LW IT SOLUTIONS

Microsoft

We can help you strengthen your Security Operations Center

The expanding digital estate has resulted in new SecOps challenges.

Digital estates produce greater quantity and diversity of data than ever
To protect them, defenders need visibility into everything—including many different endpoints, clouds, and more—and respond to these threats from a single pane of glass.

Managing many siloed security products is incredibly complex
Security Information and Event Management (SIEM) systems are poorly integrated across security products; this leaves gaps and can waste SecOps time juggling security products, and hunting and linking alerts together.

Modern environments generate overwhelming alerts and noise
SecOps teams struggle to separate the signal from massive amounts of noise, resulting in longer resolution times full of manual investigation.

We can help you enhance your SIEM with three critical components in order to meet these challenges:

The Cloud

Get large-scale intelligence on demand so you can analyze more data with greater efficiency than ever before.

AI

AI analyzes this enormous breadth of data and turns signals into meaningful intelligence, fueling every step of security operations from detection to response to hunting.

Automation

Automation is built into every stage of the security lifecycle, allowing SecOps to spend time on what really matters: focusing on deeper, more proactive work.

Get ready for your SecOps command and control center

We're experts at providing Microsoft security solutions and we can help you deploy Microsoft Sentinel, so you get cloud speed and scale, AI, and automation.

Collect and analyze data with the power and scale of the cloud

It all starts with the cloud. Microsoft Sentinel is cloud-native, which means that you have unlimited compute and storage resources, the ability to scale at will, and can eliminate infrastructure set-up and maintenance.

- 250+ built-in connectors
- Discover and deploy everything you need for your use cases with a single click
- Flexible, customizable, and cost-effective data ingestion and storage

Fuse data to detect evolving threats

Detect evolving and unknown threats with fusion, which looks across all your data to turn signal into meaningful incidents. Easily incorporate threat intelligence across multiple sources into your detections and investigations. Plus, get deeper insight into user and entity behavior with built-in, native user and entity behavioral analytics.

- Combine Microsoft's expert threat intelligence (TI) with your own insights.
- Analyze entity behavior with built-in user and entity behavior analytics (UEBA).
- Customize or bring your own machine learning with easy-to-use built-in tools.

Investigate incidents with full context

AI automatically maps related alerts into incidents so you can understand the full scope of an attack immediately. Seamlessly take your investigation deeper with bi-directional incident sync with Microsoft 365 Defender and Microsoft Defender for Cloud.

- Visually investigate the full scope of incidents.
- Pivot deeper with native Microsoft 365 Defender and Microsoft Defender for Cloud integration.
- Use automation to enrich your investigations with additional insights.

Respond across all of your tools with built-in SOAR

Built-in security orchestration, automation, and response (SOAR) capabilities allow you to automate and orchestrate responses directly from your control center. Reduce mean time to respond from hours to minutes using built in automation tools.

- Security orchestration is built-in, with LogicApps.
- Use more than 300+ pre-built playbooks, with infinite custom possibilities.

Shift from reactive to proactive with advanced threat hunting

With efficiency gains, you'll be able to do more proactive hunting. Rapidly hunt for threats using the speed and scale of the cloud, armed with advanced hunting tools.

- Hunt across all your data, including archives, in real-time.
- Get everything you need for hunting in an intuitive dashboard, sorted by Adversarial Machine Learning Threat Matrix techniques.
- Use built-in queries or make your own using a robust query language. Plus, easily create detections from your queries.

Isn't it time to help your SecOps proactively manage security threats with insights and speed?

As a Microsoft partner with extensive experience in the security space, we want to assist you in fortifying your SecOps with comprehensive threat intelligence and scalable AI. We've helped many business just like yours modernize their security strategies—and we're standing by to help you deploy Microsoft Sentinel.

Get ready to protect your entire digital estate with robust threat detection, investigation and response.

Contact us today!

www.lwitsolutions.co.uk

07940973228

liam.wytcherley@lwitsolutions.co.uk

LW IT SOLUTIONS