Cyber Onboarding is 'Broken'

Cyril Onwubiko[*] and Karim Ouazzane[+]

[*]Cyber Security Intelligence, E-Security Group, Research Series, London, UK
[+]Cyber Security Research Centre (CSRC), London Metropolitan University, London, UK

Abstract – Cyber security operations centre (CSOC) is a horizontal business function responsible primarily for managing cyber incidents, in addition to cyber-attack detection, security monitoring, security incident triage, analysis and coordination. To monitor systems, networks, applications and services the CSOC must first on-board the systems and services onto their security monitoring and incident management platforms. Cyber Onboarding (a.k.a. Onboarding) is a specialist technical process of setting up and configuring systems and services to produce appropriate events, logs and metrics which are monitored through the CSOC security monitoring and incident management platform. First, logging must be enabled on the systems and applications, second, they must produce the right set of computing and security logs, events, traps and messages which are analysed by the detection controls, security analytics systems and security event monitoring systems such as SIEM, and sensors etc.; and further, network-wide information e.g. flow data, heartbeats and network traffic information are collected and analysed, and finally, threat intelligence data are ingested in real-time to detect, or be informed of threats which are out in the wild. While setting up a CSOC could be straightforward, unfortunately, the 'people' and 'process' aspects that underpin the CSOC are often challenging, complicated and occasionally unworkable. In this paper, CSOC and Cyber Onboarding are thoroughly discussed, and the differences between SOC vs SIEM are explained. Key challenges to Cyber Onboarding are identified through *the reframing matrix methodology*, obtained from four notable perspectives – Cyber Onboarding Perspective, CSOC Perspective, Client Perspective and Senior Management Team Perspective. Each of the views and interests are discussed, and finally, recommendations are provided based on lessons learned implementing CSOCs for many organisations – e.g. government departments, financial institutions and private sectors.

Keywords: *Cyber Onboarding, SOC, CSOC, Security Operations Centre, SIEM, Reframing Matrix*

I. Introduction

Cyber security operations centre (CSOC[1]) is a *horizontal business function* (as opposed to a *capability*), responsible for cyber security incident management, detection, monitoring, log and event management. It is a horizontal business function because it should be a SOC for the entire organisation, catering for the needs and requirements of all groups, units and departments of the entire organisation, as opposed to multiple, tactical, isolated, standalone and fragmented SOCs that lacks situational awareness of the risks the organisation bears as a whole.

SOC is a *business requirement*, and for some government departments, it is a *mandatory business requirement*, in addition to a *compliance requirement* (see Her Majesty's Government (HMG) Security Policy Framework (SPF) [1]). This means that government departments are required to have SOCs, which may be interpreted as technical, process, policy and procedural (T3P) controls appropriate to detect, protect, and respond to incident, and however, of appropriate levels of their business impact assessments, and government security classifications assessment, such as OFFICIAL, SECRET and TOP SECRET[2], to comply with the UK Government HMG security policy framework.

As a *horizontal business function*, SOC executes the organisation's cyber security strategy and monitors controls (technical, process, policy and procedural) that enable, support and enhance the overarching cyber strategy of the organisation. For example, if an organisation's cyber strategy is one underpinned on active defence, it means that SOC activities should enable and support active defence to happen and including controls and policy mandates that promote and enable active defence, such as take down operations, tear down of connections, ports and services deemed malicious and suspicious etc. (see details of our proposed cyber security on Section IV of this paper).

SOC is equally a *compliance requirement* and may be used to fulfill other compliance requirements and regimes such as to perform security or protective monitoring requirements, comply to payment card industry data security standard (PCI DSS) or information security standards (ISO 27001) and information security management system (ISMS) etc.

Unfortunately, many organisations set up SOCs driven by compliance alone rather than for both active risk reduction and compliance. Majority of such SOCs are often generally not fit for purpose, (see extensive discussion in Section IV of this paper).

Large enterprises, who claim to have experience setting up SOCs have not done better either, as interviews and/or

[1] CSOC and SOC are used in this paper interchangeably, and means one and the same thing.

[2] UK Government Security Classification can be accessed from https://www.gov.uk/government/publications/government-security-classifications

experiences across many sectors who have used known large enterprises to establish their SOCs or outsourced their SOC function to large enterprise supplier organisations do not seem content with the level of service they received and/or are not entirely content of the maturity of supplier SOC service, either.

There are small to medium size (SME) supplier organisations who are specialist SOC providers, however, many of these SMEs are focused on the 'design and build aspects of the SOC service' and may struggle to operate the service due to the manpower or resource levels required to run a SOC; while a few of the SMEs are unknown brands and therefore find it extremely challenging to pass through the extraordinary economic, financial, commercial and procurement due diligence carried out by client organisations or government departments when procuring a SOC service, hence do not even get shortlisted to provide SOC services to large government departments or big financial institutions. Therefore, most of these specialist SOC SMEs operate at their equivalent tier of small to medium size client organisations.

Building a SOC comprises two key aspects – first, *building of the central log collection, aggregation, analysis and incident management platform* (here we refer this to as the **SOC Monitoring Platform**), and the second, is *onboarding or enabling of both new and existing services to be monitoring by the SOC monitoring platform*, (here we refer this to as **Cyber Onboarding**).

While a SOC monitoring platform may be built but the problem lays with onboarding services into it so that they can be securely and protectively monitored. We use the analogy of a *property* and its *content*. You could have an unfurnished property, where the property is built with the necessary doors and windows, but the property is empty and has no content, such as beds, chairs, cooker or electricity. The same can be said of a SOC monitoring platform without onboarding of the services and infrastructures it was built to monitor. Therefore, to have a functioning and operational SOC, then onboarding of services, systems and network infrastructure to the SOC monitoring platform must occur.

Note: In this paper, we use 'system' in its generic term to mean and encompass *computing device*, its *subsystems*, *applications* installed in it, and the *networking infrastructure*. For example, *computing devices* include servers, desktops, workstations, mobile, Tablet; and its *subsystems* include compute, middleware, storage e.g. storage area network (SAN), network attached storage (NAS) etc. *Applications installed* in the system include databases, operating systems, and agents such as anti-virus, intrusion detection systems, firewalls etc., while the underlaying *networking infrastructure* include routers, switches, fabric, hubs, cables etc.

The contributions of this paper are:

a) the differences between security information and event management (SIEM) and SOC are explained.
b) the factors impacting Cyber Onboarding are examined using the reframing matrix methodology.
c) recommendations to address the challenges facing organisation's Cyber Onboarding function are offered.

The remainder of the paper is arranged as follows: Section II discusses SOC vs SIEM, and in section III Cyber Onboarding is explained with a view to understanding its processes, activities and responsibilities. Section IV identifies and discusses factors affecting Cyber Onboarding deduced by applying the reframing matrix methodology. Section V offers recommendations to address Cyber Onboarding challenges, and finally, the paper is concluded in Section VI.

II. SOC vs SIEM

Many people conflate SOC with SIEM. This is the one primary confusion in this space. SIEM is a tool, which offers log management, event and log correlation, analysis and dashboard. Conversely, SOC is a horizontal business function comprising *People, Process* and *Technology* as shown in Figure 1, and expanded in Figure 2.

A: People

People may include analysts, administrators, incident responders, SOC manager and other managers etc. who are accountable for monitoring the organisations services by leveraging the capabilities offered by *Technology* (e.g. SIEM tool), and guided by the organisation's *policies, processes and procedures*. So a SIEM is not a SOC. Rather, a SIEM is a component or a subset of a SOC.

People are subdivided into two broad categories, namely: **cyber onboarding** people, and **SOC monitoring and incident management** personnel (see Figure 2). *Cyber onboarding* is a multidisciplinary team composed of solutions and technical architects, SOC designers, business analysts, risks and information assurance consultant and project managers (see Figure 2 and details in Section III). These are the people who carry out project related activities to ensure that each business service (a *business service* usually comprises, at the least, systems, network infrastructures and applications) to be monitored are properly onboarded to the SOC monitoring and incident management platform.

SOC monitoring and incident management is solely responsible for security monitoring, operational monitoring of onboarded services that are in the SOC platform, providing 'eyes-on-glass' monitoring, alerting and event analysis, incident triage, cyber incident management, coordination and reporting. They are also the custodians for fascinating and coordinating major incidents, incident governance and command, investigations and post incident reports.

B: Process

SOC processes in this paper encompass operational guides, local working instructions (LWI), knowledge articles (KA), procedures and operations-level policies. A sample of some SOC essential processes (see Figure 2) are cyber incident management playbook, incident response process, operational runbook or knowledge articles, joiners, movers and leavers (JML) process, SOC access control policy, security operating procedures (SyOPS) etc.

C: Technology

The *technology aspect*, as shown in Figure 2, comprise of the tools that are deployed in a typical SOC, such as SIEM, web fraud detection (WFD) to detect web-based transactional fraud, typically for financial orientated SOCs, IDS/IPS to detect and/or prevent intrusions, threat intelligence e.g. malware information sharing platform (MISP - *an open source threat intel feed*) and cyber incident management ticketing system for tracking security incidents tickets, assigning tasks and on-going incidents and issues. There are myriad of SOC tools, but the set discussed in this paper are core and essential.

The SIEM market is very mature with well-established products and a set of criteria to assess their offerings, e.g. Gartner SIEM Magic Quadrant [2]. Mainstream tools range from leaders IBM QRadar and Micro Focus ArcSight to the niche players such as Alien Vault USM, FireEye etc.

The misunderstanding is that many people procure SIEM tools and therefore believe they now have a SOC. This is absolutely incorrect. The tools, when setup properly, will no doubt help the SOC to perform its functions better, provided the 'the challenging' task of onboarding systems, logs, applications and networks to the SIEM is completed, including having the correct parsers, plugins or API (application programming interface) to ingest events from disparate log sources e.g. firewall, routers, applications, intrusion detection systems (IDS) etc. and also, the ability to ingest network-wide information such as flow events and threat intelligence information to detect emerging and inflight incidents [3, 4, 5].

A SOC must have the appropriate policies and processes to allow them to react swiftly to a cyber incident. For example, a SOC must have a cyber incident management playbook to respond to incident and coordinate significant cyber incidents [6], they should have other operating procedures such as security operating procedures (SyOPs), cyber recovery process, incident response process and reporting and escalation procedures.

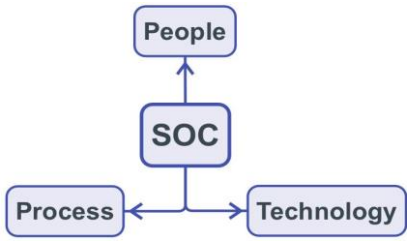

Figure 1: Security Operations Centre (SOC)

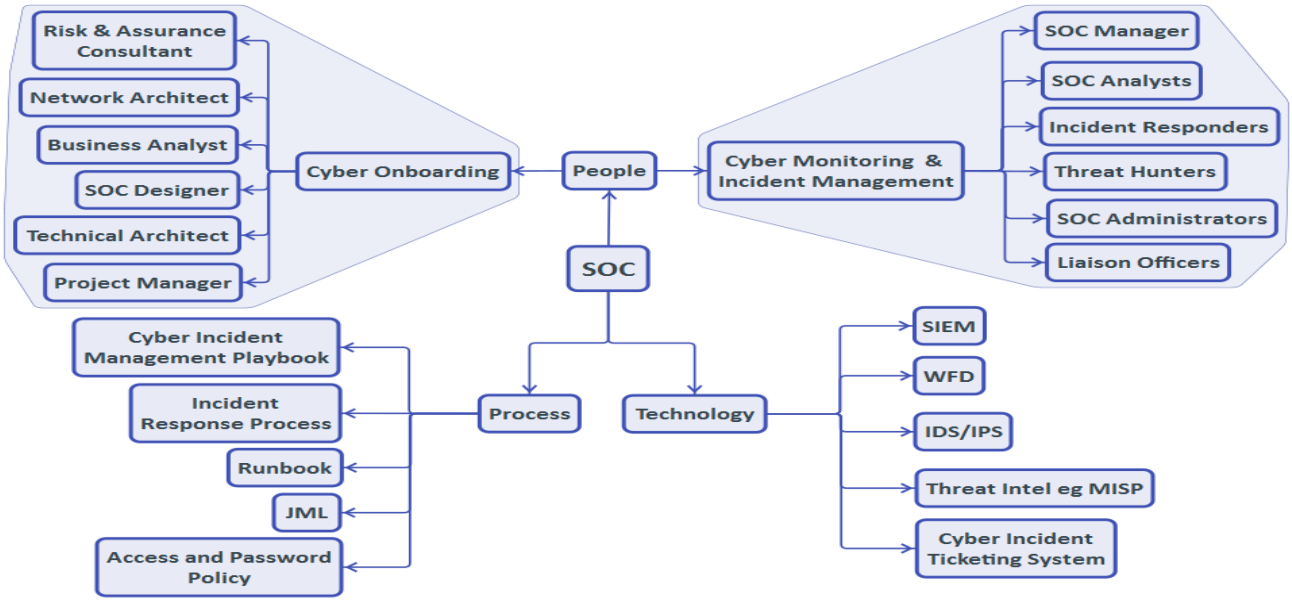

Figure 2: Expanded diagram of the SOC (as shown in Figure 1)

Human operators are required to monitor and conduct incident management and decision making. A SOC includes humans (a.k.a. people) who operate the SIEM, operationally monitor the dashboards and follow alerts and coordinate cyber incident response. These are some of the fundamental differences that make a SIEM not the same as a SOC. A SOC must have a human-in-the-loop, even with artificial intelligence (AI) and machine learning (ML) embedded endpoints and point solutions deployed in the SOC to better and faster detect incidents and threats, yet it needs human-in-the-loop to make decision and to conduct incident management and follow governance and incident commands.

The drive to 'outsource' everything was met with 'bring everything back in house' a couple of years ago, and recently, we observe that most companies now operate a hybrid managed SOC model. This is the case, for example, where a framework exists for organisations to outsource some aspects of the SOC service e.g. protective monitoring or "eyes-on-glass" (a.k.a. operations security monitoring) responsibility to a supplier organisation while incident management remains their accountability. While there are many reasons for outsourcing SOC function to supplier organisations, the two main reasons are:

a) The supplier organisation is tasked to do "the heavy lifting and shifting" – a perception that the expertise to run a functional SOC is readily available in the supplier organisation, hence it is believed that the supplier organisation is by far better to run and maintain a SOC service, while the client organisation becomes responsible for security incident management, escalation and decision making as the overarching risk owner.
b) Most client organisations work 9am to 5pm, therefore, client organisations prefer to leverage the 24x7[3] SOC service operated by the supplier organisations, a preference many client organisations believe to offer cost saving and value for money.

III. Cyber Onboarding

Cyber Onboarding follows a set of well-defined processes to onboard a service for cyber security monitoring (see Figure 3), covering discovery workshop, security monitoring requirements gathering, risk assessment, topology and architecture design, implementation, assurance and security testing, and handover.

These distinct processes are discussed briefly:

a) Discovery workshops are conducted per organisation, business unit or service to be onboard to the SOC monitoring platform in order to understand the specific monitoring needs of that organisation, business unit or service such that security monitoring is implemented appropriately to address the unique security monitoring requirements for that department, business unit or service.
b) Solutions design, architecture and integration patterns are produced based on the organisation's business needs, hosting arrangements, integration requirements, and connectivity options.
c) Topology map of the existing hosted environments is required in order to allow appropriate monitoring use cases to be developed to ensure that critical assets of the organisation are protected.
d) The implemented security monitoring solution will need to be tested and assured, and
e) Finally the solution is handed over to the SOC to monitor and operate.

Cyber Onboarding is a team in a **SOC function** responsible for ensuring that business services to be monitored by the SOC are appropriately onboarded to the SOC monitoring platform. This means, ensuring that the business services and the underpinning infrastructure and applications within that business area, such as firewalls, servers, desktops and network infrastructures are configured to produce logs and events, and that these events are transported and ingested by the SOC monitoring platform for analysis, correlation, alerting and incident triage (see Figure 4).

In some organisations, both the cyber onboarding team and the SOC monitoring and incident management team are the same; however, in this paper, we have presented these teams as distinct but cooperative teams under one management. Hence, the cyber onboarding may not exist as a distinct business unit in most organisations as their duties are performed by the SOC under one accountability business unit. Regardless, the cyber onboarding activities as shown in Figure 4, must be performed to have a functioning and operational SOC.

These activities include:

- creating design patterns and implementing architecture solutions for any service (existing or new) to be onboarded to the SOC platform for security monitoring;
- ensuring the assets of the business units to be monitored are enabled for logging and events generated by these disparate log sources are ingested and monitored by the SOC;
- enabling the right parsers and plugins so that logs are normalised[4] and forwarded to the SOC platform;
- ensuring that a transport mechanism exists for conveying logs, metrics, events, messages and flows from disparate environments to a central log collection, aggregation and analysis point for the SOC monitoring platform.

[3] 24x7 means 24 hours in a day and 7 days in a week.

[4] Normalisation is a process of using a consistent schema to process data, events or logs in exactly the same way so that meta-data types are stored on the same columns, for optimised querying and database performance

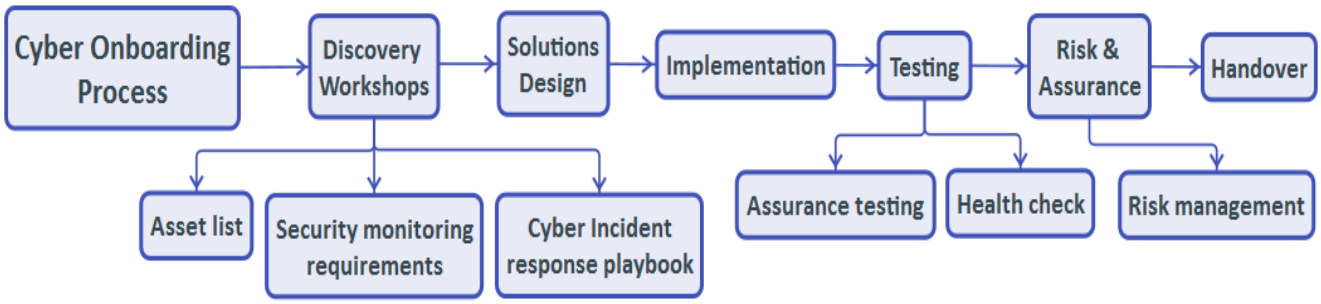

Figure 3: Cyber Onboarding Process

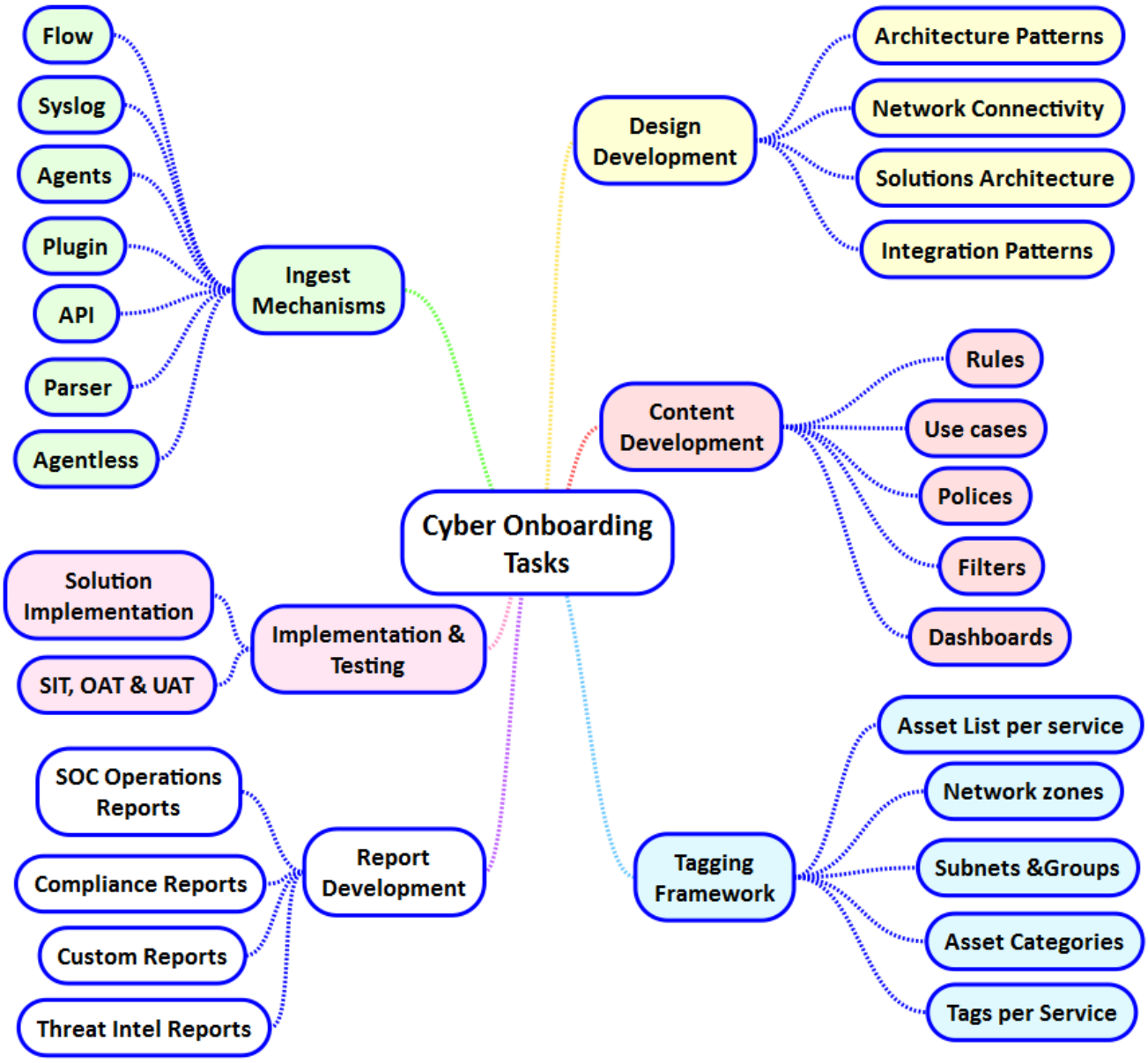

Figure 4: Cyber Onboarding Activities

Figure 4 is a representation of the activities carried out by the Cyber Onboarding team for the SOC.

These include:

a) Ingest mechanisms: This is a method to ensure that the different and disparate log types generated by the vast array of log sources in the monitored estates are appropriately ingested, normalised and analysed by the SIEM platform. This means ensuring that an ingest mechanism exist e.g., agentless, parser, API and plugin (see log source types in Table 1) for the appropriate log type and format; otherwise, custom parsers must be developed. Custom parsers are especially important for ingesting proprietary logs whose schemas do not comply or conform with appropriate and known standards, e.g. logging standards such as the IETF RFC 5424 format[5].

Table 1:Monitoring Metric and Formats [3]

S-N	Log Source Type	Log Source Example
1	Events and logs	Raw log, Alert, Event, Windows events, Syslog, Alarm
2	Network Information	Heartbeat, Flow, Session, Trap
3	Structured Digital Feed	Scan, Vulnerability Information, PCAP[6], TVM[7], CMDB[8], NVD[9]
4	Semi and Unstructured Digital	Trace, Manual Input, Wetware
5	Threat Intelligence	Indicators of Compromise (IoC)

b) Agent vs agentless: Agent and agentless are both mechanisms to ingest events by the SIEM. Agent-based ingest requires a third-party application or a package of the SIEM to be installed at the end device or endpoint. This is needed, in most cases, when the SIEM tool does not have a matching plugin to ingest logs or events of a particular log source type. For example, windows events do not follow the IETF RFC 5424 standard hence one way to ingest windows events is to install a third-party agent or software at the endpoint to convert windows events to syslog compliant format – this processing of using a third-party software or an agent to ingest logs and event is regarded as agent-based ingestion. The other option is to use agentless method where a third-party agent is not required, instead the SIEM tool accepts native or raw logs or uses API to receives and ingest the events.

c) Design development: The primary function of the technical and solutions architects in the cyber onboarding team is to develop robust and reusable architecture patterns, solutions design and integration patterns artefacts that allow various systems and business services hosted in different locations to be integrated to the SOC monitoring platform, allowing the SOC to securely monitor these services and systems. The created reusable architecture and solutions artefacts are signed-off and approved by the organisation's technical design authorities.

d) Implementation and testing: This allows the design artefacts to be implemented and tested. Testing can be carried out by other specialist teams, however, this activity should be coordinated through the cyber onboarding team, since they are the project-based arm of the SOC. Testing should not only include assurance testing, but also, security testing such as IT health checks, penetration testing and vulnerability scanning and testing. This is done so that any vulnerability (intrinsic or extrinsic) are mitigated prior to go-live. Since IT health checks are carried to establish intrinsic and extrinsic cyber hygiene of the solution, then it is best to be conducted by an external or independent provider (this is to avoid bias), however, the continuous vulnerability and threat management should still remain an in-house activity.

e) Tagging framework: This is a process of tagging events from specific business services as a way of distinguishing and separating services and this is particularly important in a multi-tenant and multi-customer SOC service, where incident response and escalation maybe different for each business services. Tagging is not only used to differentiate services, but also useful to manage business services with overlapping IP addresses, and where name resolution is not working properly.

f) Alerting and tuning: This is a process of improving the reliability of the service by ensuring that 'noise' and false positives are reduced and minimised. This is done by filtering out known noise on the monitored environment to improve both performance and reliability. The purpose of tuning is to baseline the service so that SOC alerts/alarms are reliable and trustworthy. Tuning do take time and could be considerably longer depending on size, scale and complexity of the SOC platform. On the average, it is common to allow three to six months for this.

g) Network groupings: This is a process of customising networks and subnets into their appropriate business areas, functions and groups to allow for quicker identification of incidents to affected business areas and networks.

[5] RFC 5424 – The Syslog Protocol, https://tools.ietf.org/html/rfc5424
[6] PCAP – Packet Capture
[7] TVM – Threat and Vulnerability Management
[8] CMDB – Configuration and Management Database
[9] NVD – National Vulnerability Database

h) Content development: This is a process of setting up some of the SOC monitoring artefacts such as rules, filters, use cases, queries and dashboards etc. Monitoring content is important as different business services may face unique risks and concerns; therefore, it is essential that the use cases are adapted to address their respective concerns and risks.

i) Report development: This is a process of creating both generic and custom monitoring reports for each business area and business service being monitored. Reports are used for many purposes, e.g. to assess the performance of the SOC service, benchmark the SOC service, review service and operation level agreements (SLA/OLA), key performance indicators (KPI), and most importantly, to measure the return on security investment (RoSI). Cyber metrics such as report against the risks mitigated, report on threats prevented or incidents encountered can be useful barometers to assess RoSI of the SOC. Sample SOC reports include SOC operations report, Good Practice Guide number 13 (GPG 13[10]) report and custom reports, which can be used for a number of other compliance purposes.

IV. Why is Onboarding "Broken"?

To build a **mature and effective SOC** takes time, especially one for a large enterprise, such as a government department or financial institution. It is a project that could easily span between 2-4 years dependent on a number of factors, e.g. technical, programmatic, commercial, logistic and organisational. For instance, the footprint of the estate to be monitored, the number hosting environments to be monitored, size, coverage and complexity of the organisation, the quality of monitoring required and the size of the project workforce, structure and organisation – internal, external, suppliers and partners, procurement frameworks and vehicle etc.

As discussed in Section III, Cyber Onboarding is a multi-stakeholder project involving multidisciplinary activities. Managing projects involving multiple stakeholders is challenging on its own, let alone doing so for a complex and challenging project. Since the main aim of this paper is to understand factors or reasons why many perceive cyber onboarding to be 'broken', we employ a proven methodology – **the reframing matrix**.

The reframing matrix [7], created by Michael Morgan [8], is a tool for critical reflection, insight and innovation. An ideal tool for analysing organisational issues from various perspectives that then allows the problem to be viewed from multi-stakeholder perspectives and viewpoints encouraging issues to be seen from different lens, opinions and insights.

As a problem-solving tool, the reframing matrix uses the four perspectives (4Ps) for insights, viewpoints, interests and concerns. Each quadrant of the matrix is a perspective. The problem to be solved is placed at the centre of the matrix, and opinions, views and concerns are then sought from the respective stakeholders. Based on the different views, solutions to the problems are obtained. It is pertinent that the stakeholders (4Ps) are selected based on their relevance and importance to the problem domain since the strength of the reframing matrix lies on the fact the different stakeholders with different experiences approach problems in different ways.

Our application of the reframing matrix to cyber onboarding is as shown in Figure 5. First, we put the question been assessed in the middle of a grid. We use boxes around the grid for the different perspectives. Each perspective represents a stakeholder group consulted in the assessment. The 4Ps are the Onboarding Team themselves, the CSOC team, the Client and the Senior Management Team.

Using the reframing matrix to identify the challenges faced by cyber onboarding (as shown in Figure 5), we identified **16 different issues** from **four perspective**, namely (clockwise):

- **Onboarding perspective –** as the function responsible for onboarding services for different clients and business units, they deal with the day-to-day fallouts and know the issue best, however, from a unique perspective.
- **CSOC perspective** – as the custodian for security monitoring, and people at the frontline' of the SOC service, so it is important that they are consulted for any reliable solution to the cyber onboarding problem to be identified, besides, they are the direct 'customers' of the Cyber Onboarding Team.
- **Client Perspective** – it is important that we consulted the client for a say, after all, they pay and consume the SOC service. If they are not happy then the business case for standing a SOC capability could easily disintegrate.
- **SMT perspective** – these are the senior management team, comprising the SRO, CTO, Directors and Heads of service. SMT are sponsor, fund and are accountable for the SOC service, therefore has an interest and a viewpoint of the problem.

The 16 issues identified are briefly explained.

From *Onboarding perspective*, they feel that lacked SMT support on a couple of organisational and process issues. They feel SOC is not mature in their operations and skillsets. There is a sense of acceptance that cyber onboarding is indeed complex and complicated, and there are a number of dependencies hindering progress.

[10] Protective monitoring of HMG system guide - good practice guide number 13 –. A defunct guidance but still being reference by many UK government departments.

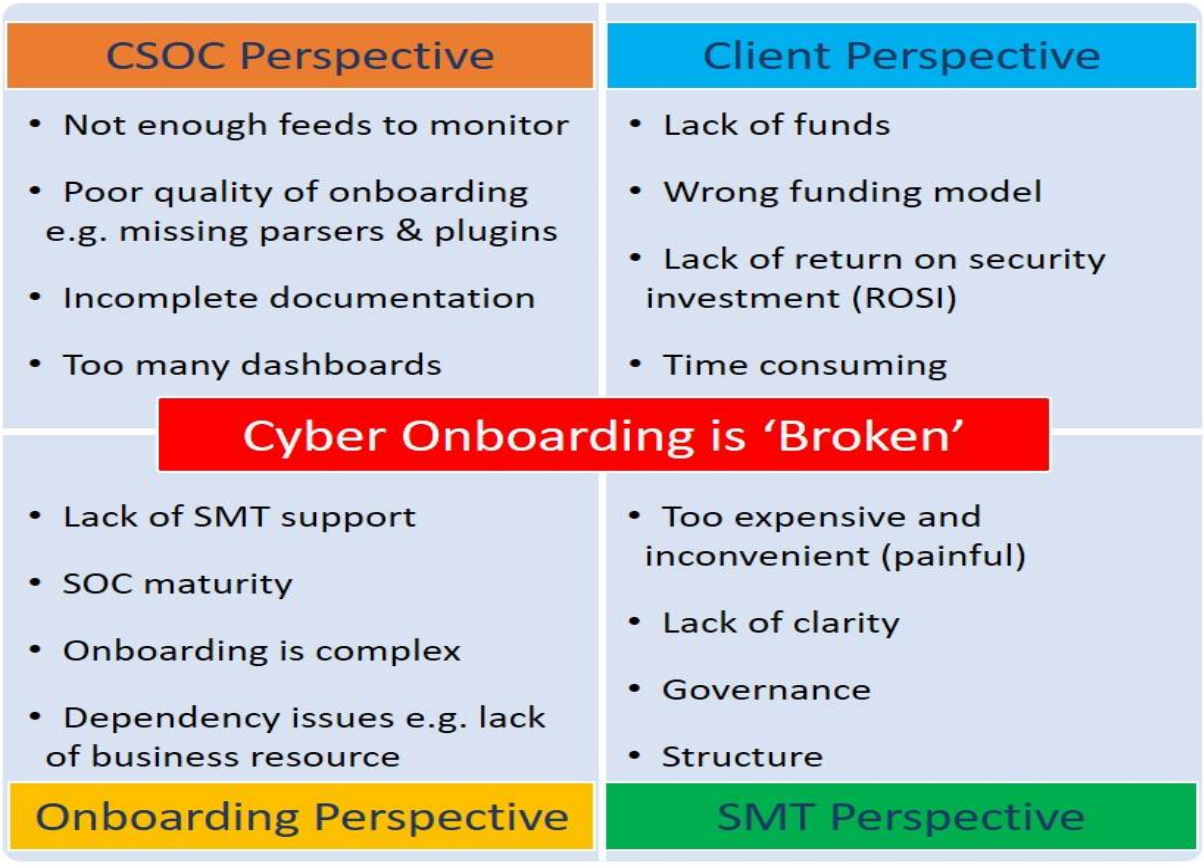

Figure 5: Cyber Onboarding Reframing Matrix

From *CSOC perspective*, they feel they are not provided with enough information feeds to monitor. So the onboarding team are not onboarding systems and services quick enough. There is quality issues and incomplete documentations provided to them, which then impacts how quickly they can react, and also, they feel there are many screens to monitor.

From *Client perspective*, there is appreciation of lack of funds. So they do not have funds to pay for the SOC service, and they feel they should not have to pay for a SOC service operated in-house, therefore the funding model is not appropriate. They said there is nothing to show for security monitoring even when it is enabled because they do not receive regular reports or KPIs for the SOC service, and they feel cyber onboarding is very time consuming to rollout.

From *SMT perspective*, they feel cyber onboarding is costing them far too much, hence it is an upscale project. They feel that the metrics and progress they receive from the onboarding team is not clear most times, and that the governance and structure between CSOC and Onboarding teams should be improved.

Following the reframing matrix analysis (see Figure 5), we conducted a further assessment to see if some of the viewpoints could converge. The 16 viewpoints are now consolidated to 8 key factors that make cyber onboarding challenging and often perceived to be 'broken', as follows:

A) Complexity

If cyber onboarding is simple then establishing a functioning SOC would not have been so difficult, unfortunately, this is not the case. The process to onboard a service is straightforward in principle (see Figure 3) but often challenging in practice. For example, a service to be onboarded may be hosted in multiple locations and comprising a myriad of different log sources, across the stack, ranging from physical, network, operating systems, middleware, databases to applications. In addition, for a cloud service, this may include hypervisors and/or containers, which also need to be monitored. Each of these stacks will need to be monitored to have a truly complete service onboarding. The problem is that many of these stacks produce logs and messages in varying formats (see Table 1) most of which are non-compliant with the IETF RFC 5424 standard, and a couple may include proprietary formats, especially applications coded in non-compliant formats, therefore the mechanism to ingest and normalise these events is not so trivial. All of these contribute to the complexity, complication and convolutedness.

Additional factors contributing to complexity include A1-A3:

A1) Architecture designs and patterns

SOC design and architecture is not a one size fits all. Each service onboarding requires a unique design, and at best may leverage existing patterns which will still need to be adapted and implemented, and at worst, a new set of designs are to be produced. The design requirements may be different to the overall design of the SOC monitoring platform itself, therefore, each service to be onboarded will need its own design and solutions architecture, which may utilise existing network connectivity or the provisioning of a new network connectivity to transports logs, events or messages of the onboarded business services to the SOC platform for analysis, correlation and cyber incident triage. The network connectivity (local area networks included) may require a form of wide area network, routing, and security controls enabled to ensure that appropriate policies such as access controls, security groups, blacklisting and firewall policies are correctly implemented.

A2) Risk assessment

Each business services to be monitored has its own risks or concerns for why it needs security monitoring. For example, a bank implementing security monitoring for their online banking system may do so in order that the SOC will monitor its online bank transactions, hence the risks or concerns are about monitoring of their online banking transactions and ensuring the right customers and correct payments are made; however for a government department responsible for immigration or issuance of national passports, their risks and concerns for security monitoring is obviously different. Here, their concern is to ensure that national passports are only issued to legitimate citizens, that passports are not flaunted on 'black market', and illegitimate documents are not used to obtain national passports. Security risks and concerns are bound to be different based on business functions for different corporations, institutions and government departments. These unique risks and concerns will need to be turned into security monitoring use cases and policies. This process requires niche skillsets, not trivial, and adds a layer of complexity, too.

A3) Security monitoring requirements

As organisations' business offerings and services are different so are their security monitoring needs. Security monitoring requirements will differ among departments, business units and services, therefore onboarding of each department, business unit or service is bound to be subtly different. While onboarding may follow a fairly straightforward process, however, each business service onboarding requires unique set of solutions ranging from architecture pattern to monitoring use cases.

Take two UK Government Departments for comparison. The Department for Work and Pensions (DWP) for example, their primary responsibility to the UK citizens and government is social welfare to UK citizens in the form of housing allowances, job seekers' allowances etc. to appropriate UK citizens, and on a timely manner. Conversely, HM Revenue and Customs (HMRC) is responsible for collecting taxes e.g. VAT, annual returns, PAYE, customs etc. from citizens and corporations, hence the former's cyber security monitoring need is focusing on ensuring appropriate social welfare arrangements are paid to suitably qualified citizens while the latter ensures and enforces taxes are received from citizens and corporations. Of course, their security monitoring requirements are different and predicated on their business obligations. This goes to demonstrate again that security monitoring and cyber onboarding is not a one size fits all proposition. This uniqueness and tailoring of the cyber onboarding deliverables per business service onboarding adds a layer of complexity and intricacy.

B) Strategic Support

SOC, like every organisational cyber security programme, has a slim chance of success without strategic support from the senior management teams (SMT). Strategic support is particularly fundamental with SOCs because of its remit, since it serves both as a *horizontal business function*, and as a *compliance mandate*. Without strategic support, SOC will be unable to perform its role of compliance, audit and regulations.

One of the main challenges facing SOCs is having appropriate authority to conduct protective and security monitoring across an entire organisation if SMT have not lend their support and approval. SOC is a horizontal business function, meaning it should be instituted to serve all business units of an entire organisation and should have the prerequisite authority to perform audit, security compliance checks and as an enabler to drive continuous security improvements across the organisation. This is important since cyber-attacks can be exploited from any aspect of the organisation and may use a weakness in one aspect as a channel or conduit to exploit other parts of the business. Hence, SOCs must be empowered, as monitoring custodians, to perform its duties accordingly.

C) Funding Model

SOC is an upscale project, requiring the procurement and implementation of a myriad of cyber tools, such as SIEM, intrusion detection systems, flow analyser, transaction monitoring (web fraud detection), threat intelligence and possibly user and entity behaviour analytics (UEBA) etc. These tools can be expensive, including software licenses and professional services costs. In addition, the SOC needs facility – the physical operating environment, and human resources to operate and monitor the service and including handling incident response and management. Considering that the project, depending on the organisation's size and scale, may last for a couple of years from start to go-live, and subsequently, the operational people aspect to manage and operate the SOC as normal business as usual (BAU) staff, who must still be costed, then, it is essential that the right funding model for the SOC exists.

The absence of appropriate funding model is likely to impact the success, or the effectiveness of a SOC. SOCs are a medium to address cyber risk and encourage good cyber hygiene, it is therefore pertinent that SOC's funding model is based around *active risk reduction* as other funding models is likely to

encourage 'wrong cyber behaviour'. For example, the 'right cyber behaviour' is to encourage active risk reduction as opposed to risk mitigation approach based on 'low hanging fruit'. The reasons for this are that 'easy and quick wins' do not necessarily mean effective prioritisation and efficient risk reduction, because the 'quick wins' may not yield the same risk reduction. We posit that, based on risk proportionality, monitoring an organisation's asset that is either marked for decommissioning or that is not particularly important to the organisation does not yield the same risk reduction as opposed to monitoring the origination's customer database, or their intellectual property.

Similarly, protectively monitoring a standalone guest WiFi just because the guest WiFi project is funded as opposed to offering the same security monitoring on citizens data based on risk reduction encourages wrong cyber behaviour.

Our proposal to addressing the 'cyber behaviour problem', one we strongly recommend, is to ensure that SOC – here we mean SOC and its composite teams such as Cyber Onboarding – is **directly funded**. We distinguish between **direct** vs **central** funding. **Direct funding**, we define as funding allocated directly by the organisation, usually granted or assigned to a business unit and ringfenced for its purpose alone and secured through a business case. On the other hand, **Central funding**, we define as a type of funding arrangement which is obtained by *collectively levying other business units as a contribution for payment of service they have received, or will receive*, and are often referred to as '**cross-charge**'.

SOCs should be **directly funded** to afford it the autonomy to onboard and monitor services that *actively attribute to actual risk reduction*. Prioritisation of services to be monitored by the SOC must not be decided or dictated solely on the basis that an individual business unit has funds or budget, but because the services to be onboarded are those that will *reduce risk exposure* in the ecosystem and to the organisation as a whole.

The premise for onboarding a service just because the project has funds is totally unacceptable. We see this as one of the main drivers of wrong cyber behaviour across many government departments. Fundamentally, if a SOC is centrally funded, it means it has no choice as to which services it monitors, because it will be underpinned on 'first come, first served'. That is, the SOC will serve those who have contributed or paid for their services and this may mean monitoring services of lesser priority/criticality over those that are significantly critical.

D) Strategy

Every efficient SOC has a clear strategy underpinned by the organisation's Cyber Strategy. Every organisation should have a Cyber Strategy. An organisation cyber strategy is a blueprint for cyber, business transformation, business enablers, governance, risk and compliance.

Organisation Cyber Strategy should adopt cyber principles that encourage, support and enable business and digital transformation agenda, e.g. digital by default, secure by default, active risk management, active defence, proactive and continuous monitoring, cyber resilience and recovery etc. These are the enablers of strong economic wellbeing, creating an environment where businesses thrive by ensuring that digital technology and its frontier are secure. The UK Cyber Strategy [9], a blueprint for national cyber security strategy, aims to create an environment where businesses are confident, capable and resilient in transformational digital world.

For both national and organisational cyber security strategy to be achieved, investments in SOC, Cyber Programme, Governance, Risk and Compliance (GRC), Personnel and Physical security, Cyber Security Training, Awareness and Education need to occur.

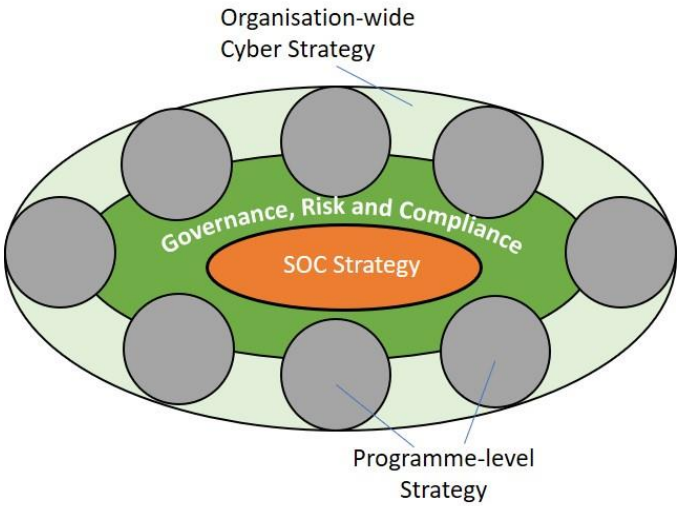

Figure 6: Conceptual Cyber Security Strategy supporting and enabling programme-level strategies

In Figure 6, we present our proposed conceptual organisation cyber strategy. It starts with an organisation-wide Cyber Strategy underpinned by GRC and SOC strategies. GRC provides the steer, direction and metrics for 'what good looks like', while SOC executes and monitors.

The proposed cyber strategy is conceptual, which makes easily adaptive. The rationale for proposing one is because often cyber strategies are discussed in abstraction, so we thought a better way to evolve the discussion is by providing a conceptual blueprint. As shown in Figure 6 are three concentric ovals (not circles[11]), the overarching one being the organisation-wide cyber strategy, supported by the GRC strategy, and underpinned by a stronger but much smaller oval, which is the SOC strategy. The various smaller circles each represent programme-level strategies being enabled by the Cyber and

[11] We use ovals to represent the organisation strategy, the GRC and SOC strategies because in reality, such strategies will continuously improve, hence, will be at odd with the geometric properties of a circle.

GRC strategies and supported by the SOC. A SOC strategy is not one that supports and enables the overarching organisational cyber strategy, but also, one that creates a continuum for it to be implemented, practiced and embedded. We argue that the dependability of both the GRC and SOC makes the organisation-wide cyber strategy and all the other programme-level strategies achievable, reliable and capable.

E) Goals and Objectives

With Cyber and SOC strategies come functional goals and objectives. Functional objectives help achieve business goals, and both in turn enable the strategy to be achieved.

To achieve the SOC strategy, high-level **business goals** which are fulfilled by low-level **functional objectives** must exist. A successful SOC function (comprising people, process and technology) is realised on overarching strategy, business goals and functional objectives.

Using the Cyber strategy discussed in Section IV D) as an example, a primary goal of the SOC will be to provide realtime security monitoring across the monitored estates. The rationale for this goal is that a goal must directly support its strategy; therefore, to support the SOC strategy of active defence and digital transformation a key enabler is proactive and realtime security monitoring. Further, a key functional objective to achieve the business goal, will be to ensure that the SOC has trained and capable personnel to operate the SOC (i.e. towards SOC maturity).

For SOC to be successful, it must have clear set of goals and objectives that support its strategy, and the wider Cyber Strategy.

F) Governance and Onboarding Prioritisation

Every organisation should have governance boards, well-defined governance structure, and clear delineation of roles and responsibilities. At a strategic level, there should be a Cyber Governance Board accountable for Cyber. Membership to this board should include the following, at the very least, Cyber SRO, Director of Cybersecurity, Head of GRC, SOC Director/Head, Programme-Level Directors from Business Services. This board should be responsible for deciding on the critical services and systems, through a risk based prioritisation, to be onboarded for security monitoring.

Further, organisational governance structure and hierarchy must be clear so that SOC knows who is in charge with clear point of escalation and reporting. It is important that such structures are communicated not only to the SOC, but also, to the entire organisation. After all, security is everyone's responsibility.

There must be a clear set of rationale based on active risk management for the candidate systems and services to be prioritised. The risk-based prioritisation scheme should take into consideration such metrics as:

- sensitivity of the assets
- criticality of the asset e.g. critical national infrastructure
- value of business data it holds e.g. citizens data, business data, national data
- value at loss
- degree of susceptibility of attack
- vulnerability of the asset, or that may exist with the controls currently protecting the asset
- mean time to restore
- disaster recovery targets
- cyber response and recovery objectives

G) SOC Structure and Approach

All the capabilities shown in Figure 2 should sit under one SOC structure. Getting a **SOC structure** right cannot be overstated. It is often the prime causes of an inefficient and immature SOC. The rationale for recommending that all the composite aspects of a SOC sits under one authority is because, it works better and more coherent under one leadership.

If some of the functions, such as Cyber Onboarding were to be under a different structure or authority it will cause friction and fester the perception of 'them' and 'us' mentality, which is needless. Secondly, coherence is key for an effective SOC. That is, the ability to have consistency in processes, administration, methodologies and communication. Communication is important. Information from the SOC to the entire organisation should be concise and consistent.

A SOC structure should support and enable its approach. There are various approaches to operating a SOC, and in this, we are referring to the operating model rather than whether it is outsourced or insourced. The operating model, that is, the SOC operating service hours, for example, 24x7 or 9x5 or 7x7 plus on-call hours. Operating model is governed by business cases determined by the ways of working of all the other stakeholders performing reliant activities either for the SOC or to the business.

Most SOCs operate 24x7 service, which means they work round the clock, 24 hours in a day, 7 days in a week, including Saturdays, Sundays and bank holidays. While some SOCs operate 24x7, this could be arranged as 9x5 plus on-call for after hours and weekend; or 7x7 services complemented with on-call for after hours. Either way, the objective is to have a service coverage that supports the organisation's risk appetite and that are relevant and efficient.

It is pertinent to note that, for example, if a SOC operates 24x7, but some business teams or stakeholder groups are not, then it may make the need for 24x7 SOC ineffective, because if an incident happens during non-working hours and the business teams that are needed to assist with the incident, e.g. networks and infrastructure teams are not 24x7, it then means that the incident will be queued to this team and will be in their queue until when they start work in the following morning. This is not

an ideal case and one the puts the effectiveness of the SOC in jeopardy.

SOC operating model must be approved by the SMT based on business case, benefit realisation and business efficiencies. It is important to note that, SOC can operate 24x7 in many formats efficiently as discussed prior.

H) SOC Maturity

SOC maturity is assessed against many factors, unfortunately, there is no consensus on the factors or criteria that should be used. In this paper, we have carefully selected five generic criteria, we believe should help with operating an effective SOC underpinned on risk reduction, in our assessment. Further, we have also provided a list of some quantitative and qualitative factors that organisations may consider when conducting SOC assessment of their own.

The **generic factors** include:

1. adequate and capably trained staff,
2. robust SOC and Onboarding processes, policies and procedures,
3. appropriately tuned SIEM tool,
4. cyber incident management, reporting and investigation,
5. threat intelligence and threat hunting.

The maturity of a SOC can be assessed on other factors such as **qualitative factors** e.g.

- quality of logging
- how quickly the SOC can recover from a cyber-attack
- how quickly they can respond to a significant cyber incident
- cyber response and recovery readiness
- forensic readiness

On the other hand, SOC maturity can be assessed by **quantitative factors** such as:

- the number of true positives or incidents the SOC detects
- the volume of data analysed in seconds or minutes,
- the number of events processed,
- the number of metrics used in the analysis, e.g. logs, events, flows, PCAP and traps (see Table 1) and
- finally, if monitoring is across the full stack of infrastructure, operating systems, middleware, containers, databases and applications.

Whichever criteria (generic, quantitative, qualitative or a combination of all) are used to assess the maturity of a SOC, there must be rationale for their uses.

I) Supplier Incentive

As discussed in Section IV, to build a SOC service often involves multiple stakeholders ranging from internal teams e.g. SOC team, networks and infrastructure teams, to external organisations e.g., suppliers and professional services partners. For instances, a supplier may be responsible for hosting, another for management of existing legacy services and another for deployment of new services. Whatever their responsibilities are, to deploy a SOC multiple stakeholders are often required. Since the main objective of a SOC is to ensure that all services to be monitored, whether in the supplier environment, hosted applications or cloud-based applications are onboarded, therefore, the SOC will deal with a range of multiple stakeholders and should have a plan to incentivise suppliers and delivery partners in order that the desired outcomes are achieved.

Supplier incentives could be by way of communication to the supplier community of the SOC strategy, and the need for cooperation in order for all assets to be onboarded. This may include *change notices* and *contract change notices* (that is, payment related change notices), impacting and assessment processes that are lean and workable. In addition, supplier incentives may take other forms of collaborative frameworks or memorandum of understanding, such as co-location agreements or deployment of third-party applications into an existing hosting arrangements or procurement of new contractual arrangements.

V. Recommendations

Our recommendations stem from arguments in the preceding sections of this paper. The recommendations are MoSCoW'ed (*Must*, *Should*, *Could* or *Would*) to highlight importance, as follows:

a) An organisation **must** have a cyber strategy upon which SOC strategy and other programme-level strategies hinge, such as network operations centre (NOC) strategy, network and infrastructure strategy, programme management strategy etc. The absence of a cyber strategy will mean that there is no coherent organisation-wide blueprint to work toward, and this is likely to lead to standalone, tower-based models that are fragmented, isolated and divergent.

b) A SOC strategy **should** support and enable the organisation's cyber strategy and offer a mechanism to deliver the cyber strategy.

c) Governance, structure and approach **must** exist, and are fundamental to achieving a fit for purpose and functional SOC. It is imperative to have clear delineation of roles and responsibilities and a distinct line of escalation and reporting, as these will build the enabling environment for an efficient SOC.

d) All SOC composite teams as shown in Figure 2 **should** be under one authority and governance structure as this will enable the SOC to operate much more efficiently. SOC is complex and adding extra layer of complexity by way of segmenting SOC composite teams under different governance may stifle SOC progress and its autonomy.

e) Whether SOC is funded centrally or directly, having its own ring-fenced funds devolved from individually funded projects allows it to make security decision based on risks rather than funding. Onboarding prioritisation or selection of candidate services to be continuously and protectively monitored based on funding drives wrong behaviour as we have seen in Section IV C). Hence onboarding prioritisation of candidate system to be monitored **must** be based on active risk reduction.

f) Finally, as SOC is both a horizontal business function and compliance mandate, therefore, it **should** be assessed so that business return on investment and return on cyber security investment are measurable. SOC maturity is one way of achieving this and it is pertinent that the organisation is clear on what metrics or criteria they want to use to measure this growth. As discussed in this paper, we have offered three sets of assessment factors including quantitative, qualitative and generic (see Section IV H).

VI. Conclusions

SOC is a major organisational investment driven by two needs:

a) cyber security needs of detection, monitoring, response and recovery from cyber-attacks, especially since modern cyber-attacks are emerging, complex and challenging.

b) compliance mandate to satisfy regulatory and compliance obligations such as the HMG security policy framework, PCI DSS, ISO 27001 and other compliance regimes.

Building an efficient SOC takes time and effort. Organisations must have a roadmap of SOC delivery aligned with capability and maturity. This is so that it can assess its achievements but more so, to be better planned.

SOC is not a one-size-fits-all. Even when a SOC is built for a single organisation, business unit requirements will be different, and risks and concerns are likely to be subtly different and hence SOC and security monitoring use cases must be adapted, tailored and relevant.

While SOC processes maybe straightforward, however its success is dependent on cooperation from multiple stakeholders, and in most cases suppliers; therefore, organisations that find themselves in a similar model should have an approach to incentivise suppliers and stakeholders in order that their overarching goals and objectives are accomplished.

Finally, SOC must have an operating model, and this must be predicated on business case, relevance and wider stakeholders' ways of working. For example, a SOC can operate 24x7 in multiple ways; and of course, should not operate 24x7 if the organisation's business case and risk appetite dictate differently.

Future work

Three key areas of future work either for the authors or for other researchers, and maybe to form a PhD study are as follows:

- It will be helpful if research on organisational cyber security behaviour is conducted to assess what factors drive good or wrong cyber behaviours among organisations, e.g. compliance, funding models, governance structure, complexity etc.
- It will be useful to have agreed set of SOC maturity metrics. While we have provided three compelling set of metrics (quantitative, qualitative and generic) on SOC maturity, we believe, it still requires further in-depth studies.
- Finally, it would be interesting to conduct the same research the authors have carried out in this paper from a SOC supplier standpoint.

References

[1] HMG (2012), "HMG Security Policy Framework", Version 8, April 2012.

[2] Gartner (2018), "Gartner SIEM Quadrant", 2018 Reviews

[3] C. Onwubiko (2018), "CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process" published in 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 10.1109/CyberSA.2018.8551486

[4] C. Onwubiko (2017), "Security Operations Centre: Situation Awareness, Threat Intelligence and Cybercrime" published in 2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 10.1109/CyberSA.2017.8073384

[5] C. Onwubiko (2015), "Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy, published in 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)

[6] C. Onwubiko and K. Ouazzane (2019), "SOTER: A Playbook for Cyber Security Incident Management" yet unpublished.

[7] Mindtools (2018), "The Reframing Matrix", accessed 30th December 2018, https://www.mindtools.com/pages/article/newCT_05.htm

[8] M. Morgan (1993), "Creating Workforce Innovation", Business and Professional Publishing, Sydney, 1993

[9] HMG (2016), "National Cyber Security Strategy 2016-2021", 1 November 2016.