MANAGEMENT GUIDE SERIES

Your 10 Minute Guide to
Security Information & Event Management

+44 (0) 1274 736 223 | info@ecsc.co.uk | www.ecsc.co.uk
Introduction

Security Information and Event Management (SIEM) is usually a label applied to a piece of software. However, it is much more than this, and this ECSC Management Guide is designed to help you understand how to develop and maintain an effective SIEM, irrespective of your software choice.

The first problem with SIEM is that, in most cases, it is mis-sold and never really delivers effective security. Understanding why this is the case will help you avoid similar mistakes and start to develop truly effective systems.

Making sense of cyber security information, events and alerts is complex and time-consuming. SIEM ‘solutions’ tend to promise to make this easy, and appeal to non-specialists. However, if security was easy, or could be made so with a software package, there wouldn’t be so many breaches.

A common element in SIEM software is that disparate data feeds are combined into relatively simple (and usually pretty) graphical displays. However, in reality, this doesn’t tend to give you more than an impressive demo.

Imagine you are sat in the cockpit of a complex passenger airliner, looking at the vast array of dials, warning lights and displays. If you aren’t a fully trained pilot, what would be the value in combining this into a simple dashboard? Would that make you able to fly the plane?

So, having cast doubt on the value of SIEM, let’s start to understand it and see where real value can be gained from its implementation.

Each ECSC Management Guide is carefully authored for a management audience, and designed for both the technically knowledgeable and also senior managers with an interest, but not necessarily a deep technical background.

ECSC Group plc has nearly two decades experience within cyber security. As such, we encounter many examples of failed technologies. Sometimes these technologies are just the wrong idea; however, in many cases, the concept has merit, but is badly implemented and poorly managed.

You can benefit from this extensive experience, avoid these mistakes, and ensure your cyber security developments delivery real benefits. This paper is designed to help you start that process.
Going back to our pilot, if they really understand what the plane controls and displays are telling them, they don’t need some overriding software to simplify it. In reality, such software could make it more difficult, putting an extra layer between them and the systems they need to monitor.

That is why, where you find a highly skilled and experienced team doing a professional job with what we might call ‘protective monitoring’, they seldom use a recognised SIEM ‘solution’. They have no difficulty monitoring different system outputs and find that a tool for monitoring one system may not work for another. As they become more skilled, you will find they are more interested in the raw data, and not looking at graphics produced from it.

Now, if you’ve been subject to the promises of SIEM software providers, by now you might be screaming ‘event correlation!’ Let’s explore that.

In addition to bringing a wide variety of feeds together under a simple dashboard, SIEM software also usually promises to alert you where different data feeds have been correlated to indicate a breach. This sounds compelling, and the vendors usually have some initially impressive looking demos to prove the point. However, based on our 17 years’ experience in running a Security Operations Centre (SOC) and conducting incident response, we don’t think it’s that simple.

The problem with correlations is that, in the real world of your network and systems, they are almost impossible to predict. The ‘demo’ examples rarely apply to you, and predicting them for your systems is virtually impossible.

So, is there any value to SIEM and should you keep reading?

The answer is yes. However, you must stop thinking about SIEM as a piece of software. It is not really even a technology, but rather a process applied to technologies.

Even better, think of it as a job title. The job of a specialist team.

Why a team? Because hackers work bank holidays, weekends and in different time zones. Therefore, your SIEM team needs to be 24/7/365.
So, if you don’t have specialists, and you can’t effectively monitor and respond to your SIEM at any time, day or night, then a software solution isn’t for you.

However, if you think about SIEM as the role of a Security Operations Centre, whether internal or outsourced, then things start to makes sense.

Rather than throw everything possible into a SIEM pot, why not start with the basics, get them right, and then expand from there?

For example, are you collecting important internal system security logs in one place and reviewing them regularly – and critically – then taking action to understand what they are telling you, and investigating potential issues?

This is an important step in:
1. Understanding your systems.
2. Developing a process to respond to unusual activity.
3. Taking action to correct issues highlighted in the logs and reducing the ‘noise’ each day.

Another useful check is to look at logs from your firewalls to see if unusual outbound traffic is getting blocked – another good indication of an internal compromise. You can do your own correlation here if the firewall is blocking new traffic from a system also generating unusual security logs.

The next step might be to implement File Integrity Monitoring (FIM) for your external Internet-facing systems. As FIM alerts you to changes, it makes sense in an environment that doesn’t change very often. You then need a process to confirm that the changes that FIM alerts you to are caused by your system administrators (good change records are important here), as other changes could indicate a breach. This really should be a daily process, usually first thing in the morning, as night-time attacks are common.

A common element in both these examples of effective SIEM processes is that they create work. A SIEM that doesn’t generate work for the IT team is usually just a white elephant and largely ineffective; almost as bad as having penetration testing, getting a clear FAIL, and then taking no remedial action.
Where Next?

In summary, SIEM as a software ‘solution’, whilst sometimes making an impressive demo, usually fails to deliver in the real world and can be an expensive white elephant.

The simple act of combining information you don’t currently understand and don’t currently act upon, however pretty the graphics, isn’t going to solve the underlying problem.

Rather, by thinking of SIEM as a process, and particularly that of a Security Operations Centre, you can start to make real progress. If you start with getting some basics right, you start to deliver effective protective monitoring and won’t have spent a fortune on software in the process.

Remember that, with the hours that hackers work and their global spread, you also need to consider the viability of building, and retaining, the skills to consistently deliver a 24 hour, 7 day a week, 365 days a year monitoring and incident response solution.

This ECSC Management Guide has been designed to help you understand the most critical aspects of a key cyber security technology. This knowledge should help you procure, implement, and manage a solution that is right for your organisation and delivers effective cyber security.

ECSC can help you, whether through a wide range of consultancy services or with outsourced Security Operations Centre (SOC) provision through our global delivery from the UK and Australia.