Security Operations Centre (SOC)

Actively Monitoring Your Security

AZTech IT take a multi-layered approach to IT Security to protect you against the latest security threats.

Keeping your organisation secure has never been so vital - cybercriminals are finding more ways to infiltrate your business, and if you aren't monitoring for suspicious activity, your organisation is easier to breach.

Our Security Operations Centre will monitor and scan for suspicious activity across your systems, searching and identifying anything that may signify a security breach or compromised system.

Our SOC offers a hassle-free and cost-effective solution for organisations that may not have the resources to build their own in-house operation.

Unlike traditional antivirus software that simply identifies and quarantines files suspected of Malware, AZTech's Managed Detection and Response is designed to look for and record system activity on your endpoints, providing you with the real-time visibility you need.

Focusing on the detection of suspicious activities

We monitor everything from endpoints, websites and apps, to networks, servers and databases.

We're there to help ensure any possible security incidents are promptly and correctly identified.

Organisations are constantly adding to their endpoints, whether it's desktops, smartphones or even Internet of Things (IoT) - there are now countless ways for cybercriminals to gain access to your data.

Endpoint visibility is critical to every organisation as antivirus software can only protect you so far against cybercrime.

Many types of Malware are hard to detect with traditional methods, such as file-less malware that operates in your computer's memory, hidden from malware signature scanners.

Enhance your security with a Security Operations Centre (SOC) from AZTech IT Solutions

www.aztechIT.co.uk | email: info@aztechIT.co.uk | phone: 03300 949 420

Managed Detection & Response (MDR)
Managed Detection and Response from AZTech IT scans your endpoints for any type of abnormal activity and sends alerts to the security team.

This way any type of malware, whether it's hidden from malware signature scanners or easily detected, our SOC team will be alerted and begin investigating further, isolating and removing the issue, so you can continue business as usual.

Dark Web Monitoring
We monitor the dark web daily, scanning for your organisation's credentials. You'll receive daily reports of any compromised data, including passwords and where they were stolen (if available).

Passwords and personal data are being sold on the Dark Web every day for as little as £2, this includes credit card details and more.

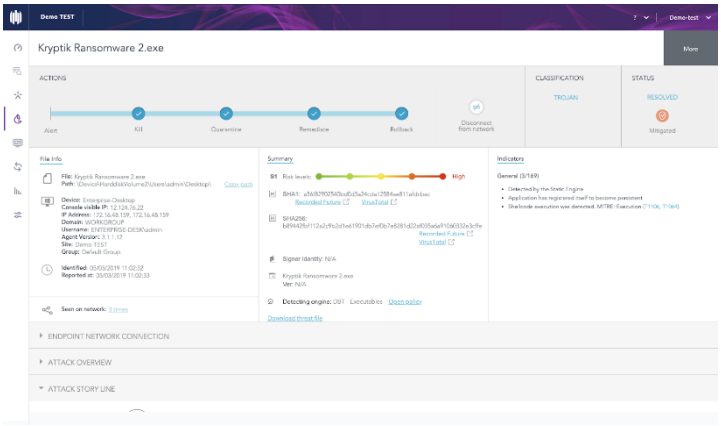
Dark Web Monitoring searches the Dark Web for compromised data so you can act before a breach happens.

Secure DNS (Web Filtering)
Secure DNS helps to protect your business while your users are online, regardless of their location.

It protects and blocks malware, phishing, spoofing, malicious sites and more – helping to keep your data safe.

Managed SIEM
Leveraging SIEM technology to collect, analyse and correlate information from network devices, endpoint logs and threat intelligence feeds.

This information is used to identify security incidents, policy violations, fraudulent activity, and other threats – when these activities are identified, our SOC quickly takes action to mitigate the attack while providing advanced mediation documentation and recommended next steps.



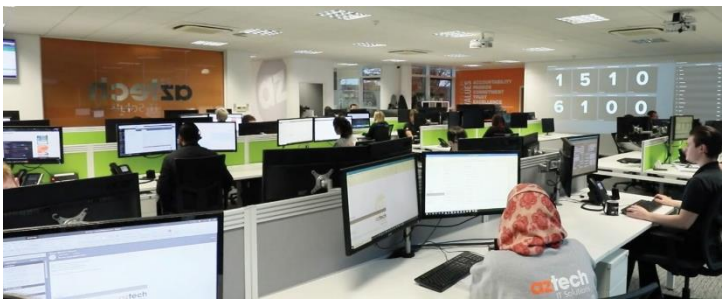
24/7/365 Detection & Response
With 24/7/365 threat detection and response, our Security Operation Centre (SOC) Team gain real-time visibility of cyber threats to your endpoints and network.

By utilising multi-layered best of breed security tools and continuous monitoring, any anomaly or suspicious activity will alert our security team to investigate and respond immediately, 24/7.

Threats are evaluated and dealt with accordingly, allowing our team to respond and diffuse directly, and for you to focus on your business.

Cloud Risk Watch
We utilise best of breed solutions to protect your digital environment from spam, malware, malicious links, phishing and more.

High-risk, abnormal usage, and evolving threats are identified within your Cloud environments, gaining visibility and uncovering Shadow IT, to help protect your organisation against cybercrime.



Enhance your security with a Security Operations Centre (SOC) from AZTech IT Solutions

www.aztechIT.co.uk | email: info@aztechIT.co.uk | phone: 03300 949 420

- **Monitor**
  With our MDR Solutions, your endpoints will be monitored daily with real-time visibility to collect activity data that may indicate threats.

- **Analyse**
  We can analyse the collected data to identify threat patterns to help detect any breach attempts and stop them immediately.

- **Fast Response**
  Fast and accurate response to remove, contain or stop attacks before they become a breach, so you can continue business as usual.

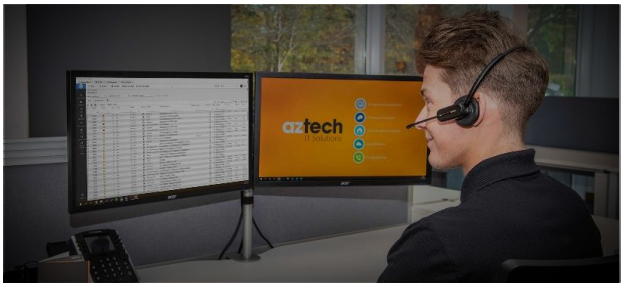
- **Research**
  Analysis tools research known and identified threats and search for suspicious activity.

Why is having a SOC important?
Every device connected to your network is a potential entry point to your data, making it a target for cybercriminals.

Zero-day attacks and Advanced Persistent Threats are some of the more serious security issues organisations face, and with the rise of BYOD (Bring Your Own Device), mobile attacks and advanced hacking techniques have only increased your risk of becoming a victim to a data breach.

Your classic anti-virus software can detect malware when there's a matching signature, but it cannot determine if the attacker has access to your endpoint just by monitoring the activity.

Cybercriminals have evolved their ways of attacking businesses and individual users, which is why you need Security Operations Centres to react to their new ways of infiltrating your organisation's data.



Key Benefits

Proactive Monitoring
We scan your network 24/7, flagging abnormal activity so we can respond to emerging threats immediately

Real-Time Visibility
Real-time visibility allows you to act as soon as any anomaly is detected, helping to prevent a breach

Analysis
The data collected is analysed to detect threats patterns, allowing unknown threats to be detected quicker in future attacks

Log Management
We collect, maintain and regularly view the log of your network activity to establish what's considered 'normal' for your network, allowing faster detection of anomalies

24/7/365 Threat Detection and Response
24/7/365 visibility of your endpoints and network and detection of cyberthreats

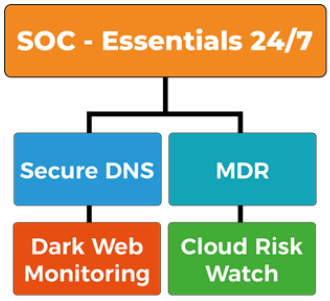
Fast Response
Quick and accurate response to threats, stopping them in their tracks, allowing business continuity

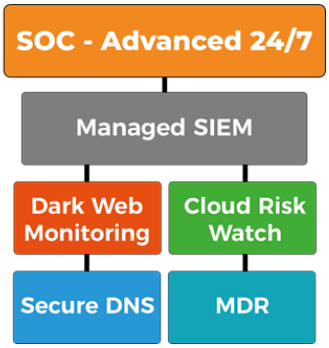
Research
Analysis tools research known and identified threats and search for suspicious activity

Why AZTech?

Our SOC combines a team of experts and industry leading and best of breed security tools to ensure the best possible protection for your organisation.

Packages Available:





For more information on the AZTech SOC services, call our security team on 03300 949 420 or email us at info@aztechit.co.uk

Enhance your security with a Security Operations Centre (SOC) from AZTech IT Solutions