



SECURITY
INFORMATION
& EVENT
MANAGEMENT



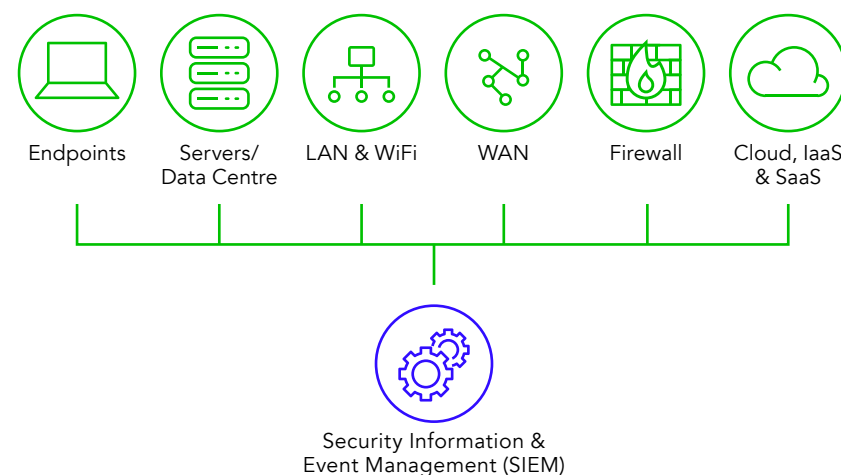
ANALYSIS, INVESTIGATION AND ALERTING TO IMPROVE YOUR SECURITY POSTURE

Few organisations in the current digital climate have yet to recognise the risk posed by cybersecurity and take positive action. However, many organisations are not large enough to justify bringing security expertise into their in-house teams. This lack of resources means they are unable to manage the critical task of Security Information & Event Management (SIEM), which analyses data across your infrastructure to monitor, alert and manage threats. If you are looking to enhance your cyber security posture but do not have the internal skills to do so, Daisy has the ideal solution.

Overview

Daisy works with leading Security Information & Event Management (SIEM) vendors to help you better understand your threat landscape and be able to react to threats in real-time. Log-data from throughout your technology infrastructure is collected and aggregated; from host systems and applications to network and security devices such as switches and firewalls. This information is then analysed to detect potential security incidents and alert on cyber threats.

Working with Daisy to deploy technology which constantly analyses relevant events across your entire infrastructure, means that cyberattacks and breaches can be quickly identified, studied and mitigated. This capability can help to reduce the detection time of a security incident from months to hours, which is especially important with disclosure regulations such as the GDPR.



— Customer Technology — Daisy Solution



SECURITY INFORMATION & EVENT MANAGEMENT

What does Security Information & Event Management deliver?

Daisy can install, support and manage a dedicated SIEM platform with a choice of services:

Service	Service Desk	Vendor Management	Remote Technical Advice	Security Event Monitoring	Policy Updates	Log Management	Regular Reporting	Review Meeting	Automated Response	Threat Hunting
Essentials: This service level is ideal if you want to take a direct role in managing your security environment, with access to Daisy's experienced Security Operations Centre for third line technical assistance.	✓	✓	✓					○		
Enterprise Plus: Daisy's fully managed service level, if you want peace of mind that Daisy has it covered, leaving you to focus on strategy and meeting business objectives.	✓	✓	N/A	✓	✓	✓	✓	✓	○	○

Who we work with:

Microsoft Sentinel

Microsoft Sentinel from Microsoft is a cloud-native SIEM platform that uses built-in AI to help analyse large volumes of data across an enterprise – fast. Microsoft Sentinel aggregates data from all sources, including users, applications, servers and devices running on-premises or in any cloud, letting you reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of popular security solutions. Collect data from any source with support for open standard formats such as CEF and Syslog.

USM Anywhere

USM Anywhere from AT&T Cybersecurity (previously AlienVault) was created to help organisations of all shapes and sizes achieve world-class security without the headaches and huge expense of other solutions. The cloud-based platform combines key security capabilities with expert threat intelligence to deliver:

- Discovery
- Detection
- Assessment
- Analyse
- Response
- Reporting

Why Daisy?

Daisy has a 25-year track record of supplying managed security services:

- **End-to-end expertise** – from data centre to device across cloud, connectivity and communications
- **The best technology** – highest levels of accreditation with the world's leading vendors
- **Skills and expertise** – state-of-the-art Security Operations Centre

Have you thought about...?

Vulnerability Management: We can analyse the changing vulnerabilities across your infrastructure and mitigate against them before they can be exploited by cybercriminals.

Critical Threat Advisory: We can send you regular alerts of industry threats and vendor vulnerabilities which are relevant to your environment, so you can save time filtering irrelevant information and respond quickly.



Find out more about Daisy's Security Information & Event Management, speak to one of our sales specialists today:

enquiry@daisyuk.tech

0344 863 3000