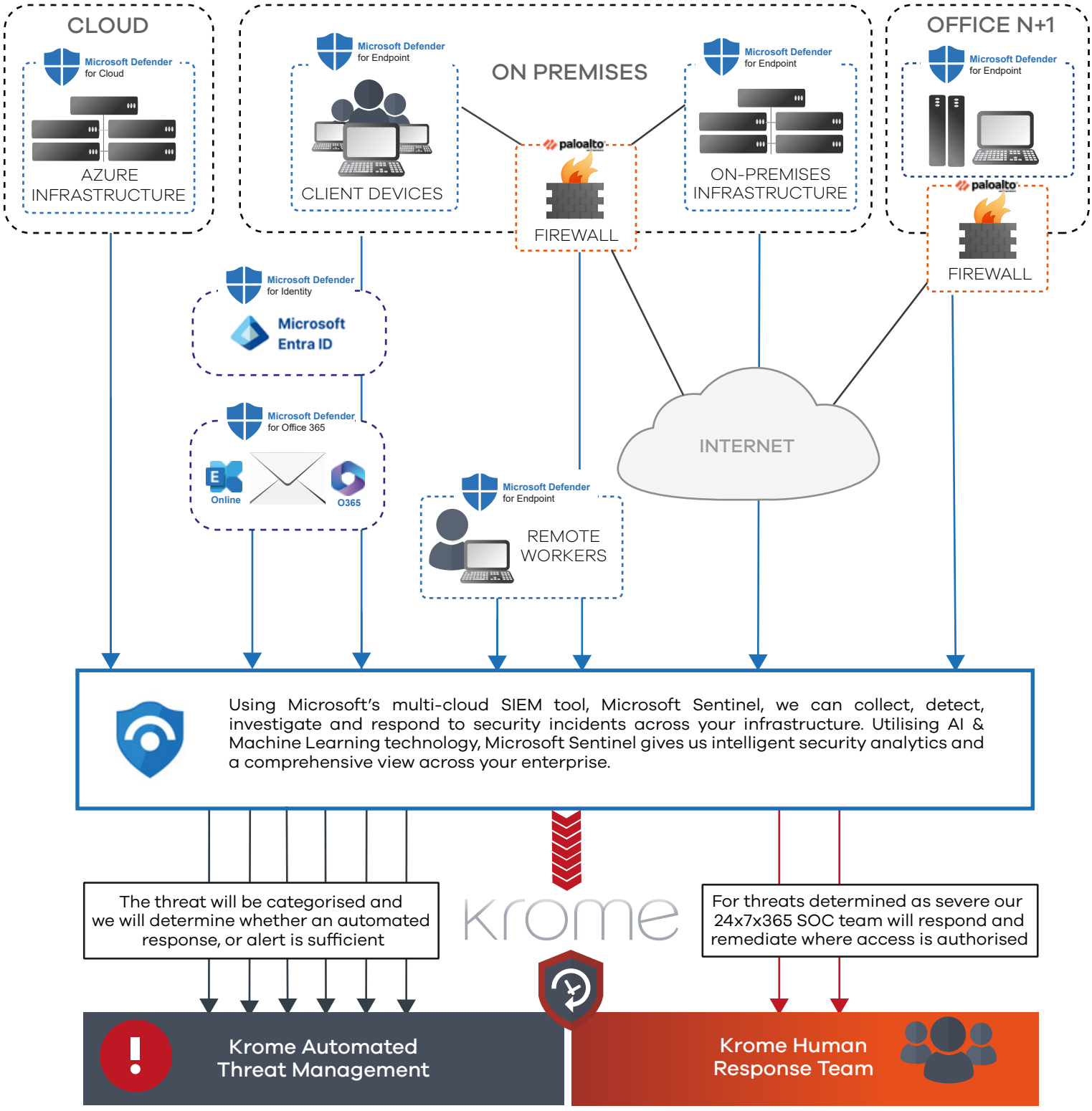
Email & Collaboration: Microsoft Defender for Office 365

Microsoft Defender for Office 365, securing email and collaboration tools against phishing, malware, and business email compromise. Detects and blocks threats in real time, while automated investigation and response capabilities help contain and remediate attacks.

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.

HOW DOES THE SOC WORK?



Krome Technologies Ltd
Head Office: Krome House Pound Road Chertsey Surrey KT16 8ER Tel:01932 232345
Manchester Office: Krome House Quays Reach Salford Manchester M50 2ZY Tel: 0161 868 1360
www.krome.co.uk | sales@krome.co.uk

krome

KROME TECHNOLOGIES

Fully Leverage the Power of Advanced Cybersecurity 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 cybersecurity 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.

Krome Technologies Ltd
Head Office: Krome House Pound Road Chertsey Surrey KT16 8ER Tel:01932 232345
Manchester Office: Quays Reach Salford Manchester M50 2ZY Tel: 0161 868 1360
www.krome.co.uk | sales@krome.co.uk

krome