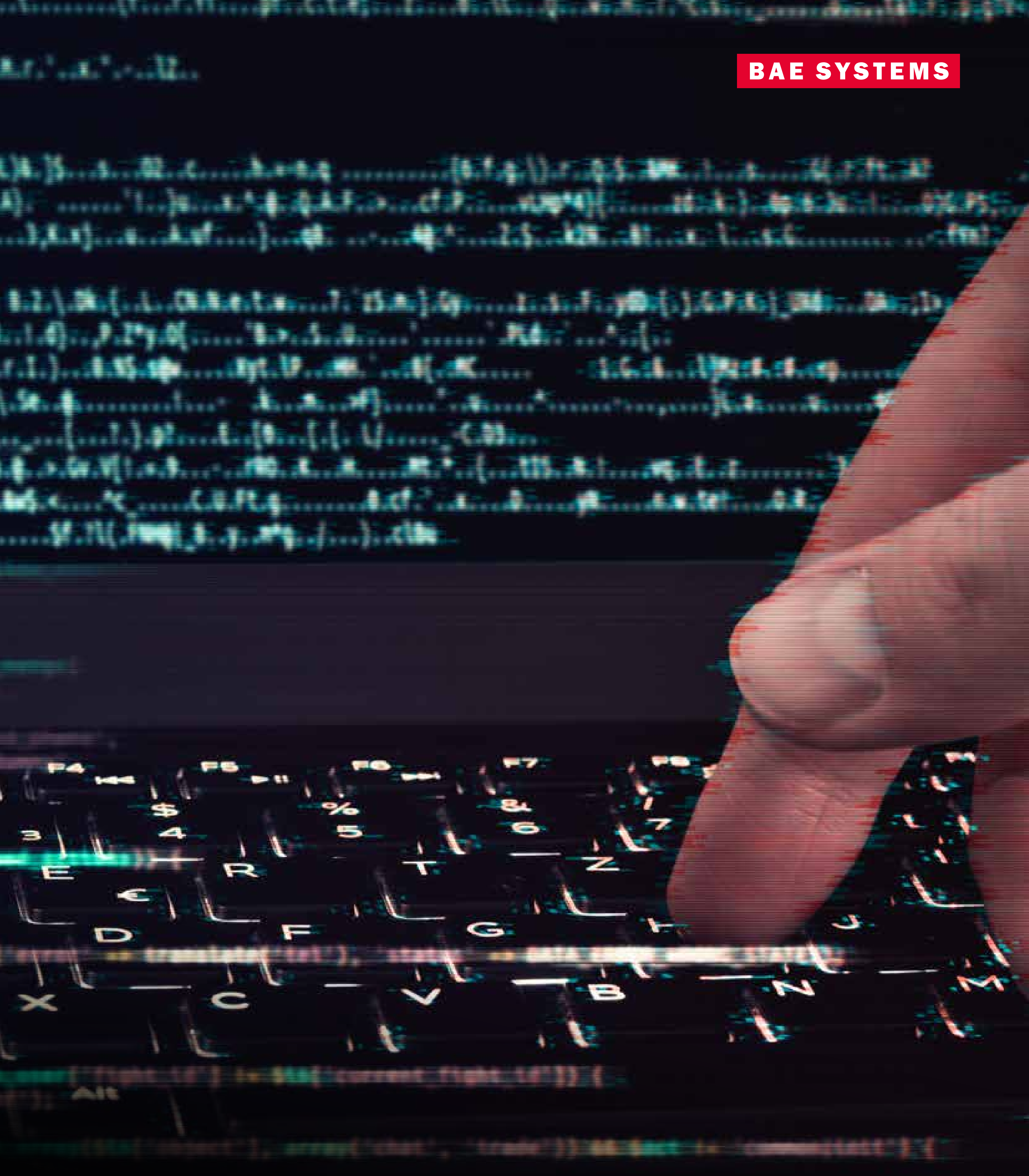


BAE SYSTEMS

Six steps to proactive cyber security protection

Prevention used to be enough, but now organisations need to take a stratified approach to IT security

Context

Your patient diplomacy and awareness activity has paid off: it has been a grueling 30 minutes in which you have put to the board the reasons the firm needs to improve its IT security. The board has given you consent to investigate the options and report back. Closing the board room doors behind you, you are elated but as you walk back to your desk, you realise that you are at a crossroads. Presenting a rational analysis of the options to the Board, and successfully implementing your recommended option, will be a feather in your cap; but failure to gain the trust of the board could result in further inaction, or the task being handed to someone else. What should you do?

- Recognise that you won't be able to stop everything
- Monitor to ensure that you can detect malicious activity
- Rehearse your incident response

Introduction

Prevention used to be enough, but now organisations need to take a stratified approach to IT security. An approach that uses threat intelligence to prevent badness from getting onto your network; recognising that you won't be able to stop everything, so monitors your environment to ensure that you can detect malicious activity in good time and extinguish it; and as a last line of defence, rehearse your incident response plans so that you can respond effectively to security incidents and minimise their impact on your business.

This note identifies the 6 steps that will help CIOs, CTOs, CISOs and IT Security Managers justify the adoption of monitoring to quickly detect targeted attacks, assess the right approach for their business and propel their career forward with a compelling recommendation to the Board.

Six steps to obtain the monitoring capability that you need

Step 1 – Understand and document an assessment of the firm's cyber security risk

Before you do anything, identify the firm's key information assets; its regulatory obligations; the trustworthiness of its staff and suppliers; and IT vulnerabilities that can be exploited; and the quality of the firm's information security controls. Doing so has two benefits:

- It allows you to define and prioritise monitoring requirements that will support your cyber risk strategy
- It allows you to demonstrate to clients and regulators that you are putting in place cyber security that is appropriate to your needs

If this has already been done, check that it was performed or updated in the last six months. If it hasn't, refresh the threat intelligence analysis and check your IT asset records for any significant changes.

Risk targets and tolerances should be set based on appetite for risk and the business' capacity to bear it.

Step 2 – Obtain Board agreement on a strategy for managing cyber risk

It's hard to present a detailed business case for IT security because it is difficult to define the range of breaches and associated costs that are avoided. Other ways to quantify IT security benefits are: its contribution to winning and retaining new business; and comparing it to the amounts spent to mitigate other existential threats (e.g. property damage, production losses).

Judgements about security sufficiency are essentially emotional and hinge on the Board's risk appetite. Risk targets and tolerances should be set based on appetite for risk and the business' capacity to bear it. Quantitative risk appetite measures may include maximum tolerance for operational losses; for example, "we will tolerate a potential loss of 5% of earnings for a 50% probability of increasing earnings by >20%". Qualitative risk appetite statements address: regulatory and reputational risks; reputation risk; or operational risks in the execution of business plans; for example, "we will not accept risks from which our brand cannot recover within 1 month".

Risks and rewards need to be balanced against their potential impacts and the cost of managing risks. Use the risk appetite statements to define combinations of costed security measures appropriate to each colour of the risk appetite spectrum and help the board to decide which colour on the spectrum represents the optimum balance of risk and reward. Be sure to include both business developers and lawyers in the process; they sit at opposite ends of the risk appetite spectrum and must both be included for a balanced view.

If based on the board's risk appetite, a network monitoring capability is to form part of its cyber risk management strategy, proceed to step 3.

Step 3 – Define and prioritise your business requirements

Talk to business representatives first. Using the output of the cyber risk assessment, define a set of "use cases" – statements of need – and ask business representatives to elaborate on them and to rank them in terms of business impact should a security incident relating to each one of them occur. An example output is illustrated below.

Priority	Title	Use case description
Very high	Espionage	I want to protect my sensitive client data and IP from theft by outsiders
Very high	Malware insertion	I want to detect targeted attacks
Very high	Malware execution	I want to detect malware executing on my network
Very high	Advanced targeted attack detection	I want to identify novel malware and infiltration activities
Very high	Malicious data leakage detection	I want to identify insiders leaking sensitive data from my network
Very high	Sabotage	I want to defend my network from deliberate damage by insiders
Very high	Faster detection	I want to respond as soon as possible to serious security threats
Very high	Extortion	I want to protect my network from a sophisticated external campaign (e.g. extortion using ransomware)
Very high	Real-time alerting	I want real-time awareness of my security risks
High	Untargeted attack detection	I want to detect untargeted phishing emails
High	Web app protection	I want to protect my web applications from compromise
High	Targeted denial of service	I want to protect my network from deliberate damage by outsiders
High	Unauthorised network usage	I want to prevent unauthorised processing of data on my network (e.g. by privilege escalation detection)
High	Illegal processing of data	I want to prevent my systems from being used for malicious acts on others
Moderate	Denial of service	I want to prevent degradation or denial of service
Moderate	Access control	I want to prevent outsiders from misusing legitimate remote access channels
Moderate	Secure access	I want to secure and control legitimate supplier access to my network
Moderate	Human error	I want to reduce impacts arising from human error

Having defined and prioritised your business needs, investigate solution options, next.

Step 4 – Identify and analyse advanced monitoring solution options

The most important decision you will need to make is whether to build and operate the monitoring capability yourself or to outsource it. The answers are not always obvious so the chart on page 7 contrasts the outcomes of good and bad decision-making and underlines why it is important to be certain the decision you are making is the right one for your business!

If neither model is ideal, you might consider a hybrid model whereby:

- Monitoring capability is provided by a combination of in-house and outsourced services

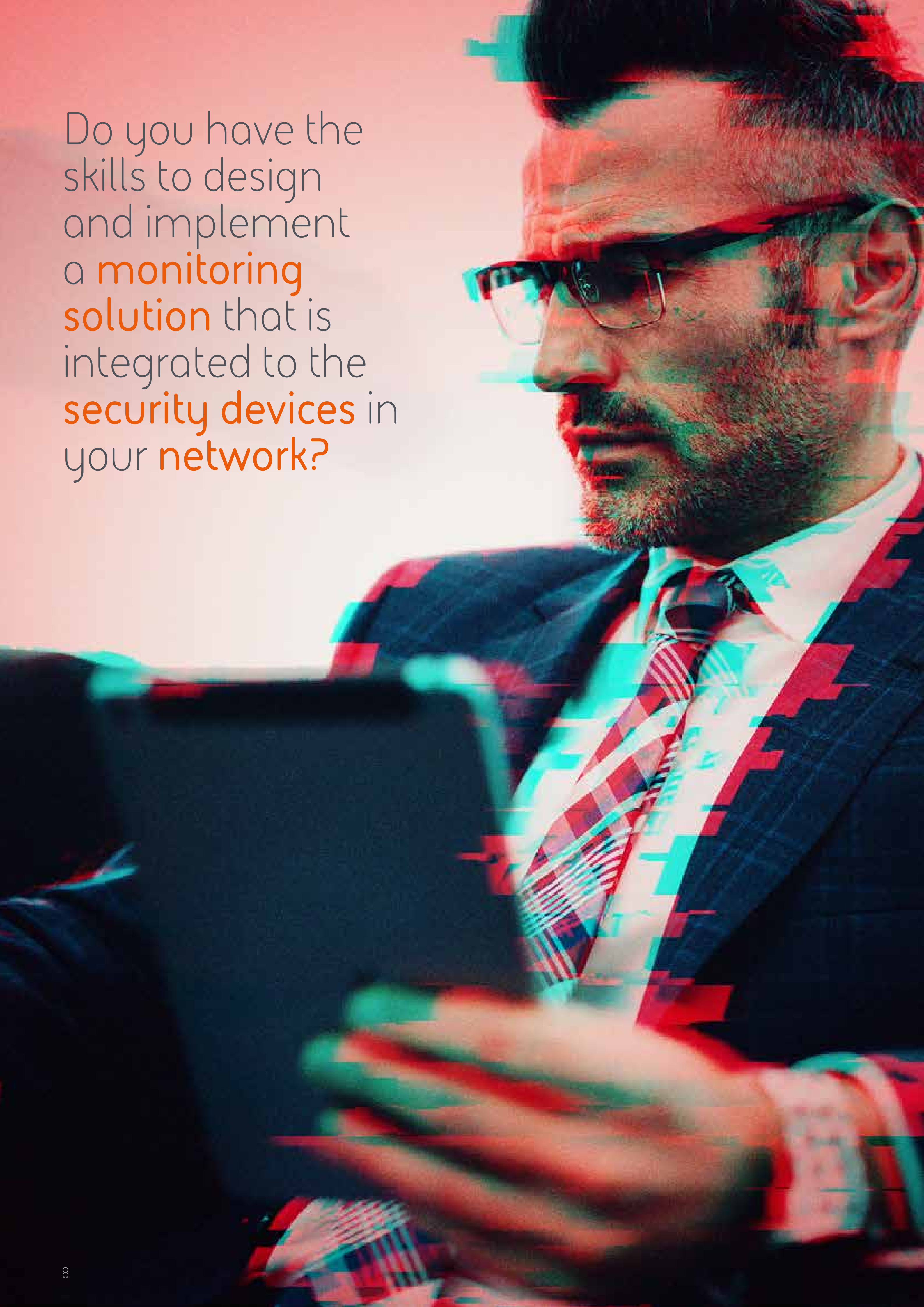
- Out-of-hours monitoring is outsourced; or

- Analytical tools are available in-house to allow ad hoc queries on the most urgent or sensitive matters to be discretely performed

Having decided which model is right for you, the next step is to design a solution.

	Right decision-making outcomes	Wrong decision-making outcomes
Build and operate the monitoring capability	• The quality and efficiency of the Security Operations Centre (SOC) analysts' decision making is high because they have an intimate understanding of the business they are defending • We can adapt the technology to fit the evolving security priorities of our business • We have a seamless view of both internal and external security events • We have all our logs in hand which allows us to fully investigate security alerts	• The capital costs to set up a SOC were so large we could not afford a solution that fully meets our needs • It is hard to demonstrate the value of the SOC when we have limited investment to evolve our capability • Our analysts are over-worked and under-trained. Their career path within our business is limited and morale is low. The risk of collusion with attackers is a problem • It is hard to recruit and retain talented resources • We don't have the experience to train our analysts properly • Our analysts do not have an outside perspective which makes them prone to missing large scale malicious activity conducted across our business
Buy a Managed Security Service (MSS)	• Spreading the transition costs over the contract term makes the service affordable • An MSS costs us less than building and operating an equivalent service • My MSSP uses threat intelligence to generate new rules and analytics to maintain effective protection against the evolving threat • As soon as a new threat is detected in the MSSP's customer base, we are protected • My MSSP involves me in developing its roadmap and prioritising new developments • Their SOC analysts are well trained, experienced and long-serving • Analysts' judgements are unbiased; they are based on a much wider context • The services are easy to scale and costs are predictable • Service quality is governed by a SLA and is continuously improving	• They provide little remedial support because they don't understand our network • They deluge us with false positive alerts and they miss alerts that matter • They are remote and slow to respond to queries • It takes more effort to instruct them than it would take to do the job ourselves • Their service is inflexible. The contract rules our relationship • Service requests cost us a fortune and they are hard to predict • Every week I deal with someone different. It is hard to build any teamwork • When things go wrong, no one seems to be accountable • We have to trust that they are doing their job. Unless we have a breach, there is no way of knowing

Do you have the skills to design and implement a **monitoring solution** that is integrated to the **security devices** in your **network?**

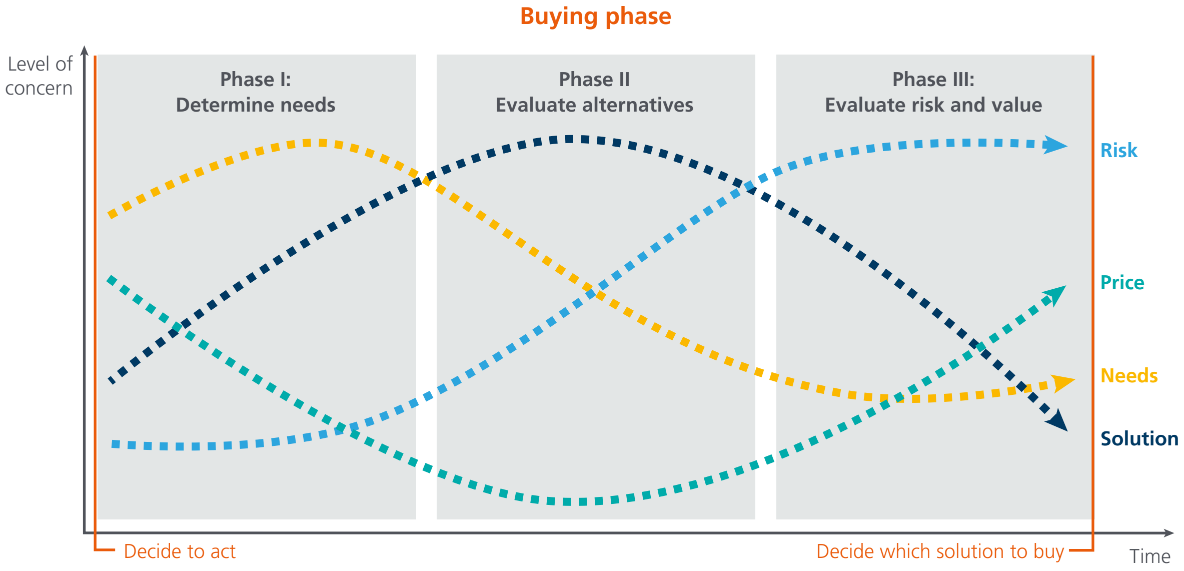


Step 5 – Defining the solution

Talk to your IT architects and operations managers to identify the options for meeting your monitoring needs. The right answer depends on your organisation's operational constraints. The main ones are:

- **Affordability:** can you obtain the capital expenditure budget required to set up a monitoring capability?
- **Training and awareness:** to what extent could good security awareness allow you to reduce your reliance on monitoring technology?
- **Operational maturity:** do you have a 24/7 SOC? Does it deliver a consistent service across the globe, even at weekends? Is it integrated with the incident response function?
- **IT assets:** do you own and control your network devices?
- **Threat intelligence:** do you know how to exploit it to maintain an effective monitoring capability?
- **In-house skills:** are you able to attract and retain the skills to support an in-house capability?
- **Standards:** are there any architectural requirements or regulatory standards that a solution must support?
- **Existing investments:** which components could be harnessed to form a monitoring solution?
- **Solution development:** do you have the skills to design and implement a monitoring solution that is integrated to the security devices in your network?
- **Commercial Off The Shelf (COTS) solution quality:** if you decide to buy a monitoring product, how easily could it fit with your IT security architecture, and how much of its capability could you exploit?

Build or buy decisions made in the context of such operational constraints will be logically founded and defensible. In general, only the well-resourced organisations in regulated market sectors such as banks and energy companies choose to build their own monitoring capability. The rest of the market favours outsourcing. In both cases, you will need to find the right security partner to support you.



Step 6 – Selecting the right company

The IT security market is like the Wild West. It is immature and there are hundreds of technology and service providers and new entrants to the market every week. How do you find and select the right company?

Procurement specialists and accountants take a quantitative approach based on solution quality, price and risk. Towards the end of procurement, it is price and risk that matters most as illustrated in the chart above.

BAE Systems has bought and sold security products and services for many years. We generally do it well, but we have made mistakes from which we have learned. When selecting a security company, price and risk should be considered alongside the following advice:

- **Pick a partner –** especially if you are looking to outsource IT security – you will spend a lot of money with them, they will have an intimate knowledge of your business and when things go wrong, you need to be confident that they will respond in the right way. It is unrealistic to expect these qualities from a supplier. Qualities to seek of a partner are:
    - An understanding of your organisation, its business goals and the market in which it operates
    - Long term perspective: they are there for the long run
    - Transparency: regular, open communications
    - Responsiveness and flexibility, underpinned by meaningful SLAs
    - When things go wrong, lessons are learned and improvement demonstrated
- **Pick a company for whom security is its core business:** your will get more from a partner whose whole reputation depends on the quality of its security products and services
- **Look at their heritage:** start-ups are lean and flexible. If they are private-equity backed, their primary aim is to gain market share fast and cash out. You need to be confident that your relationship will survive this fate. Companies that live off their profits are generally slower and more expensive but form deeper, long-term relationships and have more resources to draw on in a crisis. They also offer more assurance to clients' security auditors
- **What are they investing?** How detailed is the roadmap; to what features are they committing to deliver? Would you be consulted and what influence would you have over the roadmap?
- **See past the sales team:** focus in the people with whom you will work rather than the A-team that is selling the product or service. Ask them how long they have worked for the company, what value do they bring, and assess how keen they are to delight you

- **Verify what the prospective partner tells you:** you will learn much more about them by talking to their customers

- **Make sure they understand your business:** monitoring is most effective when outsourced services are delivered from a single 24/7 SOC where quality of service is easier to control. "Follow-the-sun" operating models are very cost effective for security device management tasks, but are less effective for monitoring tasks which require the analyst to have some appreciation of your business when investigating threats

- **Focus less on tech and more on the analytics and rules** used to detect cyber threats: how relevant are the rules and analytics to the use cases that are most important to you; how effectively do they work; how efficiently are new ones created to detect new threats?

- **Price transparency:** insist on catalogue prices for the term of the contract

- **Start small:** a security partnership is like a marriage so it is sensible to first date your prospective partner. Test your compatibility with a modest consulting project or a service trial. If you end up fighting like a bag of ferrets, you will be pleased to be free of each other by the end

Monitoring outcomes to aim for

A network monitoring capability delivers a wide range of outcomes to business stakeholders. You will know that you have made the right choices, if the outcomes you deliver resemble those in the table below.

BAE Systems provides consulting services to support you in building or improving your own monitoring capability. We can also provide you threat detection products and outsourced management security services. If you would like to discuss how we can help you acquire an IT security monitoring capability that is right for your business, please contact us below.

Role	Challenge	Monitoring outcome
CEO	• Cyber security is of increasing concern to my clients and regulators • Growing the business and managing risk is more difficult	• Having a robust monitoring capability allows me to differentiate my services, access new markets, and win and retain more business
CIO	• I lack real-time awareness of my security risks • IT security is seen as a business constraint • Disruptive technologies add risk to the way I support the business	• I have visibility across my network • In supporting the business, I can rely on proactive security management and leadership • I get more from my existing IT security investments
Security Operations	• We cannot detect cyber threats among the large volume of alerts • It is difficult to hire and retain IT security staff when we don't provide the tools they need • It is becoming more difficult to assure clients of our security	• We are protected from vastly more cyber threats • Our monitoring allows us to take appropriate remedial action before they damage our business • It is easier to retain staff and develop our IT security capability
Clients	• I need a company that can manage my sensitive data and to support me in growing markets • ...but with whom can I entrust my business?	• I trust your company to keep my sensitive data secure
Regulator	• I need evidence that in the event of a data breach, your company has the security controls to deal with it • I need evidence for how well those controls are working	• You give me confidence that you have sufficient visibility of your network to minimise the impact of a malicious activity on it

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
1676 International Drive, Suite 1000,
McLean,
VA 22102,
United States
T: +1 (703)848 7000

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai
twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST

CESG Certified Service
Cyber Incident Response

CPNI
Centre for the Protection of National Infrastructure