SIEM BUYER'S GUIDE

BULLETPROOF

SIEM: BUILD, BUY OR OUTSOURCE?

THE PROS AND CONS OF SIEM INVESTMENT

INTRODUCTION

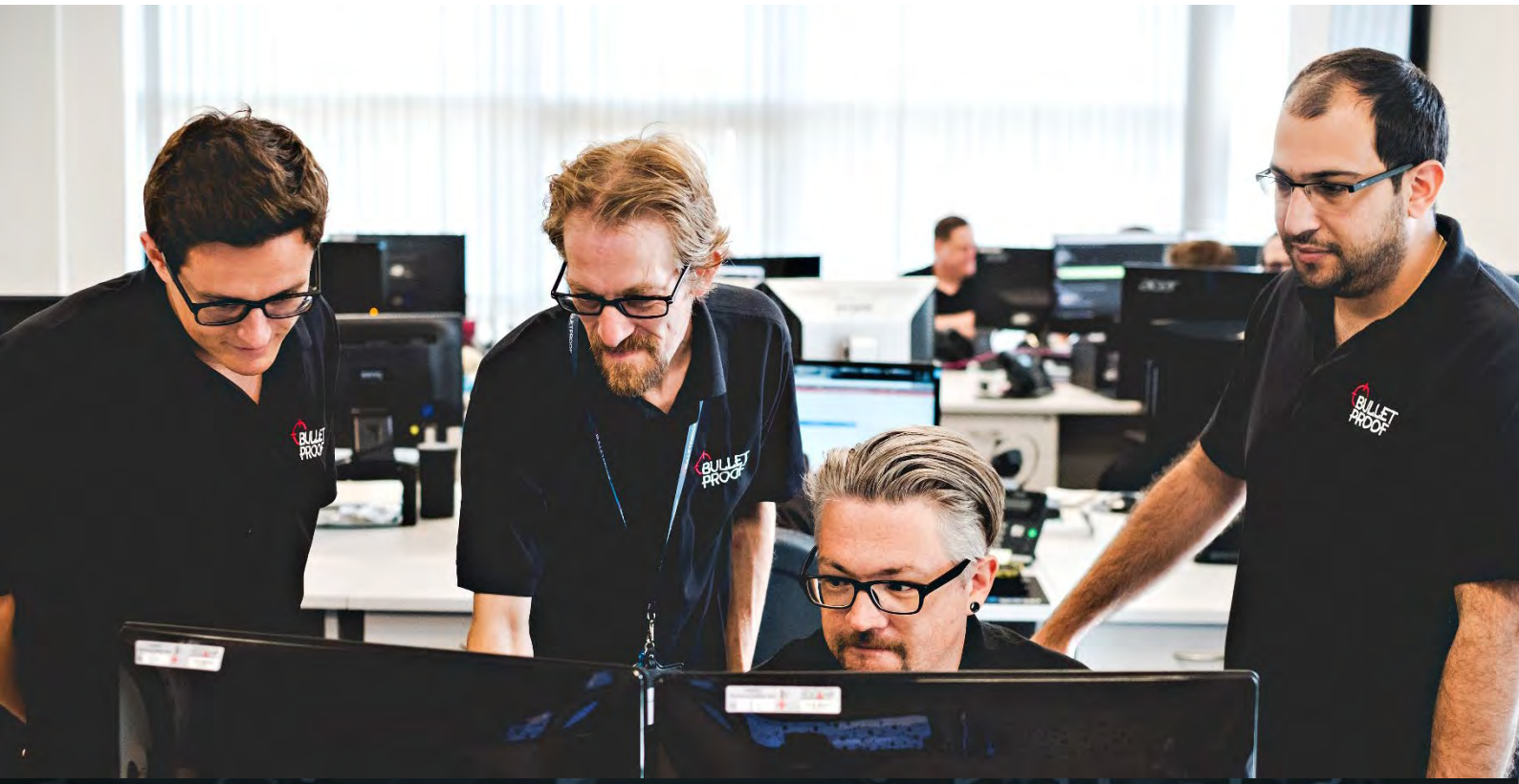
This handy guide looks at the pros and cons of different buying options for SIEM investment and outlines the key questions you need to ask when considering a SIEM technology or vendor.

WHAT IS SIEM?

Security Information and Event Management, or SIEM, is increasingly becoming a fundamental element to businesses' information security. A SIEM is intended to protect environments by taking log data from various sources and identifying suspicious activity. If an issue is spotted, such as scanning activity from a region not associated with the business, this can be raised as an alert and appropriate action taken.

At its simplest, SIEM works via a programmed set of rules. Events can be raised depending on what constitutes as 'normal' behaviour within a certain business. For example, a multinational retailer will regularly communicate with devices in multiple regions, whereas it's unlikely that local Government would. An effective SIEM must be programmed to recognise these different behaviours and raise alerts accordingly.

SIEM has evolved over the years from simple log monitoring to include a much more well-rounded feature set, which increases the challenge when managing a SIEM procurement process. This, combined with the increasing number of compliance standards which make some form of SIEM mandatory, only add to the confusion. Therefore, Bulletproof have created this quick guide to help you make the right choices for your organisation and get the most from your SIEM investment.



BUILD, BUY OR OUTSOURCE?

There are three approaches to incorporating a SIEM into a business: build, buy or outsource. What option is right for you will very much depend on the size and nature of your business, as well as your security objectives. There are benefits and drawbacks to each option and it's important to remember that, even within each, no two SIEMs are the same.

1. BUILD

We often say at Bulletproof, if you have the funds, build it yourself. Building a SOC and a SIEM platform specific to your company can deliver the strongest security outcomes, but at the largest cost.

Benefits

- You'll have complete control
- Being built specifically for your environment means you will have clarity on infrastructure priorities, monitoring requirements and the best way of capturing the relevant information
- Staff can instantly react to alerts
- Analysts will be working for you

Having something built specifically for your business will mean the service will integrate smoothly and work reliably from the outset, without having to do much on-going reconfiguration or tuning. You will have complete visibility of everything going on in your environment.

Drawbacks

Whilst benefits of building your own SIEM and SOC are powerful, it comes at a cost:

- It is extremely expensive, putting it out of reach for most organisations
  - The hardware and software costs alone will likely be in excess of £400,000
  - Staffing costs push the ongoing cost higher, particularly as the industry currently has a shortage of skilled professionals
- To be effective, monitoring must be 24/7 and conducted by dedicated security analysts
  - If not using dedicated security analysts, continuous monitoring and threat hunting will distract your IT department from their regular duties, or vice versa
  - Arranging round-the-clock shifts can be complex, particularly when taking holiday and sickness into consideration

Again, companies with enough funding will likely find the benefits outweigh the negatives, but for most companies this approach simply isn't financially feasible.

2. BUY

Buying is another option, with a marketplace of different vendors offering products providing different services and suitability. Many companies offer prebuilt SIEM software or hardware appliances to fulfil their customers' monitoring requirements.

Benefits

- More affordable than building your own
- System is already designed and ready to deploy
- One-off payment
- Will likely be a versatile asset

Drawbacks

- The system is not configured for your environment
  - An off-the-shelf SIEM will require multiple stages of reconfiguring to reduce false positives and make it an effective tool
  - Being built to a one-size-fits-all specification means you may find your chosen solution doesn't provide the protection you need, or was mis-sold owing to overpromised sales or incorrect scoping
- Much like building your own, you will still need staff resources to run the SIEM, which will incur cost in both time and money
- Deploying and reconfiguring can be challenging without assistance from the vendor
- Accessing the latest updates can incur additional costs
- Up-front payments for initial hardware can be expensive, especially if combined with on-going charges for support contracts. In addition, retrieving, parsing and archiving the log files might require a lot of storage, further adding to the costs
- Patchy integration with modern infrastructures. With cloud-first, serverless, containerised and ephemeral infrastructure increasingly common, many legacy hardware appliance SIEMs fail to integrate and offer the full feature set

Whilst specific benefits and drawbacks are dependent on the vendor, buying does come with a number of challenges that may be costly and time consuming to overcome, particularly in configuration and maintenance. In addition, searching for the right solution from the right vendor can be a time-consuming exercise. Ultimately, buying incurs similar staffing costs as building, without delivering the additional control and customisation.

3. OUTSOURCE

Outsourcing your SIEM requirements is often seen as a more balanced option. Having a third-party manage your monitoring responsibilities can be a robust and affordable approach to security. As with buying, services will differ from vendor to vendor, but the benefits of outsourcing remain consistent.

Benefits

- Affordable retainer-based service with no large upfront fees
- Access to experienced staff all year round
- Deployment and reconfigurations managed by a trusted third party
- No hardware appliances or support contracts to manage
- Access to a wider variety of threat intelligence
- Proactive threat hunting
- Immediate access to updates as and when they're produced – often at no extra cost
- Native integration with cloud and other modern infrastructures

Drawbacks

- You are one of many customers
- Action is reliant on effective communication
- Limited reconfiguration options you can undertake yourself
- Lack of control over software platform

The outsourced model is gaining significant traction in the industry thanks to its affordability and comprehensive suite of value-added services. Combatting the drawbacks of outsourcing can be achieved by selecting the right partner. Carefully evaluate your shortlist of vendors, as you'll be entirely reliant on them for effective escalation and on-going tuning of the services. Select the vendor that provides you with the most confidence that they can be a trusted security provider for your organisation.

CHOOSE WHAT'S RIGHT FOR YOU

When it comes to investing in SIEM, it's important to know your budget and scope, as well as your specific security and business objectives. Organisations need to weigh up the pros and cons of each solution and choose the path that will deliver the clearest benefits at the best value.

Historically, buying dedicated hardware appliances was the most popular solution, with building your own SOC/SIEM service reserved for larger enterprises. Increasingly, the industry is moving towards the outsourced model as it delivers the highest tier of service for the most manageable cost, and thus supplies the greatest value.

It's important to remember that the key element to any SIEM solution is the staff behind the service. Security alerts are only worthwhile if you have knowledgeable people to understand and react appropriately and quickly. Unfortunately, quality analysts can be hard to source and doing so can absorb a lot of resources in both time and cost. Whether you build, buy or outsource, investing in the right people will ultimately deliver the best outcome.

S.W.A.T. DEFENCE®

NEXT-GENERATION CYBER THREAT PROTECTION

SERVICE SUMMARY

Bulletproof's S.W.A.T. Defence® is our outsourced managed SIEM service, where proactive threat hunting by dedicated security analysts keep your staff, applications, systems and network secure 24/7. We believe human expertise, insight and ingenuity are fundamental to keeping ahead of the modern dynamic threat landscape. That's why Bulletproof puts experienced security analysts at the core of this service.

By escalating outcomes and actions, not floods of alerts, S.W.A.T. Defence® delivers credible security improvements to your organisation. Combining this ethos with our world-leading suite of SIEM tools and 'as a Service' delivery model makes S.W.A.T. Defence® a powerful solution to today's security challenges.

FEATURE OVERVIEW

S.W.A.T. Defence® delivers comprehensive security thanks to its full list of protection features, including:

- 24/7 cyber protection
- Proactive threat hunting
- Network & host IDS/IPS
- File integrity monitoring
- Web application firewall
- Flexible VA scans
- System hardening
- Powered by expert security analysts

SAAS DELIVERY

Thanks to our continuously updated SaaS platform, you're always protected against the latest cyber vulnerabilities and exploits. SaaS delivery also means S.W.A.T. Defence® offers extremely rapid set-up and on-boarding, with a 10-minute deployment process. This approach also enables native integration with public cloud (Azure, AWS, Google), container and serverless deployments, as well as traditional on-premises infrastructure.

SEE S.W.A.T. DEFENCE® IN ACTION

BOOK A CUSTOMISED DEMO WITH US

To find out more about S.W.A.T. Defence®, get in touch today to book a live demo.

If you need further support with your SIEM requirements, installation or tuning, don't hesitate to get in touch with our SIEM experts on 01438 300 231, contact@bulletproof.co.uk and www.bulletproof.co.uk/managed-siem

BULLETPROOF

YOUR BEST DEFENCE AGAINST CYBER THREATS

Bulletproof's mission is to develop innovative products and services that solve the world's most difficult security challenges. We work with businesses of all sizes to protect their brand, value and assets against today's threat landscape.

Organisations rely on our managed security services to detect and respond to cyber threats 24/7. Our dynamic portfolio includes CREST certified penetration testing, red team assessments, threat monitoring & SIEM services, VA scans, compliance consultancy and much more.

01438 532 900 contact@bulletproof.co.uk www.bulletproof.co.uk