Cyber Security Operations Centre

Security Monitoring for protecting Business and supporting Cyber Defense Strategy

Cyril Onwubiko
Intelligence & Security Assurance, E-Security Group
Research Series
London, UK

Abstract— Cyber security operations centre (CSOC) is an essential business control aimed to protect ICT systems and support an organisation's Cyber Defense Strategy. Its overarching purpose is to ensure that incidents are identified and managed to resolution swiftly, and to maintain safe & secure business operations and services for the organisation. A CSOC framework is proposed comprising Log Collection, Analysis, Incident Response, Reporting, Personnel and Continuous Monitoring. Further, a Cyber Defense Strategy, supported by the CSOC framework, is discussed. Overlaid atop the strategy is the well-known Her Majesty's Government (HMG) Protective Monitoring Controls (PMCs). Finally, the difficulty and benefits of operating a CSOC are explained.

Keywords— *Cyber Security Operations Centre; CSOC; SOC; Cyber Incident Response; Cyber Situational Awareness; CyberSA; Log Source; Analysis; Correlation; Risk Management; CSOC Strategy; CSOC Benefits & Challenges*

I. Introduction

It is fact that the last ten years have witnessed a significant business operational shift; that is, a move away from traditional brick and mortar to the adoption of online digital market presence. At present, it is hard to see a reputable organisation without an online digital presence. The benefits of online digital marketplace are enormous, and in the 21st century, it is practically unavoidable. For instance, all manner of services are now provided online, ranging from internet banking, state welfare services, gamming, commerce and communications to electronic health services. Even services that were traditionally conducted face to face such as citizens' welfare services are now provided online.

While online digital presence offers a number of benefits, ranging from substantive economic benefits, ease of use to quick and instant access to people and services across different physical geographies, it has also offered proportionate challenges at times. One of such challenges is that organisations or individuals with online digital presence are highly susceptible to cybercrime and cyber-attacks. This worry is further exacerbated by the continuous expansion of the cyberspace, and the emergence of disruptive technologies such as Cloud computing, Internet of Things (IoT), Internet of Everything (IoET), which in turn have extended the attack surface.

That said, emerging technologies are a good thing. Emerging technologies such as wearables, social media, cloud computing are there to be exploited to provide quality and swift access to services, enhance social interactions, improve communications, provide reliable and trusted transactions. In addition, other business related ventures are much more straightforward, accessible, instantaneous and reachable online.

Cybercrime and cyberattacks are real and unavoidable. Even the 'best' protected services and businesses can be attacked and exploited. Vulnerabilities exist in every asset and organisation, which can be exploited or used as a conduit to cause exposure or compromise to critical services. Technologies are continuously evolved, and growing in complexity, cyber landscape is increasing, for instance LANs, MANs, WANs, Internet, Cloud Computing, IoT and IoET, which in turn increase the attack surface.

Some of the current cyberattacks and cybercrime are unprecedented, complex and cause substantive financial losses. For instance, in 2011 an RSA security breach claimed to have stolen intellectual property (IP) material of RSA security platform (RSA SecurID software) resulted to significant losses to the organisation [i]. In August 2014, a data breach to JP Morgan Chase resulted to the loss of personally identifiable information (PII) of over 76 million households and about 7 million small and medium size businesses [ii]. In January 2014, Sony suffered an unprecedented cyberattack to its gaming and film platforms, resulting to the delay in the release of the movie 'The Interview', resulting to yet to be quantified financial losses [iii], and most recently, in Jan. 2015, whilst President Barak Obama was passing to bill the United State inaugural Cyber Security Policy, the US Central Command (CentCOM) twitter account was compromised by a group who referred to themselves as the 'CyberCaliphate' [iv]. These are demonstrable evidence that cybercrime and cyberattacks are real, and should be taken seriously.

To protect an organisation's critical services, networks, systems and infrastructure an approach is to continuously and protectively monitored the organisation's ICT and applications, and to ensure there is an incident response plan in the event of a security breach, compromise or policy violation.

To continuously and protectively monitor business services and operations, a cyber security operations centre is required who should be responsible for monitoring critical business ICT systems in the estate; infrastructure and business applications that perform critical business services. The CSOC should be tasked with the operational responsibility of continuously monitoring privileged user access, and ensuring privileged users have access to only services they should have access to, access rights should be granted/provisioned based the least privileged principle, and that access is limited to roles and responsibilities, and are uncontrolled. Access must also be based on the 'need to know' principle, and driven based on business functions being performed by the individual.

In this paper we propose the use of the cyber security operations centre to continuously and protectively monitor critical business services in order to protect online digital services, response and manage cyber incidents, and support both forensic and incident readiness processes, as shown on Figure 1.

The remainder of the paper is organised as follows: Section II discusses the CSOC framework, including log collection, analysis and response, as the primary responsibility of the CSOC. Section III describes the people, process and training needs of the individuals operating the CSOC; section IV outlines a CSOC strategy, driven by business needs and strategic goals, and finally, the paper is concluded in section V.

II. CYBER SECURITY OPERATIONS CENTRE

A *security operations centre* (SOC) has been defined as a generic term describing part, or all of a platform whose purpose is to provide detection and reaction services to security incidents [13].

In this paper, we describe a *Cyber Security Operations Centre* (CSOC) - as a centre that comprises People (*Analyst, Operators, and Administrators* etc.) who monitor ICT systems, infrastructure, applications and services. They use Processes, Procedures and Technology in order to ***deter*** computer misuse and policy violation, ***prevent*** and ***detect*** cyber-attacks, security breaches, and abuse, and ***respond*** to cyber incidents (see Figure 1).

The terms SOC and CSOC are used to denote the same meaning in this paper.

What do SOCs/CSOCs do? They

- Ensure ICT systems, infrastructure and business applications of an organisation are identified.
- Ensure systems, infrastructure and applications are protected and monitored.
- Ensure vulnerabilities that may exist in, and within the IT estates are identified and managed.
- Identify threats that could compromise or exploit the vulnerabilities to break in.
- Identify threat actors that could be interested or that may wish to attack the business.
- Monitor the IT estate for real-time or near real-time cyber-attacks, policy violations, security breaches or anomalous and symptomatic events, or deviations.
- Profile identities that appear suspicious, interesting and 'risky'.
- Analyse events and alerts in order to determine if they are associated/related to streams of ongoing attack.
- Analyse historical events logs for patterns and trends (trending) symptomatic of an attack / compromise.
- Triage and investigate incidents.
- Coordinate, contain and respond to cyber incidents.
- Provide report and management information.

The responsibility of the CSOC can be split into three major categories – Collection, Analysis and Response, as shown in Figure 1. The organisation's ICT systems, infrastructure and business applications are configured to produce logs, for example, switches, firewalls, servers, mobile devices etc. They are referred to as Log Sources, because they produce/generate logs whenever an event occurs. The logs they produce are stored locally on each device making it difficult to be analysed centrally. Log collection is a process by which locally stored logs on each device are transferred to a central repository where they can be collectively analysed in order to detect incidents, especially network-wide or organisation-wide incidents. By monitoring the assets in the organisation, security analysts and operators are presented with the opportunity to gain some understanding of the patching level, the health of the assets in the estate, knowledge of vulnerabilities and policy gaps that may exist in and around them, understanding of the risks and impacts, including knowledge and foresight to determine, and hence predict possible situations that could lead to compromise or exposure – that is, *situational awareness* of the entire estate or of the monitored infrastructure. *Cyber situational awareness* of an organisation's estate not only provides a rich picture of the health of the enterprise – systems, infrastructure and critical applications of the organisation, but also, offers knowledge and insight into the wellbeing of the security analysts and operators supporting and operating the CSOC service. For instance, identifying and understanding the number of *faults* and *issues* caused by *operator mistake*, *administrator error*, or *analyst programming error*, could help provide context and insight to the security analyst's training needs, workload and/or cognitive health.

Detailed discussions of each of the functional components (collection, analysis and response) are presented as follows:

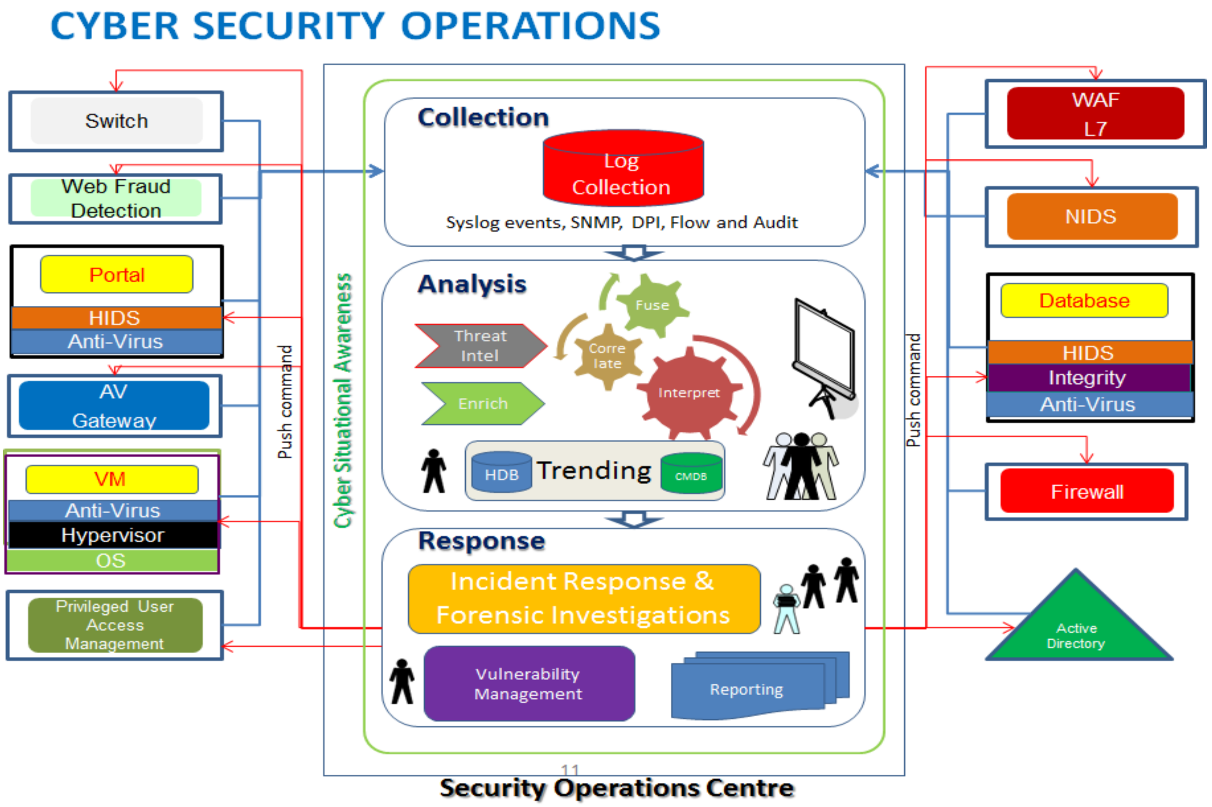


Figure 1: CSOC Framework

A. *Collection*

Log collection is an essential aspect of security monitoring (see Figure 2). Without events logs it will be challenging to detect when an asset is compromised, or when an attempt or intrusion is carried on the asset. So the first thing in monitoring is to configure systems in the IT asset and including handheld devices such as mobile and tablets to produce logs. The second most important is to setup a common and centralized clock, and ensure that all the assets take their timing information from the common clock source. This is absolutely important because if the timing information is not consistent, it will be challenging to detect if an event happened at the same time across the estate, and also, it will be harder to correlate if the same event, but from different log sources where related in time or happened at the same time. To ensure consistent network timing information is setup across the estate, network time protocol (NTP) (see IETF RFC5907 [6]) is recommended to be setup in the estate. NTP is used to synchronise the network timing information (clock synchronization) for ICT systems in the estate so that consistent and synchronized time information is distributed to all ICT systems for the organisation.

Log collection is the generic term used to describe the central repository, where logs generated from systems in the organisation, such as computer systems, infrastructure, subsystems and applications are stored. Logging happen on the local logging repository of a system or subsystem, which are then transported to the central logging repository for the CSOC to analyse.

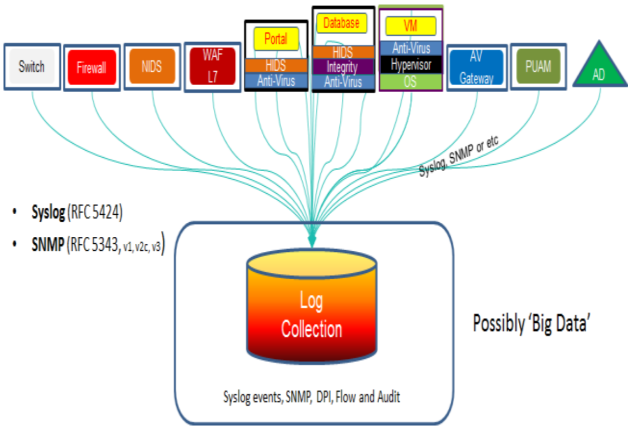


Figure 2: Centralized Log Collection

Logs can be collected through a number of mechanisms or protocols such as Syslog (IETF 5424), SNMP (IETF 5343), traffic flow (i.e. netflow), streaming data, such as Packet Capture (PCAP), DPI (Deep Packet Inspection) and Audit log (logs produced when system audit policy is enabled) as shown in Figure 2.

The quality of logs produced by the assets (log sources) will determine whether alerts or incidents will be detected or not. To ensure high quality logs are generated by the log sources, system audit policy must be defined and setup on the log sources. For instance, system audit policy should be setup on all log source, such as:

- ‘trigger an alert when a log file is deleted or an attempt to delete the file is executed or invoked’.
- ‘trigger an alert when an attempt to delete the /etc/passwd file or when an attempt to copy the /etc/passwd is executed’.
- ‘trigger an alert when a new account is setup on the server, or when an exist account is deleted or modified’
- ‘trigger an alert when the privilege/rights of an existing account is escalated to administrator or root level’

While all events are recorded and logged, however, events that trigger or generate an alertare are instantly prioritised for incident triage. Incident triage is a process to carryout further investigate/analysis on an event that generated alert in order to ascertain whether it is an incident or leads to an encident. Note that not all alerts lead to an incident. There are false incident (false positive), which occur for a number of reasons, but are not incident. A good CSOC ought to have very low false positives if the monitoring is tuned, trained and baselined appropriately.

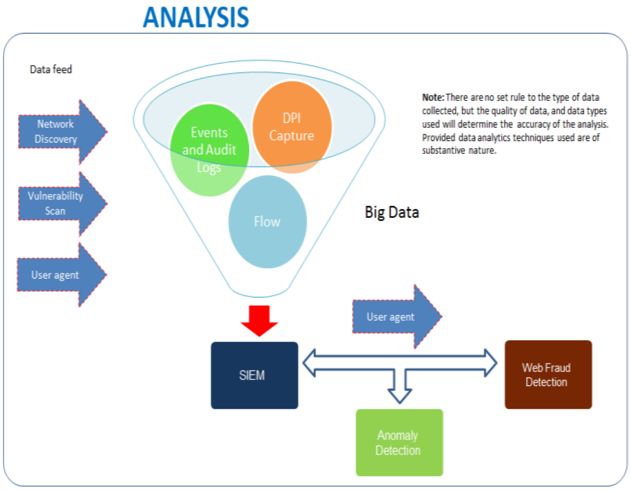
Similarly, logging levels should be setup proportionate to the risk level (risk appetite) and security sensitivity of the estate. For instance, if an organisation’s risk tolerance is low, and the sensitivity of the estate is high, then the logging level set using the Syslog protocol should be such that allows more log events to be collected, for instance setting a level to below ‘Warning’ level may be recommended (see Syslog RFC5424 [5] – Logging Levels).

Log collection should be realtime, or at least, near realtime. The reason for recommending log collection in realtime is to ensure analysis and response can be achieved as quickly as possible in order to minimise impact if it is a real attack by providing swift response or mitigation to the identified incident. To detect attack in realtime requires both log generation and log collection to be in realtime. Again, to stand any real chance of minimising the impact of cyber attacks, or security breaches, for example, data exfiltration, then the detection mechanisms including log collection should be in realtime, or at least in near realtime. Our expectation of realtime is in *miliseconds* of the log being generated or produced by the log source (i.e. firewall, IDS, server etc.) to when it is transported to the central repository for analysis. To achieve this, some of the underlying components such as the protocol and transport mechanism should be configured and setup to either push/pull logs in similar intervals (i.e. miliseconds or seconds).

B. Analysis

Analysis is the ‘brain’ behind the CSOC (see Figure 3). It is where the logs collected from various assets in the organisation are analysed.

Analysis can be achieved through a number of ways, for example through manual, semi-automated, fully-automated, and hybrid methods. *Manual analysis* is analysis performed by security analysts without the use of technology, it is non-automated tasks often carried out using improvised tools; for instance, using MS Excel to analyse event logs to sort or re-arrange IP addresses, or compute average occurrence of a particular aspect of the log statistics of interest. While manual analysis could be used for analysing events / log statistics for reporting purposes, is highly inadequate for performing enterprise IT events monitoring. This is because manual analysis lags in time (very slow); it is prone to human errors and limitations, takes longer time to compute very complex series of correlations of a number of varieties. Can you imagine analysing hundreds of millions of events per second or logs of over 1TB in volume using MS Excel? When will the analysis finish, and by what time will the attack be detected?



Note: There are no set rule to the type of data collected, but the quality of data, and data types used will determine the accuracy of the analysis. Provided data analytics techniques used are of substantive nature.

Figure 3: Analysis

Automated analysis is the use of technology to perform analysis comprising series of tasks automated to execute without human intervention. Semi-automated analysis is analysis combining both manual and automated computation. *Hybrid analysis* is fully automated analysis combined with human decision making (security analysts) in the loop. Hybrid analysis is the recommended and best analysis suitable for protective and continuous monitoring of the enterprise. *Automated log analysis* use technologies such as Security Information and Event Management (SIEM) systems, e.g. HP Arcsight, QRadar, NVision etc. to normalize, correlate and analyse data (structured and semi-structured data) swiftly, quickly and accurately in order to detect suspicious events and incidents. Other tools such as anomaly and web fraud detection systems are used to complement the tasks of SIEM systems. *Anomaly detection system* rely heuristic – machine learning algorithms to detect subtle, symptomatic and stealth events that are non-signature based. To gain better use of anomaly detection tools, it is advisable to ensure that the network is baselined, tuned and trained, so that deviations can be flagged, and also to minimize false positives. *Web fraud detection* systems are used to detect fraudulent transaction or cybercrime by profiling endpoints, analysing data streams, channels and behaviours. It identifies transactional risk associated to an online transaction by profiling the entity’s attributes, and behavioural pattern, and comparing those against historical baseline pattern of the entity.

Obviously, technology alone will not perform the analysis function adequately, conversely, humans alone neither will; hence trained and skilled security analysts are required to create use case scenarios, script queries, apply filters and automate actionable intelligence in order for the technology to be fully utilized efficiently (hybrid analysis).

To improve the results from the analysis, data enrichment will be required. For example, log data from configuration management database (CMDB), user agents, privileged user monitoring, network discovery and vulnerability scans data may be combined in order to detect anomalous, symptomatic, stealth and suspicious events.

Analysis of logs focusing on correlation must ensure that filters are setup and applied for the different use case scenarios such that alerts can be generated instantaneously when data stream containing suspicious payloads are detected in inflight traffic. Use case scenarios are identified either by the organisation, or the CSOC Supplier, in the case of an outsourced CSOC. It is pertinent that use case scenarios are created or derived based on the business requirements of the monitored organisation.

Log analysis should include trending of both inflight data stream and historical logs in order to observe patterns, trends, occurrences and situations that may have gone undetected previously, or that was previously not an issue but now have manifested as an incident. For instance, zero-day attacks that could have been previously exploit without anyone knowing these were even an issue at the time (no knowledge or awareness of the vulnerability until when it is out in the wild).

C. Monitoring

Monitoring should be performed by security analysts and operators who monitor the systems, networks, applications and services. Monitoring can be structured in a number of ways as directed by business requirements and organisation strategy. For example, some organisation refer to the people, process and technology monitoring infrastructure-related assets as the Network Operations Centre (NOC), while the group monitoring services and systems for attack and crime-related abuses are referred to as the SOC (Security Operations Centre). Whatever the operating nomenclature, both NOCs and SOCs operate a monitoring service. For instance, some CSOCs have security analysts and operators monitoring the service 24/7, others monitor the service 9/5 with on-call Level 2/3 support when a major incident occurs; while other CSOCs monitor the service 9/5 only. It is important to note that the CSOC operating structure should be driven by business needs and supported by the organisation's defense strategy.

Figure 4 shows security analysts monitoring the service, watching indicator when they change in set preferences. Monitoring related to 'eyes of glass' – describes security analysts and operators watching events on plasma screens or monitors for changes in set baseline, pre-configured filters, thresholds and indicators.

The task of monitoring (see Figure 4) is much more efficient when it is automated such that triggers or alerts are raised when an attack occurs so the security analysts can focus on observable and actionable indicators. This can be done through setting up baseline thresholds, alerting conditions, and triggers which 'fire' or are raised when there is a deviation from set baseline, conditions or parameters.

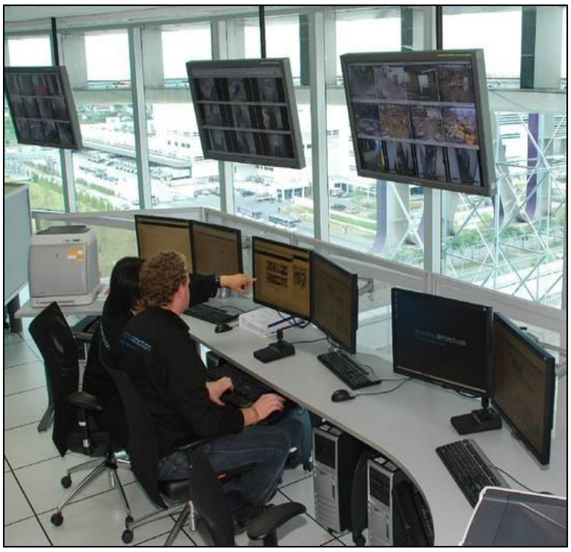


Figure 4: Security Monitoring ('Eyes on Glass')

Security monitoring encompasses both proactive and retrospective monitoring. With *proactive monitoring*, analysts are expected to create filters, queries and scripts which are setup using the SIEM technology and applied to log traffic to determine when an 'abnormal' condition occurs. *Retrospective monitoring* is the aspect of monitoring that focuses on analysing historical logs in order to determine or reveal if in the past there were situations symptomatic of attack, or known suspicious occurrence, which may have gone undetected. For instance, freshly identified vulnerability (zero-day) could be exploited without anyone noticing it until when it has widely publicised and patches made available to mitigate it. In such instances, security analysts are requested to analyse historical logs to reveal if that particular vulnerability was exploited, and if an attack or compromise may have gone unnoticed. Similarly, when a new malware signature becomes available security analysts are required to correlate this new piece of information against the historical logs in order to determine if the organisation had been previously breached.

D. Response

At present, it is no longer if an organisation will be attacked, or whether there will be a security breach, it is now a matter of when a security breach occurs, and of what magnitude.

Incident response is the underpinning of the cyber security operations centre responsibility. It is a people, policy, process and technology control to ensure incidents are swiftly contained, controlled and mitigated. This requires incident response processes to be well established, known and proven to work. It means readiness processes and plans must exist including incident response readiness and digital forensic readiness. The ability to minimize the impact of an incident allowing business to continue while incident is still on-going is incident management (see Figure 5).

The task of incident response starts when suspicious events that trigger alerts (an alert) is triaged and confirmed to be an incident worth investigating further. Following an incident triage, the details of the incident are provided for further investigation, such as:

- Traffic originating entity (source IP address of event or group of events),
- Entity name (hostname, fully qualified domain name),
- Traffic type (RDP, SSH, FTP, HTTP, HTTPS, TLS, SSL etc.),
- Protocol (TCP/UDP)
- Payload information,
- Suspected attack payload / attack vector (provided by the log source that raised the alert, e.g., known signature or heuristics),
- target asset (IP address of the target endpoint), and occasional the
- GeoIP location[1] information (this is geographic information associated to the origin of the source IP address used in the attack. E.g. IP address originating from a country/city)

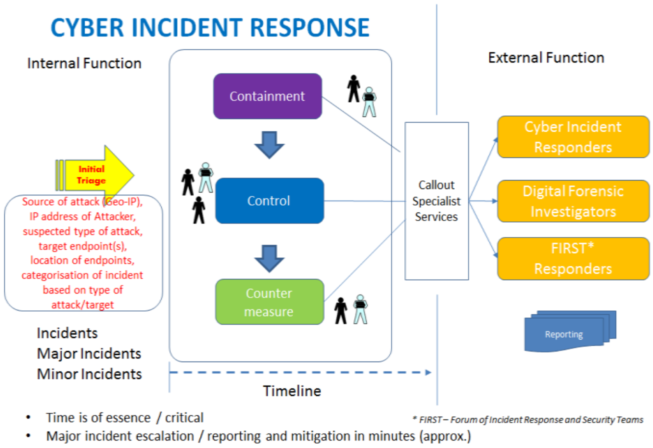

CYBER INCIDENT RESPONSE
Internal Function
External Function
Containment
Control
Counter measure
Initial Triage
Source of attack (Geo-IP), IP address of Attacker, suspected type of attack, target endpoint(s), location of endpoints, categorisation of incident based on type of attack/target
Incidents
Major Incidents
Minor Incidents
Timeline
Callout Specialist Services
Cyber Incident Responders
Digital Forensic Investigators
FIRST* Responders
Reporting
• Time is of essence / critical
• Major incident escalation / reporting and mitigation in minutes (approx.)
* FIRST – Forum of Incident Response and Security Teams

Figure 5: Incident Response & Management

Incident response and readiness plans should be tested on a regular basis, to ensure the plans are responsive, reflexive, and account for new personnel and technology [7].

While the CSOC may be equipped to deal with all types of cyber incidents, unfortunately, there will be cases where it may be challenging for the team to completely address, contain or/and mitigate the incident, either because they are under resourced (e.g. lack of skilled personnel, tooling and expertise). In this case, external specialist organisation may be required (callout specialist services) such as the Cyber Incident Responders, Digital Forensic Investigators or FIRST (Forum for Incident Response and Security Teams) as shown in Figure 5.

As the impact of cybercrimes continue to be costly [8, 9], in some cases unprecedented. Some businesses have actually closed down due to the consequential financial impact of a cyber-attack. Ironically, these are not SME companies, rather large enterprise. Of course, the impact of cyberattacks also has resulted to the loss of several CxOs jobs. For instance, Amy Pascal, co-chair of Sony Pictures Entertainment announced she will be stepping down after unprecedented cyberattack (hackers angry about a movie 'The Interview' she championed mocking North Korea's dictator exposed a raft of embarrassing emails between Pascal and other Hollywood figures) [10].

III. PEOPLE, PROCESSES AND TRAINING

People are the most vital aspect of a security operations centre; without people a CSOC responsibility will not be achieved through technology alone. Without people, the systems, network and applications will not be adequately monitored. The service could be tricked into a denial of service by itself. For instance, if every system in an organisation is automated, a well-crafted attack could scan the network biasing the network to sense that it is under attack, and hence shuts itself down, therefore causing a denial of service attack to itself.

In August 2014, Microsoft's Patch Tuesday server was infiltrated by a bogus software update which was downloaded by the millions of Microsoft-powered assets during a Patch Tuesday update [1], this action was noticed and remedied by security analysts. This also goes to show the importance of humans in the security recovery and remediation chain.

Unfortunately, it is hard to find the right people. At present, it is extremely challenging to hire or recruit people with the right skills and expertise. Cyber security skills gap is a known issue, and remains a top societal issues.

Therefore, to get the best out of the people an organisation already have, they need to be trained, skilled and equipped. There needs to be a well-thought out training and development plan in place for staff, and there also needs to be improvement and career progression plans in place. In summary:

- People are as important as Technology.
- Analysts & Operators must be well trained and skilled.
- Processes must exist, and should be followed, and policies must be adhered.
- Cyber operations require specialist skills, and continuous investments in – training, courses, certifications, memberships
- The best Cyber operations can only be achieved through people. 'Man in the loop'.
- People are always the weakness link.

A. *Reporting*

The CSOC service, like most services, will have agreed service level agreements (SLAs), key performance indicators

[1] GeoIP Location – Geographic IP location is the mapping or identify of the physical geographic location of an entity/endpoint using its IP address.

(KPIs) and measurement metrics in order to determine the return on investment, and also to assurance the business leads of the benefits.

There are a number of metrics senior management may be interested to know. Here is an example of the top five you might want to consider:

1. The number of incidents detected in a certain period, say in a month, six months or a year.
2. Performance of the cyber operations, such as the number of false positives, false negatives, true negatives and true positives. These figures are used to determine if the service is reliable, and hence should be trusted. For example, if the number of false positives continuously outnumbers the true positives, then the service has not been properly tuned or trained.
3. Rolling top five or ten cyber-attacks, by geography of origin, nation-state sponsored attacks, capability and severity.
4. Summary of internal policy violations, non-compliance and critical of exposures.
5. The number and summary of privileged user misuse and abuse.

Reports must be tailored for user groups. Senior management reports should be very 'high level' and lightweight, providing only synopsis of what should be of interest to them. However, technical reports for the administrators, security architects or SOC manager should include technical details that will help this community diagnose and prevent further occurrence and future re-occurrence. Here is an example of five of some of the parameters to consider for inclusion in technical reports:

1. Data and Time of attack (Note: the entire estate should have consistent and synchronized network time clock).
2. Date, Time and Log record reference.
3. Malware name, Application stream that detected it, and compromise path.
4. Risk score, Data stream, GeoIP location of the originating traffic of a fraudulent transaction.
5. Entity identifier, source traffic identifier, IP address, boundary device ID, Command invoked for the exploit.

IV. CSOC STRATEGY

A CSOC strategy is the overarching blueprint for the full lifecycle of the security operations centre service. It should drive, dictate and guide the CSOC service, including the capabilities established in the CSOC.

The CSOC strategy should be driven by the business requirements of the organisation, and should be organisation-focused and user-centered. Specifically, this means, the capability of a CSOC will vary from one organisation to the other; and in accordance to the organisation's business needs and requirements. For instance, if one organisation's business needs are driven by the ability to respond and defend nation-state sponsored attacks, then the capabilities they should have in their CSOC service will be certainly different to another organisation whose business requirements and needs are focused on mitigating internal privileged user misuse. For the same reasons, CSOC of organisations in same vertical tends to have similar capabilities. For instance, CSOC capabilities for the financial sector organisations, such as Banks tend to focus primarily on capabilities that enable them to mitigate online transactional crime, address financial compliance obligations and monitor accounts and entities.

While the capabilities of one CSOC may differ from the other, interestingly though, they all operate a 'common' central principle. The central underpinning principle is to prevent and detect threats, and respond to incidents swiftly. Based on this common principle, we present a CSOC strategy to achieve this common goal; further, we overlaid the HMG Good Practice Guide #13 (GPG13) - Protective Monitoring for HMG ICT Systems [12] PMC controls to the CSOC representation in order to validate its usefulness and appropriateness as shown in Figure 6.

GPG13 is the UK's HMG framework for security and protective monitoring of ICT systems and infrastructure, recommended for use or adherence of organisations, mainly public sector organisations. It is a popular framework within the UK public sector for the provision of guidance when setting up IT security related monitoring. It comprises 12 protective monitoring controls (PMCs), which are often reported against for coverage. These controls are mapped to our representation, which are shown in BLUE ovals; named 1-12 (see Figure 6).

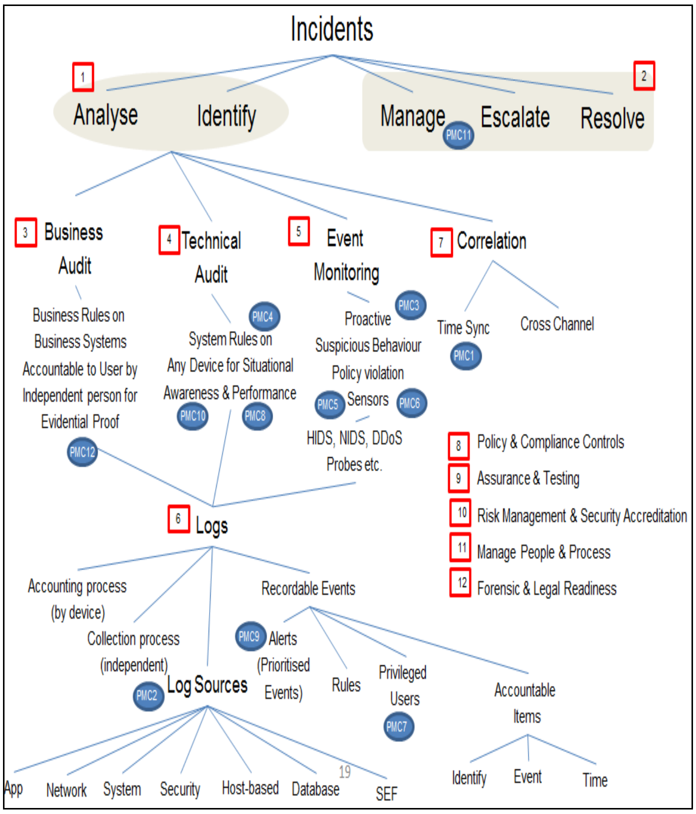


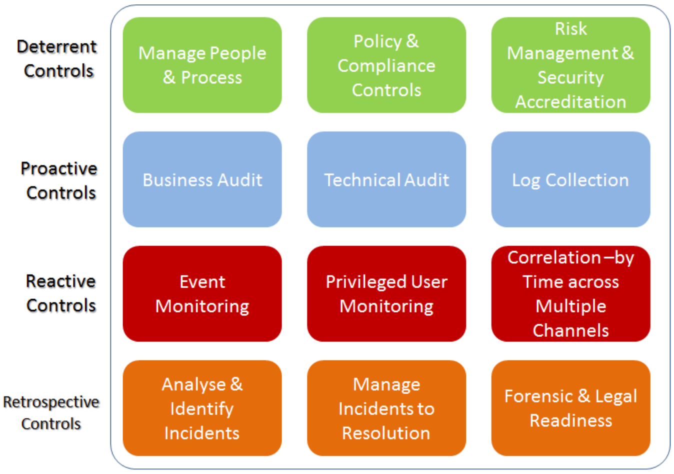
Figure 6: Mapping CSOC Strategy to HMG Protective Monitoring Controls

Our CSOC strategy shows (from bottom to top) the log sources (e.g. application network, system to SEFs[2]). The log sources produce logs, and these logs contain streams of events, most of which are recorded for analyse, forensic and investigation purposes. The events record contain accounting items, such as time the event was generated, which system produced it, and the event identify (*event_ID*). Logs are also produced when systems audit policies are setup on the log source (as described in Section IIA), these can be from business audits or technical audit policies. The centralized log (central log repository) is then analysed (Event Monitoring) using technology and powerful tooling, such as SIEM, Anomaly Detection or Web Fraud Detection in order that suspicious behaviour, fraudulent transaction, policy violations can be detected and reported. The analysis (correlation) can be carried out in a number of ways, such as by time (i.e. time that the event was detected, time when the incident occurred), or correlation by the channel (online/offline/both) that event was observed from, and by a combination of other parameters. The analysis is useful for identifying incidents, which must then be prioritized, contained, resolved and managed. As shown in Figure 6, each focal area of the CSOC strategy is associated to the GPG 13 PMC (shown in BLUE ovals), while the key objectives of the strategy is shown in RED square boxes.

It is evident that our CSOC strategy covers all the PMCs, identifies other key areas not represented in the good practice guide, and informs new and additional aspects to be investigated. Following the CSOC strategy, 12 key controls are identified and categorised as discussed below.

A. *CSOC Controls*

The key CSOC controls derived from the CSOC Strategy are represented in Figure 7, these are grouped into four primary control areas – deterrent, proactive, reactive and retrospective controls.



Deterrent Controls	Manage People & Process	Policy & Compliance Controls	Risk Management & Security Accreditation
Proactive Controls	Business Audit	Technical Audit	Log Collection
Reactive Controls	Event Monitoring	Privileged User Monitoring	Correlation –by Time across Multiple Channels
Retrospective Controls	Analyse & Identify Incidents	Manage Incidents to Resolution	Forensic & Legal Readiness

Figure 7: SOC Strategic Objectives

Deterrent controls are used to deter users (internal and external users) of the systems/service of intended misuse. The controls identified through our CSOC strategy are - *manage people and process, policy and compliance*, and *risk management security accreditation*. These controls are utilised by the CSOC to deter users and customers from misusing or abusing the service, or any parts of the platform. For instance, acceptable use policy, confidentiality agreements are policies that users' sign up to that deter them from misuse, as they know beforehand the consequences should they misuse or abuse the service. *People and processes* are managed, for instance, some users are mandated to gain a certain personnel security clearance (SC[3], DV[4]) before they can take on certain roles for the CSOC or the organisation. According to the UK's Government Security Classification Policy [14], principle 2: "Everyone who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training." *Risk management and accreditation* are additional personnel and system controls that are used to demonstrate that the accredited service adheres to a number of security operating procedures, policies, processes and uses technology to enforce baseline controls, which in themselves provide deterrent and preventative controls.

Proactive Controls are used to execute preventative measures to ensure instantaneous identification and detection of attacks, anomaly and policy violation and misuse. From the CSOC Strategy, the controls identified are – *Business Audit*, *Technical Audit* and *Log Collection*. These controls are enforced by the CSOC in order to detect attacks, and monitor the service. *Business audit* stipulate the dos and don'ts (rules) for all business applications. These rules are applied to business critical applications that the CSOC monitors. In the same vein, technical audit (that is, system audit policy) are implemented on all systems that the CSOC monitors, such that any deviation from these set policies and metrics are raised as an alert, which are in turn investigated by the analysts. For instance, business and technical audit rules are configured on firewalls, IDS etc. to prevent (*deny and log*) known threats. Similarly, baseline profiles and heuristics are setup on anomaly detection systems to trigger an alert when there is deviation to these profiles or when there is suspicious or symptomatic events. The logs generated by business audits, technical audits and events from the various log sources, such as probes, sensors and specific-purpose appliances are collectively transported to a central repository (*log collection*) for analysis.

Reactive Controls are used to provide analysis of indicators and situations observed through monitoring in order that incidents can be mitigated swiftly and accurately. The controls identified through the CSOC strategy are – *Event monitoring, privileged user monitoring*, and *Correlation by time across multiple channels*. Event monitoring, privileged

[2] SEFs – Security Enforcing Function – these are devices that perform security enforcement, such as firewalls, intrusion detection systems, Anti-Virus etc.

[3] SC – Security Check – is the 2nd tier of the UK Personnel Security Clearance. It allows the cleared/named individual regular and unsupervised/uncontrolled access to SECRET information/data.

[4] DV- Developed Vetting – is the 3rd tier of the UK Personnel Security Clearance. It allows the named /cleared individual access to and including TOP SECRET information/data.

user monitoring and correlation by time and across multiple channels are reactive controls that assist the CSOC to analyse and identify incidents when they occur. Event monitoring ensures that people, process and technology exist that the CSOC can use to analyse thousands of millions of events in order to identify suspicious events or streams of events in this myriads of events generated in seconds, and often in milliseconds. Privileged user monitoring ensures that controls exist to identify users who have misused or abused the service and in order to make them accountable for their actions. Correlation by time across multiple channels is an analysis technique to derive meaning and situations from a number of different channels in order to correlate events which ordinarily and on their own are innocuous but when fused and analysed collectively might be suspicious and symptomatic of an attack.

Retrospective Controls are used to follow-up in the aftermath of an incident in order to contain, control and counter the incident, and ensure the service continues to operate in the face of adversity. The controls identified using the CSOC strategy are – *Analyse and identify incidents*, *manage incidents to resolution*, and *forensic and legal readiness*.

V. Conclusion

The importance of CSOC over the year has heightened as cyber landscape has broadened. Cyberattacks can happen to any organisation; it is only a matter of time. Unfortunately, cyberattacks and cybercrimes can lead to substantive financial damages, and including branding, negative publicity and impact on shares and stocks prices. The other reasons for having a cyber security operations center are:

1. Volume: Most organisation possess myriad of devices in their IT estate, many of which are no longer managed, unsupported or legacy.
2. Information / Data: All organisations have valuable data that need to be protected such as Customer records, Student records, Citizens data, Bank/financial records, IP (Intellectual Property) etc.
3. Growth: There’s increasing growth in organisation user base, information and data. Networks are extended and expanded to accommodate collaboration, partnerships etc. Hence, isolated and localised point solutions struggle to protect the enterprise.
4. Point Solution Management: Localised and point solution devices (log sources) need to be monitored, and properly managed, too.
5. Borderless Perimeter: Collaboration, partnerships etc. and new ways of doing business (internet/eCommerce) means the boundary/perimeter is no longer ‘hard’ but ‘soft’.
6. Privileged User Abuse: Trusted users with privileged access can turn rogue, such risk must be monitored, mitigated and managed.

CSOCs are becoming the bedrock of organisations business controls to fend off cyberattacks, protect critical services and operations, and ensure on-going incidents are resolved swiftly and appropriately, helping for both containment, control and countermeasure so that the organisation continues to deliver services in the face of adversity. In summary:

1. CSOC is an essential business control to ensure safe and secure business operations and services, especially online digital services.
2. Business requirements should drive cyber security strategy, and CSOC capabilities and scope.
3. Continuous improvements, including lesson learned should be encouraged.
4. Cyber incident will happen, and every organisation should have proportionate incident response and management strategy, and incident readiness processes in place.
5. Forensic readiness should be considered important; hence organisations should consider having forensic readiness capability roadmap and maturity model.
6. People and process are the key, while technology is equally important, too.
7. Staff training and development, including career progressions plan should be considered essential.

VI. Future work

We plan to focus on the delivery model of the CSOC in our next publication. This will discuss the different ways, methods and models to deliver a CSOC – encompassing wholesome outsource, hybrid and wholesome insource.

References

[i] Dan Goodin, “SecurID Breach Cost RSA $66m, in 2nd Quarter Alone”, [Accessed] via http://www.theregister.co.uk/Tag/securid 20th February 2015

[ii] The New York Times, “JPMorgan Chase Hacking Affects 76 Million Households”, The New York Times, 2014. [Accessed] via http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_r=0 20th February 2015

[iii] The BBC, “The Interview: Sony’s North Korea film to be screened in US”, The British Broadcasting Corporation, 2014, [Accessed] via http://www.bbc.co.uk/news/entertainment-arts-30589472 20th February 2015.

[iv] The Register, “US CENTCOM Military in Twitter Hijack Shame”, 2015, [Accessed] via http://www.theregister.co.uk/2015/01/12/us_centcom_twitter_account_hacked/ 24th Feb 2015

[5] Syslog RFC5424, “The Syslog Protocol”, [Accessed] via https://tools.ietf.org/html/rfc5424 4th March 2015

[6] NTP – RFC5907, “Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4), [Accessed] via http://www.ietf.org/rfc/rfc5907.txt 4th March 2015

[7] NSA /CSS, “Defensive Best Practices for Destructive Malware”, Version 1.0, MIT-001R-2015, 16th January 2015

[8] Ponemon Institute, “2012 Cost of Cyber Crime Study: United States”, Benchmark Study of U.S. Companies, Ponemon Institute, October 2012, [Accessed] http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf via 6th March 2015

[9] ISF, “Threat Horizon 2016”, On the edge of trust, January 2014

[10] Reuters, “Pascal to step down as Sony Studio head after Hacking Upheaval”, February 2015, [Accessed] via http://www.reuters.com/article/2015/02/05/us-sony-pascal-idUSKBN0L92BG20150205 March 2015

[11] ZDnet, “What Went Wrong with Microsoft’s August updates”, August 2014, [Accessed] via http://www.zdnet.com/article/what-went-wrong-with-microsofts-august-updates/ March 2015

[12] HMG, “Protective Monitoring of HMG ICT System”, Good Practice Guide #13 (GPP13), Issue 1.0, October 2012

[13] R. Bidou, “Security Operation Centre Concepts & Implementation” [Accessed] via http://iv2-technologies.com/SOCConceptAndImplementation.pdf 7th March 2015

[14] UK Cabinet Office, “Government Security Classifications”, April 2014, Version 1.0 – October 2013, [Accessed] via https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf, March 2015.