Arrow's managed micro-SOC service

A proactive approach to threat detection

In today's rapidly evolving digital landscape, businesses are constantly grappling with increasingly sophisticated cybersecurity threats. From data breaches to ransomware attacks, the challenges are manifold and ever present. To address these pressing concerns a proactive and vigilant security approach is non-negotiable.

Arrow's managed micro-SOC service offers you an easy, scalable and cost-effective solution, accessible to organizations of all sizes to fortify their cyber defences. Ease the pressure on your in-house teams: our experts become an extension of your existing resources helping you ensure the highest security posture for your customers.

Arrow's Micro-SOC offering

A light touch security operations centre as a service, powered by Microsoft's cutting-edge technologies, providing a proactive approach to threat detection with continuous security improvements. Based on a subscription model, with no long-term commitment, you benefit from high qualified security analyst time, delivering actionable recommendations to effectively safeguard organization assets. With flexible (3, 6, 12 months) terms available, our vigilant analysts keep a watchful eye on Microsoft Sentinel bringing to your attention any vulnerabilities, necessary configuration adjustments, or policy changes that are essential for mitigating risk.

Bolster your defences and ensure rapid threat detection with Arrow's micro-SOC, including the following services:

- Daily monitoring Microsoft Sentinel
- Active looking for potential indicators of compromise (IoCs)
- Incident assessment and classification
- Alert to attacks
- Technical advice via tickets to open issues
- Assessing & actioning any alert raised in Sentinel
- Weekly reports with all findings and recommended actions to make improvements
- Monthly reports with service review, comprehensive security posture summary and recommendations

Setup and configuration

Proactive monitoring

Actionable recommendations

Comprehensive reporting

Micro-SOC setup: Your first line of cyber defence

Our managed micro-SOC service can be rapidly set up, swiftly ingesting logs into Sentinel from Office 365 and Defender. This unparalleled time-to-value ensures that your security infrastructure is operational and effective in the shortest possible time.

Start your micro-SOC journey today:

- **Customised setup**: Our experts collaborate with your team to design and configure a micro-SOC tailored to your organisation's unique requirements, priorities, and existing technology stack.
- **Security stack integration**: Seamlessly integrate Microsoft Sentinel, Microsoft Defender for Endpoint, and Microsoft Defender for Office 365, ensuring your security tools work harmoniously to monitor and protect your digital assets.
- **Policy and configuration**: Define security policies and configurations that align with best practices and industry standards, optimising your defences and ensuring your network is resilient.
- **Threat detection rules**: Establish customised threat detection rules, tailored to your specific environment and potential threat landscape, enabling swift incident identification.
- **Incident reporting**: Receive timely and comprehensive incident reports, complete with actionable insights, to address vulnerabilities and bolster your security posture.

Supplementary services

Incident response services

Don't wait for a security incident to escalate. Be prepared with our incident response service days, a vital component of your proactive cybersecurity strategy. Add a pool of days to your Arrow's managed micro-SOC service to bolster your incident response capabilities and protect your digital assets effectively. Our incident response service days offer you a dedicated expert team, poised to respond and mitigate security threats with agility and precision.

- **Further investigation into P1s/P2s**: In the event of a security incident, our seasoned incident response team is at your service. With a single day of dedicated support, we act promptly to limit the damage and minimise the potential impact.
- **Prompt response to a cyber breach:** When critical cybersecurity incidents strike, time is of the essence, and we help bring systems back up and running.
- **Forensic analysis**: Leveraging cutting-edge forensic techniques to investigate the incident thoroughly, our experts will uncover the root cause and provide you with a detailed analysis of what transpired.
- **Containment strategies**: Swift containment is essential to prevent further damage. We deploy targeted strategies to isolate the incident and prevent it from spreading throughout your network.
- **Remediation planning**: A critical step in incident response is devising remediation promptly. We provide recommendations and guidance on how to rectify vulnerabilities and prevent future incidents.
- **Communication and reporting**: Timely and transparent communication is key during a security incident. We keep you informed throughout the process and provide comprehensive incident reports for your records.

Supplementary technical support

Prepare your organisation for a secure and resilient future with our cybersecurity specialised technical support services days. Additional activities can be provided as airtime to be used à la carte by our seasoned cybersecurity professionals for:

- Comprehensive security assessment of your current environment.
- Development, refinement and implementation of security policies and configurations that align with industry best practices and your organisation's unique need.
- Report discussion and further security technology optimisation to leverage your investments to the full potential
- Tailored technical support.

Enhance your cybersecurity strategy. Start your micro-SOC journey with Arrow.

Ready to get started? Contact us