CAMBRIDGE CYBER
ADVISERS

Finding the needle in the haystack

Practical steps to improve your security operations and outcomes.

Sponsored by

FIREMON

Executive Summary

The role of Chief Information Security Officer (CISO) is one of the most challenging roles in any organisation.

They have to manage their organisation's risk, awareness, compliance and change, and many other areas of information security. And they have to do all of this, whilst proactively protecting their network from attacks and compromises, developing from a multitude of attack vectors.

Security operations teams, which fall under the remit of the CISO, tend to encompass the proactive and preventative controls and technology of the organisation. But over the last decade we have seen a shift in organisations leveraging external expertise to run security operations either on their behalf, or to augment their internal capabilities. And it all comes down to these three things.

- A limited talent pool of experienced security operations staff
- Rapidly growing organisations with an unprecedented number of SecOp demands
- Increasing network complexity due to rapid cloud adoption

Unearthing the best security operations approach to improve security outcomes is often described similar to "finding a needle in the haystack".

In this paper we are going to look at the challenges facing security operations and what differentiates great security operations teams from good ones. We are going to study what key components tip the balance in security operations favour, and how it can reduce the risk exposure for your organisation.

And we are going to discover, whether it is possible to find that "needle in the haystack."

About the Author

Bryan Littlefair

Cambridge Cyber Advisers

Bryan Littlefair is the Chief Executive Officer of Cambridge Cyber Advisers (CCA). He has over 25 years experience leading teams within information and cyber security. He specialises in advising executive teams and boards of some of the world's largest organisations on their security strategy as well as providing security consultancy, guidance and mentoring to the Chief Information Security Officer (CISO) community.

Prior to founding CCA, Bryan was the Global Chief Information Security Officer at multinational Insurer Aviva, transforming their security capability as the organisation adopted a fully digital way of interacting with its client base. Before Aviva, Bryan was the Global Chief Information Security Officer at Vodafone Group. He created the Information Security function within the Global telco, embedded their security strategy and oversaw day-to-day security operations for over seven years.

He also directed the Security Research Lab for British Telecom, participating in Global, EU and academic based research studies as well as driving relevant business transformation studies on behalf of BT.

He advises at an executive and non-executive level for Venture Capital funds and security start-ups. Advising on their security strategy and product vision.

Bryan holds several patents in the information security space and is a regular keynote speaker at security events.

A Spotlight on Security Operations: The Challenges in Depth

Security operations is a numbers game. There are potentially billions of security log events flowing into the central collectors on a daily basis. In fact, a good analogy is that security operations is like the human brain. Just like our brain relies on information from our senses to understand what is happening around us, a security operations centre relies on a distributed chain of technologies to inform it of the current status of security.

If a security operations centre lost access to its supporting technologies, it would be similar to our human brain trying to function without use of our senses, it would be extremely difficult to understand what was happening around us.

The challenge with security operations centres is that it's not simply a technology that you deploy and you instantly reap maximum benefits from it. It needs to be finetuned to your individual environment, and organisations need the right talent in place to not only understand the output, but ensure that they take appropriate action.

So, what should organisations be doing?

Improving your Security Outcomes

Security operations exist to proactively and effectively protect organisations from attacks and incidents of compromise (IOC), both internally and externally.

The more mature operations have clearly defined expected outcomes of which teams are benchmarked against. So what are the three principle outcomes that they track against?

1. **Speed and Simplification**
   A focus on reducing the time to detect/mitigate security incidents and to simplify complex infrastructures at every opportunity.

2. **Visibility and Control**
   Complete network visibility with effective controls that protects existing environments and the capability to pre-assess new environments before they go live.

3. **Automation and Impact**
   A reduced volume and impact of security incidents and issues through effective security baselining and automating security controls and response.

Let's take a deeper look at what these principal outcomes are, and what you need to do to achieve them.

Principle Outcome #1: Speed and Simplification

In security speed is everything.

Attacks can happen with the click of a mouse and spread across an organisation in minutes.

Or, on the flip side, attackers may "just" want to study your organisation for a while. So instead of compromising your network and "attacking", they lay in wait, watching for weeks and even months, refining their plan of attack.

So what does this mean for your security operations?

Your security operations needs to have a great level of versatility and speed of detection and response that allows them to detect 'smash and grab' attacks, and to the same degree spot the carefully planned data compromise attacks. Speed is vital, and so is a simplified infrastructure.

Simplification

To be able to launch an attack, attackers must find a way into your organisation. This can be via a vulnerability or a misconfigured system. This can be by 'hacking the human' and socially engineering an internal staff member. Or it can be by compromising a trusted third party and accessing your systems via them.

Our focus must therefore be on proactively identifying the potential risk and threat vectors, and planning our security countermeasures around them. Simply put, a threat-led approach.

And "simple" is the key word here. Whether you are improving your security operations capability or creating a new function, it's imperative that simplicity is at the heart of everything that you do. After all, complexity is the enemy of security. If something is complex then its inherently hard to secure.

But how do you simplify?

A threat-led approach means that we do not want billions of events flowing into our SOC on a daily basis and to be measured on the number of raw events flowing into the SOC. We need to be measured on impact.

We want to be measured on risk and threat reduction.

Creating an impactful risk and threat reduction log

To measure ourselves on risk and threat reduction, we need to define what a risk looks like and how it can materialise within our organisation.

In order to create an impactful risk and threat reduction log we need to assess the following:

- What would this event look and feel like?
- What users, applications, systems and processes would be impacted by this event?
- What proactive and detective controls can we deploy to help ensure the risk doesn't materialise?
- How do we make sure if anything materialises, we are first to know?

Work with your business to map out the full risk and threat model

It's imperative to partner with the business to map out the full risk and threat model. At the end of the day, it is their data you are trying to protect and they know better than anyone who needs to access it, where it's going to reside, how it will flow inside and outside your organisation, and which third parties are going to have access into the network and to data.

By collaboratively identifying risks and threats as well as designing mitigations, interventions and remediations, you will drastically improve the effectiveness and engagement of your operations function. Risks do not respect business organisation models or geography, and therefore your risk reduction approach needs to be truly global and holistic across all your environments whether they be on-premise or off.

By laying the groundwork to understand your risk and threat model, you are setting your security operations up for success. You know what you need to work to, and can track and trace threats in an impactful and effective manner.

Principle outcome #2: Visibility and Control

"You cannot secure, what you do not know about."
– A number one mantra for security operations.

Long gone are the days of a company's physical and information assets residing in the company's data centres. The reality is that the majority of organisations have embraced a hybrid world of data residing on-premise and within different cloud-based service providers and third parties.

But one thing remains constant. You are still accountable for the security of your data, wherever it resides.

As times and business demands change, so must our security operations. As we have seen in the last couple years with the shift to remote working and the adoption of a hybrid environment, security operations need to be reactive and agile. The reality is that your services and solutions need to be able to traverse organisational and geographic boundaries and operate as an effective extension of your on-premise capabilities wherever and whenever they are required.

And the only way to effectively identify and manage risk is via visibility and control.

Visibility

We often hear about the need for visibility, but what does it actually mean? How does it help your security operations?

To be effective in identifying and managing risk you need to be able to always understand the who, what, where, why and when. You need to be able to identify when a business leader spins up a new instance in a local cloud service provider in a remote region, and you need to ensure it is proactively protected prior to going live. You need visibility of what is happening, or going to happen.

In addition, you also need to understand and visualise the network and application connections within your business, all of the federations of corporate identity that are extended to cloud service providers, and where all of your data flows are occurring.

Visibility and control is not intended to constrain the business in any way. The business needs to be able to innovate and transform, to reduce costs and to evolve to market conditions and/or customer expectations. We need the ability to detect when this is occurring on the off chance we haven't been proactively engaged.

Your target should be to effectively monitor or manage the security lifecycle of all corporate technology or data from creation of service through to decommissioning, which includes the maintenance of patches and upgrades.

Security operations extend beyond monitoring into engineering and management of distributed security technology. Globalising your approach into having a single global team responsible and accountable for the operations of security related technology has to be the goal. If we use firewalls as an example, centralising all firewall change activity under a single team and equipping them with the right tools so they can ensure any firewall changes do not expose the organisation to increased threat or risk is a significantly better approach than having multiple teams performing manual firewall changes.

Automation and Impact

I have yet to meet a CISO that thinks they have all the resources in terms of people and budget. There is always more to be done and that requires more people and more resources. Compounded by the fact that you must segment your security expertise to support part of the business doing waterfall delivery and the other part doing Agile and DevOps. Every security leader needs to optimise the valuable resources that they have to ensure that risks do not go unidentified or unmanaged.

And naturally, automation plays a valuable role within resource optimisation.

Many of the tasks that are performed by the security function can be partially automated, removing part of the manual processes and codifying your security policy and approaches into automated workflow and decision making. This can deliver huge rewards in terms of operational efficiency, and enables your security experts to focus on areas which require human logic and decision making, rather than those that do not.

By adopting automated workflows, you can move rapidly towards real time risk analysis as compliance checks are performed continuously on systems, applications and infrastructure rather than waiting for a manual check to be performed maybe once or twice a year. We are used to this way of working with some of our systems, but it has not been ubiquitously deployed across the security team's workload.

Organisations are currently working at pace to industrialise some of the rapid changes that were made to their environments to handle changes in working practice due to covid. Now that flexible-working is here to stay for the majority of organisations, bandwidth hungry on-prem applications used by employees are now rapidly being transitioned to the cloud for a better user experience. But when things are done quickly, they are not always done securely.

By automating your security analysis, vulnerability assessment, compliance status monitoring and many other processes, you can ensure that when new cloud environments are brought online, they are secure by default and design. You can greatly reduce the likelihood of misconfigurations appearing upon your estate and therefore you effectively avoid leaving the door open for attackers.

You can also automate your auditing and compliance certifications, which will be a great thing for your IT colleagues to not have to go through numerous individual physical audits. By identifying the in-scope services and the systems that make up the service, you can rapidly and automatically identify compliance violations in real time and address them to maintain constant compliance.

Conclusion

So the question is, is it possible to find the proverbial needle in the haystack?

In short. Yes. It is possible.

To be successful, it's about changing your security operations approach away from ingesting billions of logs into a targeted precision approach, based on your organisation's risk and threat profile.

Moving from point in time to real-time (via automation and adoption of workflows) you can adjust your risk & threat profile in addition to your distributed technology and control environment. Enabling you to effectively respond to changing dynamics, whether that be business driven or by the release of a new threat.

A threat-led approach enables you to effectively partner with the business to deliver an aligned service that produces actionable, cotntext aware information that is of value to the business, not just false positive after false positive.

By maintaining your hybrid systems in a state of constant compliance with security requirements, you successfully reduce not only the operational burden on your security operations team but also on the wider IT and Network team.

You regain control by simplifying your environment and automating manual tasks, freeing up valuable resource to gain visibility and control which enables the business to operate with speed.

CAMBRIDGE CYBER ADVISERS

Cambridge Cyber Advisers are a specialist cyber consulting and advisory firm. We provide a unique set of services based on our experience of managing security and technology for some of the worlds largest and most valuable brands.

We offer a full range of consulting and advisory services aimed at both the C suite of the organisation and the CISO team to ensure the security strategy of the organisation is effective in the current environment of cyber security challenges.

We specialise in advising at board level and managing the relationships with regulatory and governance bodies to improve the organisations global security posture.

Sponsored by

FIREMON

FireMon is the only real-time security policy management platform that delivers a comprehensive risk management solution built for the complexities and scale needed for today's complex multi-vendor, enterprise environments. Supporting the latest firewall and policy enforcement technologies spanning on-premises networks to the cloud, only FireMon delivers visibility and control across the entire IT landscape to automate policy changes, meet compliance standards, and minimize policy-related risk. Since creating the first-ever policy management solution in 2004, FireMon has helped more than 1,700 enterprises in nearly 70 countries secure their networks. FireMon leads the way with solutions that extend and integrate policy management with today's latest technologies including SD-WAN, SASE, and SOAR. FIREMON.COM