WHY AGILITY IS ESSENTIAL FOR EFFECTIVE CYBER DEFENCE

Computacenter

INTRODUCTION

If the pandemic taught businesses one thing it was that they must become a lot more agile. The speed with which decades-old working practices were turned on their heads was astonishing, and many organisations struggled to adapt at the pace needed. Now, with the painful lessons of the past having been learnt, business agility is accepted as an essential strategy for most organisations as they embrace modern working patterns, the rise of new technologies like AI and an increasingly unpredictable world.

Agility considers organisational response to change and its ability to adapt to unforeseen circumstances. Being agile can help increase efficiency, enhance employee engagement, improve operational performance, and accelerate the speed with which business change activity is undertaken. All of which should positively impact financial performance.

Agile companies are also typically more resilient to sudden, unexpected events as they can successfully adapt to change. With strong, autonomous, and empowered agile teams that do not rely on top-down decisions to execute day to day work, agile organisations possess the right skillset and have the best tools to respond to the dynamic nature of modern business. Whilst agility is important across all organisational departments, it is now increasingly being seen as critical to the security function. Here, the ever-evolving threat landscape and the speed with which new attack methods are being deployed means that security teams must be able to respond more quickly than ever before. The need to continually pivot between operating day to day security controls, defending against attacks and proactive hunting is now accepted as the default standard. And with security teams facing ever more skills shortages and the unprecedented impact of AI, embracing agility in all its forms is essential if security teams are going to be effective.

It should of course be noted that agility is not an excuse to introduce less robust processes or reduce risk assessment. Agility is not shorthand for doing things more quickly or with less oversight, but rather embedding repeatable processes, embracing automation, establishing clear lines of communication and interaction with other stakeholders and empowering decision making within a well-defined governance framework.

CHALLENGES AND CONSIDERATIONS

Agility in any form is often hard to achieve as there are many challenges to realising its value. However, recognising where the potential blockers are is a key first step. Once an organisation realises where the barriers are it's a lot easier to address them.
The most typical issues are outlined here.

ORGANISATIONAL CULTURE

Resistance to change: Traditional organisational cultures may resist the shift towards agile methodologies, making it difficult to implement new processes and practices. Clear communication of value is needed to ensure effective adoption.

SKILLSET REQUIREMENTS FOR AGILE CYBER SECURITY TEAMS

Lack of expertise: There might be a shortage of skilled professionals who are well-versed in both cyber security and agile methodologies, making it difficult to build and maintain agile teams.

INTEGRATION WITH EXISTING PROCESSES

Legacy systems: Integration with legacy systems and processes can be complex, leading to potential conflicts and disruptions in operations.

BALANCING AGILITY WITH COMPLIANCE AND REGULATIONS

Meeting regulatory requirements: Striking a balance between agility and compliance with industry regulations and legal frameworks can be a challenge, particularly in highly regulated sectors.

COMMUNICATION AND COLLABORATION

Interdepartmental collaboration: Achieving effective communication and collaboration between various departments, including security teams, development teams, and operations, is crucial but cannot be rushed. A focus on education and awareness will help enable change.

RESOURCE CONSTRAINTS

Budget limitations: Implementing agile cyber security practices may require investment in new technologies and training, and budget constraints can impede progress. As such, long-term senior sponsorship and commitment to change is critical.

RAPID TECHNOLOGY CHANGES

Keeping pace with technology: The fast-paced evolution of cyber security threats and technologies means that organisations need to continuously update their tools and strategies to remain effective. This should not be sidelined in favour of process review, or undertaken as a one off, but should remain a core ongoing component of an established agile model.

RISK MANAGEMENT

Balancing risk and speed: Maintaining a balance between the speed of agile practices and the need for comprehensive risk management is important, as hasty decisions may result in poor risk assessment and create opportunities for exploitation by bad actors.

INCIDENT RESPONSE CHALLENGES

Rapid incident detection and response: Ensuring quick and effective responses to live security incidents is an organisation priority but agility must not be used as a reason to cut corners and compromise the value of thorough analysis and complete risk assessment.

MEASURING EFFECTIVENESS

Metrics and KPIs: Defining and measuring the success of agile cyber security practices with meaningful Key Performance Indicators (KPIs) can be challenging, as traditional metrics may not fully capture the agile approach's impact.

Addressing these challenges requires a strategic and holistic approach, involving leadership support, ongoing training, and a commitment to fostering a culture of agility and adaptability within the organisation.

UNDERSTANDING AGILITY IN CYBER SECURITY

Agile Cyber Security focuses on embedding an adaptive and proactive approach to managing and defending against cyber security threats.

There is an emphasis on flexibility, responsiveness, and continuous improvement in the face of the evolving and dynamic nature of cyber threats. Agile Cyber Security adopts the principles of other agile methodologies and incorporates techniques such as iterative development, collaboration, and rapid response to enhance an organisation's ability to prevent, detect, respond to, and recover from security incidents. Agile security functions recognise that quick and agile decision-making, continuous monitoring, and the adoption of advanced technologies and tooling is essential if they are to stay ahead of the attackers.

Organisations seeking to embed agile approaches into their Cyber Security function, should consider the following:

EMBRACE A MORE FLEXIBLE APPROACH

The traditional approach to cyber security, which focuses primarily on perimeter defences and firewalls, is no longer sufficient in today's complex threat landscape. The adoption of cloud computing, hybrid working, the proliferation of mobile devices, and the explosion of the Internet of Things (IoT) has made it more difficult to secure IT infrastructure as it extends beyond the traditional boundaries of the enterprise network. As such, an agile cyber defence model emphasises flexibility and adaptability of tooling and process to ensure that traditional methods of detection and response can now scale to respond to new and emerging threats. It also demands that cyber security teams embrace new and more varied data insights to provide additional diagnostic context to better diagnose threats, and to enable automation to implement quicker remediation.

INSTIL COLLABORATION

An agile mindset prioritises collaboration and communication and is therefore also an essential characteristic of highly effective cyber security teams. It is fair to say that cyber security is not the responsibility of a single department or individual but rather that it requires collaboration across the entire organisation. However, for a function that has traditionally been seen as a handbrake to business productivity it can be challenging to encourage this sort of cross-functional collaboration. Nevertheless, to better identify and address security risks, such collaboration is essential, and by sharing threat intelligence, establishing standards and best practices, increasing communication and above all undertaking user education, organisations can benefit from more business insight and be better prepared to respond at pace in the event of an attack. In addition, ensuring security teams get the chance to test process and skill sets with regular blue team/red team cyber security simulations, will ensure security teams to improve their own internal team dynamic.

FOCUS ON CONTINUOUS IMPROVEMENT

Adopting the principle of continuous improvement is a cornerstone of an agile organisation and is equally important to the security team. For the security team this means regularly reviewing and updating security controls to ensure they are effective. This could be an update of a detection rule to ensure that its algorithms are coping with input data changes or tuned to identify the latest threats, or it could be embracing the use of emerging technology such as machine learning and artificial intelligence (AI). AI is predicted to have a significant impact on the "infinite game" of attacker vs defender. It has the potential to transform detection and response capabilities by being able to analyse enormous amounts of data to detect patterns and anomalies that would be impossible to identify manually. However, attackers are using AI too, with capabilities like generative AI being used to create ever more convincing fraudulent emails and texts and even execution code for use in phishing campaigns. Whilst still in its infancy it is expected that AI will become a more powerful tool in the hands of attackers and, as such, embracing a culture of continual improvement to consistently stay ahead is essential for agile security teams.

CONTINUE TO DO THE BASICS

Security threats continue to evolve at pace, driven by advances in technology, the increasing professionalism and funding of attackers, the increasing financial rewards available and global instability which is driving state sponsored actors. No organisations are immune to these changes and therefore cannot afford to stand still. Cyber leaders should consider new technologies and tooling, particularly where it can drive greater automation and provide greater insight. However, being cyber agile is not just about buying the latest and most advanced technology solutions, it is also undertaking foundational security disciplines such as Asset Management, Configuration Management, secure DNS, least privilege and hardening of systems. Knowing where corporate devices/resources are and measuring their current levels of configuration compliance will improve both the effectiveness of scanning and the diagnosis of impact. Effective vulnerability and patch management is required to maintain configuration compliance and ensure devices are not left unmanaged and vulnerable to exploitation, and establishing robust cold start capabilities should be considered to ensure organisations are able to bounce back quickly after an attack. Ensuring that these foundational security basics are undertaken consistently provides defenders with greater visibility and control over their estate, helping to reduce impact diagnosis time and making it easier to contain attacks.

ENSURE THAT YOU ARE MORE RESPONSIVE

Whilst it may seem a rather obvious statement it is nevertheless clear that agile cyber security teams are also very responsive ones. However, being responsive is not a simple matter of doing things quicker, rather it is about preparation and working to well-defined procedures. Implementing a well-defined incident response plan that outlines roles, responsibilities, and escalation procedures is the first step to being able to respond promptly to security incidents. Building playbooks with clear instruction and actions will also ensure security teams are able to quickly contain and mitigate the impact of attacks. Additionally, thorough post-incident analyses will ensure that teams learn how to adapt procedures, adjust detection algorithms and improve response capabilities.

BE PROACTIVE

There is an old saying in security that it's not 'if' you will get attacked, but 'when'. There is some truth in this as security could be considered the classic "infinite game", a constant race of attackers trying to outwit defender and defenders trying to predict and prevent attackers. This means that defenders must stay proactive and assume an attack will happen, rather than simply waiting for one to hit and then scrambling to respond in the shortest time possible. Proactivity means much more than being adaptable, it means taking steps to predict where attacks are likely to happen. Ensuring there is security team representation at change boards, making sure that developers have embedded security controls into application development cycles, running regular and continuous scanning, and maintaining a commitment to deliver regular communication and awareness is essential. A genuinely agile security team has to be proactive; it has to strive to be ahead of the attackers.

DEVELOP A SECURITY-CENTRIC ORGANISATIONAL CULTURE

For an organisation to be truly responsive to cyber attacks requires a broader engagement across the business. Whilst the security function will always be ultimately responsible for the detection and response to an attack, establishing a security culture within the organisation will make this much easier. If everyone in an organisation understands the importance of cyber security and their role in maintaining it, it is much easier to both detect an attack or a vulnerability and even prevent it from occurring in the first place. The inadvertent introduction of vulnerabilities by using weak passwords or from clicking on malicious links is often a consequence of poor awareness. Yet in an organisation where there is a security-focused culture, engendered by the security function and endorsed by business leaders, not only is there less of a risk that users are the source of an attack, but it is more likely that anomalous behaviours will be identified and reported. With a security-focused culture business functions will also be responsive and supportive of the activity needed to contain and manage cyber attacks enabling security teams to respond more quickly.

EMBRACE AUTOMATION AND AI

Automation and AI can be powerful tools for improving cyber security. An agile mindset encourages organisations to embrace automation to reduce manual processes, enhance the efficiency of security operations and enable quicker more targeted responses. There are also additional benefits beyond improved agility, for example; the ability to reduce risk. By integrating security testing into the DevOps pipeline, organisations can automatically scan for vulnerabilities and ensure that new code is secure before it is deployed to production. DevOps can also implement security as code: by treating security as code, organisations can ensure that security policies are consistently enforced across their infrastructure and that any changes to security policies are properly tracked and audited.

UNDERTAKE CONTINUOUS MONITORING AND ASSESSMENT

Even the best detection rules cannot claim to uncover all potential attacks or detect the signs of potential attacks. However regular scanning is still very important to the agile security operations team. Proactive detection still allows an organisation to be on the front foot, enabling them to respond in a more effective way to any detected signs of compromise. Organisations that don't scan regularly, use detection algorithms that are not regularly updated, or lack the resource to properly assess scan results, will always be reactive, constantly in firefighting mode and therefore, by definition, not agile. As regular scanning also picks up vulnerabilities, is able to detect configuration drift, identifies anomalous behaviours, and generally identifies security gaps, it also gives security teams the chance to be pro-active. With more risks identified and more security gaps closed as a result, security teams are more able to respond quickly and decisively in the event of an attack.

THE EVOLVING CYBER THREAT LANDSCAPE

Ensuring that your organisation can respond in the most efficient and effective way to a cyber attack depends on the type of attack you are being faced with.

Whilst there is a lot of debate about the time it takes to discover a breach, with estimates ranging from hundreds of days to just a few days, it’s clear that organisations still need to do better. So, understanding the most used methods employed by attackers and how these are evolving is important to any organisation seeking to be more agile in its response.

CURRENT CYBER THREATS AND CHALLENGES

The current cyber threat landscape is changing. Ransomware, malware and phishing remain the most pervasive threats, however because of both technology evolution and current geopolitical instability, organisations are now also having to contend with AI-enabled disinformation, deepfakes and hacktivism. Long-time threats like DDoS are also staging a comeback targeting mobile networks, and IoT and supply chain attacks are on the increase. It is also worth noting that adoption of XaaS models offers attackers single points of attack across multiple targets.

AI-driven cyber threats will leverage machine learning algorithms, neural networks, and advanced automation to execute targeted and stealthy assaults on corporate networks, systems, and data repositories. These attacks will manifest in diverse forms, displaying adaptability, speed, and precision that surpasses traditional attack methodologies. Key aspects include:

1. **Advanced social engineering:**
   AI algorithms will be able to analyse extensive datasets to craft highly convincing phishing emails, messages, or voice calls, making them indistinguishable from genuine communications.
2. **More sophisticated malware:**
   AI will accelerate the creation of polymorphic malware, which constantly mutates to evade detection by conventional security measures.
3. **Automated vulnerability exploitation:**
   AI algorithms scan for vulnerabilities in real-time and launch automated attacks, exploiting weaknesses faster than human intervention can respond.

Given that these threats are difficult to detect, and often difficult to address, it is essential that security teams have the headspace to prepare and plan, and the bandwidth to respond. Agility is therefore essential to address these new threats.

RAPID CHANGES IN CYBER ATTACK TECHNIQUES

Cyber attack techniques have always changed and evolved as attackers seek to stay one step ahead of defenders. However, it is noticeable that the speed of attacker change has increased, with new techniques being replicated more quickly, attackers copying successful approaches, more use of as-a-service models by less able attackers and the use of AI to speed up the development of malware.

APT groups, and increasingly more professional cyber-criminals, now utilise legitimate tools like remote management to evade detection for much longer. These same groups now seem to focus specific types of attack on certain verticals deeming them both valuable targets and less protected against specific attack types. For example, DDOS attacks tend to target Public Sector, transport, and the banking/finance sectors, whereas ransomware targets manufacturing, healthcare and public sector, and malware often pointed at individuals and public sector organisations.

Whilst still in its infancy, generative AI has the potential to create even more impact. The increased sophistication of AI-driven attacks will enable malware to continuously evolve, necessitating advanced security measures beyond traditional defences. The blurring of the lines between real and fake caused by deepfake technology will amplify the risk of falling victim to manipulated content, demanding heightened scepticism and vigilance in in user populations. Finally, AI will allow attacks to be executed at unprecedented speeds and scales, requiring defence organisations to fortify their capabilities accordingly.

The speed and scale of attacker evolution and the potential impact on organisations demands that security defenders upgrade the approach. Key to this is the ability to react quickly, in concert with all other IT teams and the business, and by demanding greater visibility and control of their estate. Only then will defenders be able to pivot from one attack to the next without being drawn into a constant state of firefighting.

THE ROLE OF AGILITY IN RESPONDING TO DYNAMIC THREATS

Identity and Access processes and tooling were designed to limit access to data, applications, and resources to only those that should have access. Whilst it is still the most effect model defenders have, attackers have found ways to circumvent the controls. When defenders developed behaviour-based detections capability to respond to the increasing amount of polymorphic malware, attackers started to use AI to make their malware increasingly difficult to detect.

However, this infinite game of attacker vs defender, has broader implications. Effective defence requires awareness of the latest attacker techniques and the options that are available to counter them. Agility in cyber defence is not just about responding quickly in the even of an attack, or adapting at pace as the nature and scale of an attack reveals itself, it is also about being prepared and aware of the latest developments in attacker technique and having a plan to respond to them.

Ensuring that reaction playbooks are regularly reviewed, detection rules are updated, and processes are assessed in line with changing attack behaviour is critical for an organisation to be considered agile. This agility extends to include the definition of a development roadmap, regular dialogue with budget holders to ensure updates and improvements are funded, and effective risk management to ensure that evolving and emerging attacker threats are properly quantified and assessed.

TECHNOLOGIES ENABLING CYBER SECURITY AGILITY

PLATFORM SECURITY – AUTOMATION, ORCHESTRATION, AND SCALE

Many security vendors are combining multiple technologies and tools into overarching security platforms. This has the benefit of a modular capability that can be deployed as required, integrated into existing tooling, and scaled more easily. Platform security features are typically much more coherent with a level of interoperability that delivers quick insights and enables much more automation. Whilst their technical capability may not be as comprehensive as a 'best of breed' solution, platform security solutions do work in a much more agile way and bring a level or orchestration that multiple point technologies simply cannot match.

Care should be taken to consider the cost of adopting such a solution, particularly where there is significant technical debt, and there should be an assessment of platform capability to ensure that there are no gaps, but it is fair to say that the agility of a cyber defence function is greatly enhanced with the deployment of a security platform.

THREAT INTELLIGENCE PLATFORMS

A Threat Intelligence Platform collects, aggregates and organises threat intelligence data from multiple sources and formats, and provides security teams with information on known malware and other threats, helping to improve threat identification, investigation and response. Threat Intelligence is an essential tool for all security teams as it enables them to detect, identify, validate and investigate potential security threats, attacks, malicious threat actors and indicators of compromise (IOCs), and quickly establish the context and implications of a possible attack.

Threat intelligence data comes from hundreds of sources, and traditionally required a high degree of manual aggregation, however with Threat Intelligence Platforms this activity is highly automated and helps to avoid issues associated with manual threat intelligence gathering such as the wide variety of different data formats, the increasing number and type of security threats that need to be considered and the speed with which intelligence needs to be made available.

With the arrival of Threat Intelligence Platforms, security teams that were once drowning in noise and false positives, and unable to identify potential security threats and the risks they posed, are now able to access this insight at speed.

ZERO TRUST SECURITY

Identity-based cyber security models like Zero Trust are very effective at enabling secure access in today's ever-changing multi-cloud borderless networks environments. Zero Trust solution allows access to business applications, data and resource based on user, a device, application, and location context, ensuring that no user is given access by default unless verified.

Embracing a Zero Trust model is a sure way to make the security of an organisation more agile, and more responsive to changing user demands without overtly impacting user experience. However Zero Trust is a complex, multi-faceted conceptual architecture and requires expertise and time to implement effectively. Ensuring that it is designed in a modular way, using a single underpinning technology is essential to its success.

SECURITY SERVICE EDGE (SSE)

Organisations that need more than the least privileged access can contemplate SSE – which not only consists of Zero Trust but also other elements like better policy control over user access to the cloud and web-based applications.

With SSE solutions, organisations can detect and mitigate threats effectively, keep applications secure, protect sensitive data, and easily manage policies. Of course, all this without compromising on the experience and scalability.

EXTENDED DETECTION & RESPONSE (XDR)

Modern-day XDR solutions collect and automatically correlate data from multiple security layers including endpoints, network devices, emails, servers, and cloud workloads. The objective of XDR solutions is to provide real-time analysis of user and device activity, enabling security teams to detect malicious activity, investigate suspicious incidents, and respond to threats quickly. XDR is an extension of the more traditional EDR which operates on the same principles but is restricted to data on endpoints.

XDR and EDR solutions can empower security teams with data and insights to help detect, quantify and then manage potential threats and identified vulnerabilities. As such it is a very valuable addition to the security team's kitbag, and a definite enabler for greater agility within the security operations team.

CONCLUSION

Businesses are becoming more agile, more adaptive to hybrid working and the use of cloud, and security must keep up. The ponderous, often manual and at times restrictive nature of the traditional security function is at odds not just with modern business, but also with the threat posed by highly evolved cyber attackers. Against a backdrop of stubborn levels of skills shortage, increasing amounts of regulation and the existential threat of AI, security teams must adapt and become more agile.

THEY CAN DO THIS BY

Embracing tooling, processes and data insights that are flexible enough to extend beyond traditional boundaries to incorporate hybrid workers and cloud environments.

- Developing a more inclusive culture that extends responsibility for security to all IT functions and the business, and involves regular communications to the business and its people highlighting the collective importance of their role in protecting the organisation from attack or breach.
- Focusing on continually updating existing toolsets, processes, threat intelligence and detection algorithms, whilst continuing to deliver foundational security such as patching, vulnerability management, asset management and device hardening.
- Reviewing your response processes, especially after an attack to see what could be done better, quicker or differently.
- Considering how to adopt AI to both counter the threat of AI powered attacks and malware, but also to better enable scaled response, implement automation and provide quicker insight.
- Continuously monitoring and assessing to help move their organisation from reactive to proactive, enabling more effective response and better use of resource.

EMBRACING AGILITY FOR A SECURE FUTURE

An agile mindset can be a powerful tool for improving cybersecurity within an organisation. Taking a more agile approach can help organisations to be much more proactive, helping them to identify potential security risks earlier. Earlier awareness enables quicker response, better prioritisation, more flexibility in how to respond and the opportunity become more collaborative.

Robust security controls do not need to be traded to achieve agility, productivity, or even speed. In fact, more agile cyber security should be seen as an enabler of broader business agility given its capacity to reduce downtime and improve user experience.

Not all businesses have the time and the depth of security expertise to identify which solutions they need to enable agile security, to assess how mature their current approach is, whether they need new technologies and tooling or whether they have the right skills and processes.

If you recognise these challenges and see them in your own organisation, then Computacenter can help. With 25 years of experience supporting our customers to make the right technology investments, to optimise their operational processes, and to consolidation and integrate their tooling we are perfectly placed to support the journey to truly agile cyber security.

LET'S TALK

For more information contact us at **SecurityEnquiries@computacenter.com**, visit our website, or contact your Computacenter Account Manager.

Computacenter

Computacenter (UK) Ltd
Hatfield Avenue, Hatfield, Hertfordshire AL10 9TW, United Kingdom