Deloitte.

The Cyber Detection Paradox – A Directors Guide

Exploring this emerging problem and asking the right questions.

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

It takes 277 days on average to identify and contain a breach—204 days to identify and 73 days to contain*

Simply by reading the news, it's clear that material cyber incidents have become a regular occurrence across critical organisations in the Asia Pacific region.

Many of these cyber-attacks are not detected until weeks or months after initial infiltration. This often leads to a greater impact to stakeholders, all while the organisation is trying to manage an incident as it plays out in the public realm.

Cyber budgets continue to track upwards in the hope that more money equates to a better security posture. Organisations often spend the greatest portion on a 24x7 detection & response capability or service provider in the hope that early detection and response can reduce impact. As a result, there are fundamental questions emerging for boards, regulators, and management teams about why attacks aren't being detected and the effectiveness of controls and investment in this domain.

Deloitte's extensive experience in cyber incident responses and post-incident investigations has provided visibility into a wide range of incidents – how and why they occur, and lessons learnt. This guide delves into common root causes we've seen on why organisations are missing cyber-attacks until they become visible very late in the day, as well as providing a list of targeted questions that directors or regulators can ask management on this topic.

* IBM Cost of a Data Breach Report 2023

Unlocking the Potential of Security Operations Centres: Five Areas for Improvement

The vast majority of organisations understand the importance of maintaining a Security Operations Centre capability. However, through Deloitte's experience in incident response and post-incident reviews, consistent themes are emerging where the SOC isn't always as effective as assumed, and has gaps. Based on these observations, several areas including the following have been identified as potential avenues for improvement to help organisations further strengthen their cyber resilience:

01. Organisational growth and change leads to coverage 'blind spots' over time

Most organisations we encounter are complex. They have hundreds (or thousands) of technology assets and resources, and the landscape of their assets are continually evolving with new projects and change within the organisation. Here are some examples of blind spots, which mean assets aren't fully covered by detection:

- **Growth of external interfaces between technology assets**
  Many new applications are assembled using cloud-native technologies and leverage data interfaces between trusted partners in an ecosystem. (As an example, we've seen some customer billing systems with over 45 external interfaces to push or pull data from many sources such as state governments and credit bureaus. However, it's unfortunately common to see cyber detection capabilities that don't have full visibility of activity on these interfaces, or the ability to understand the nuances between normal behaviour and suspicious activity. This also encompasses the inability to detect scenarios where a trusted partner has been compromised and being used to pull large quantities of data (e.g., progressively downloading every record).
- **New assets appear over time and are increasingly dynamic in nature**
  Many detection approaches are based on a stable set of baseline technology assets, but in reality, it's common for this landscape to drift over time, resulting in blind spots. Additionally, the transient nature of some cloud assets means organisations need appropriate tooling and strong focus on asset management, change management and regular reconciliation of coverage.
- **Operational technology isn't covered and centralised response is limited in what it can do**
  Organisations with operational technology (OT) assets often have incomplete coverage of their OT landscape. Taking any response action in an OT environment (e.g. isolation of a device) can have a range of unintended consequences (e.g. unplanned outage of an industrial process).This means that the decisioning and workflow for suspicious events in OT can be poorly defined
- **Internet of things is causing an explosion in total device numbers**
  Some industries, like energy, are experiencing a steep growth in total device count, driven by the adoption of new device types like field devices, smart meters, and smart city infrastructure. Each of these devices is effectively a connected computer and can result in assets that are not appropriately integrated into a cyber monitoring or protection program. In some situations, it's not completely clear which entity is responsible for robust cyber monitoring of these new assets.
- **Weak detection of accidental misconfiguration (rather than an 'attack')**
  Many cloud services have a complex set of configuration settings, which can result in data or interfaces being accidentally exposed to the internet. The reality is that many cyber incidents have their genesis in an external attacker identifying a misconfigured asset that isn't secure (e.g., a data storage resource or interface is accidentally set to be 'public'). Some SOCs have not focused on, nor have the right tooling to detect, misconfigured cloud assets.

02. Poor visibility of suppliers

In the modern economy, most organisations have a high reliance on hundreds of individual suppliers, some of whom can access sensitive data or systems, and sometimes with a high-level privilege. This privilege isn't lost on attackers, and in recent years attacks are targeting the supply chain for this reason. A few common examples in this domain include:

- **Supplier remote access to core systems isn't well monitored nor controlled**
  Most organisations have interfaces that trusted suppliers use to log-in to core systems (e.g., for support). This is still a common channel that isn't comprehensively monitored or protected using modern Privileged and Remote Access Management solutions. There can also be gaps in the identity lifecycle for off-boarding supplier staff when their employment has ended, which means access is retained beyond employment.
- **Zero visibility of supplier's own detection**
  Organisations are usually reliant upon their suppliers' own detection effectiveness. This is a common blind spot in ecosystem models where a lot of economic activity or data analysis is done by key suppliers.

03. Keeping up with the volatility of the external cyber threat

A modern SOC may ingest more than a billion individual security event transactions per month (e.g., a failed log-on attempt being a single event), presenting enormous volumes of information. At the same time, attackers are becoming increasingly sophisticated and subtle, presenting challenges around detecting a real attack versus being overwhelmed by false alerts. Examples include:

- **Poor agility to respond to new threat intelligence**
  Cyber threats are continually evolving and it's common for cyber operations to receive daily or weekly updates on new threats or insights on the root causes of attacks seen in other organisations. This information ranges from highly technical feeds through to human-readable guidance. Some SOCs lack strong processes, platforms or abilities to be able to absorb a large volume of external information and then pivot to update the current threat model, answer basic questions such as whether the new threat is relevant to the organisation, or to search for evidence of an existing compromise based on the new intelligence.

- **Weak or dated detection capability fails to spot malicious activity**
  Whilst its relatively simple to detect high probability bad events (e.g., 50 failed log-on attempts in a minute), its common to see SOCs where the detection platform is more than 5 years old and lacks the capabilities to spot some types of modern attack.
- **Excessive false positives**
  Poorly configured security analytics tools can generate excessive false positives, leading to alert fatigue and causing SOC analysts to overlook genuine threats.

04. Poor asset understanding and mapping

When responding to a detected incident the SOC needs to perform investigation and decide on the next course of action in its attempt to investigate and contain the incident. However, in our experience fundamental aspects of technology hygiene can conspire against the SOC team in their ability to make good decisions and anticipate the impact of these. Examples include:

- **Understanding critical assets and the location of sensitive data**
  While organisations often understand which business applications are critical, this understanding does not normally extend to the individual resources (e.g., servers, storage, cloud resources) that are critical dependencies. In addition, organisations can lack a detailed mapping of where critical data is stored. This gap in understanding can make it challenging to focus detection and protection efforts effectively. It can also complicate the task of diagnosing the extent of a compromise and accurately assessing the level of risk associated with an incident.
- **Understanding the asset impact of response actions**
  Poor asset understanding can also mean that the SOC can't anticipate the full business consequences of urgent actions - like quarantining an asset, or even segmenting part of the organisation to protect it from a spreading incident.

05. Immature operational processes, staff capability and workflow

A lack of mature operational processes can contribute to SOC failures, or ad-hoc responses to a real incident. Ineffective or inconsistent incident response procedures, inadequate documentation, or insufficient training and development opportunities can hinder a SOC's ability to detect and respond to threats effectively. Examples include:

- **High reliance on manual workflows.**
  Incident investigation and response can involve multiple teams collaborating, under extreme time pressure, across the technology function and external suppliers. However, some SOCs do not have mature workflow around how individual tickets are treated through to resolution. It is also common to see an outsourced service provider using their own ticketing platform which doesn't integrate with the organisation's own ticketing system, resulting in manual steps to copy and paste information from one interface to another, or having to swivel between multiple platforms to perform further investigation.
- **System restoration from backup is untested.**
  Backup restoration is a key control for cyber-attacks but in many cases recovery test plans don't adequately cover complex ransomware scenarios. In many major incidents, restoration from backup fails to work asexpected, resulting in a crisis situation.
- **Insufficient staffing, expertise and attrition**
  Many SOC's face challenges in hiring and retaining skilled cybersecurity professionals who can identify and respond to threats effectively. A lack of experienced staff can lead to misconfigured security tools, failure to recognise emerging threats, and inadequate incident response.

What's the role of AI?

The operational efficiency of SOCs has never been more topical.

In general, SOCs are labour intensive because of the expectation to provide 24x7 staffing. In addition, in many industries there is emerging regulation that's mandating on-shore resourcing of the SOC, which in turn means it has a higher cost for staffing.

Hence, the advent of technologies like orchestration, automation and generative AI are starting to bring greater efficiency and effectiveness within SOCs. These advancements improve the accuracy of detection, improve the speed of response times, and strengthen containment activities to avoid larger incidents.

They also streamline initial information gathering which means SOC staff spend more of their time working on the key incidents that require business context or judgement to decide whether a suspicious activity is valid or just another false positive.

However, it is important to recognise that adversaries are also leveraging these very technologies in their attack strategies.

Probing questions for directors and leaders to ask

The rise of undetected cyber incidents illustrates some of the many challenges to stay ahead in this area, given the high complexity of technology and data footprint in organisations, the rate of change and the evolution of the threat.

Based on common root causes, the following range of questions can be useful to dig deeper and seek comfort:

01. Coverage of our key technology and data

- How are we identifying and prioritising our critical assets and information, and what measures are in place to protect them?
- How is our technology asset management maintained and updated, and how does this support our SOC's ability to prioritise efforts and allocate resources effectively?
- How do we have confidence that our detection capability has sufficient coverage of our technology assets and processes?
- How do we maintain currency of coverage as part of change management and project delivery, and reconcile this remains comprehensive?

02. Cloud assets

- Do we have strong detection capability and coverage for accidental misconfiguration of cloud assets and dynamic cloud assets?

03. Interfaces

- How do we maintain robust coverage of all our external interfaces to the internet or ecosystem partners, including between cloud-based assets?
- Does this capability include detection of unusual behaviour through an interface by a trusted partner?

04. Changing threats

- What are our top threats (threat scenarios and threat groups) and how are these managed?
- How do we keep this view updated and how does it feed into our detection and response capability?
- Are Purple Team exercises or other forms of assurance used to model potential attacks and refine the SOC settings and capability in response?

05. Staff skills

- How are we addressing staffing and expertise challenges within our SOC?
- Are there training and development programs in place to upskill our team?
- What's the level of staff turnover?

06. Process effectiveness

- How are our incident response processes defined, documented, and tested to ensure effective response and recovery in the event of a breach?
- How are our detection platforms configured and maintained to ensure accurate and timely threat detection?
- Are Purple Team exercises or other forms of assurance used to model potential attacks and refine the SOC capability in response?

07. Third-parties and suppliers

- How do we assess and manage risk around attacks directly against our critical third-parties, and what measures are in place to protect our organisation from potential attacks through third parties?
- How do we manage direct supplier access to our systems, especially where it is privileged?

08. Operational Efficiency

- Given the SOC can have an intensive reliance on 24x7 staffing, have we maximised the opportunity from automation of actions and responses?
- Are we exploring the potential that AI offers to create a more cost effective and efficient SOC?

09. Operational technology or Internet of Things (IoT) (where relevant)

- Do we have sufficient detection coverage of our operational technology (OT)?
- Who has responsibility and sufficient contextual understanding for the cyber monitoring and responding to suspicious behaviour in our operational technology (OT)?
- Given the risks of unintended consequences of taking action in an OT environment, is the decision model and workflow well defined?
- Do we have a growing population of connected IoT assets (e.g. field devices)? Are we clear on who is responsible for managing and monitoring the cyber security of these devices?

Bringing greater clarity and comfort

The last few years have demonstrated the increasing challenge of promptly detecting cyber-attacks, despite the growing investment in Security Operations Centres. Recent post-incident reviews have illustrated a range of structure root cause challenges around the effectiveness of these investments in t he face of an evolving threat landscape and organisational practices.

In this dynamic environment **Deloitte's Cyber SOC Advisory Practice** has been serving clients based on practical experience from designing and operating SOCs, and the library of insights that come from Deloitte's Cyber Incident Response and Post-Incident Reviews. Our practice can provide expert and balanced guidance on:

- Benchmarking and review of current SOC capability against industry standards and evolving attack techniques
- Using realistic modern attack techniques to test SOC effectiveness in detection and response
- Development of SOC strategy, including technology platforms; processes; workforce architecture; operating model, sourcing model and contractual requirements for outsourcing
- Independent reviews for boards and management teams
- Post incident-reviews where the SOC hasn't provided prompt detection
- How modern technologies such as Security Orchestration and Response (SOAR) and Artificial Intelligence (AI) can yield material improvements in productivity in SOCs

To continue the conversation, please contact:

Douglas Foster
Principal, Cyber
Deloitte Australia
dofoster@deloitte.com.au

Simon Gribble
Partner, Cyber
Deloitte Australia
sgribble@deloitte.com.au

David Owen
Partner, Cyber
Deloitte Australia
dowen@deloitte.com.au

Deloitte.

About Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche.

Tohmatsu. As one of Australia's leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au

Designed by CoRe Creative Services. RITM1525087