CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process

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

Abstract – A cybersecurity operations centre ontology for analysis (CoCoa) is proposed, which aligns to the NIST cybersecurity framework. CoCoa is a process ontology for the CSOC analysis processes that provides the cybersecurity analysts operational situational awareness of the vital aspects of the CSOC. The process ontology offers a fundamental shift from log collection to the analysis of five overarching threat intelligence and information sources (namely – *events and logs, network information, structured digital feed, semi and un-structured feed* and *threat intelligence*), which should allow the CSOC to provide proactive monitoring, detection of inflight, emerging and complex threats that would not have ordinarily been detected through only *events and logs*. Further, and most importantly, the proposed ontology is then used to identify how cyber incidents can be realised and detected through ontology-based knowledge graph.

Keywords— *Cyber Security Operations Centre; CSOC; SOC; Cyber Incident; Playbook; Ontology, Knowledge Graph; CoCoa*

I. Introduction

Cybercrime and cyberattacks are real, and will not go away! Even the 'best' protected services and businesses can be attacked and exploited. Vulnerabilities exist in every asset and organisation, but it is only when exploited or used as a conduit to breach critical services that it makes headlines. Technologies are continuously evolving both in capability and complexity, while cyber landscape is increasing both in connectivity and accessibility, for instance LANs, MANs, WANs, Internet, Cloud Computing, IoT and IoET, which in turn increases the threat and attack surface. The situation is further compounded, unfortunately though, by the fact that even when critical security vulnerabilities are discovered on critical systems, they are not patched for a long periods of time, which could be down to a number of reasons, for example, a) the patch process may take considerable time to implement in some organisations, b) operational systems may not be patched due to downtime issues. Often security patches will demand a system reboot or shutdown which are often challenging to be negotiated or be agreed, especially for business critical systems, c) change requests and change management may be lengthy and protracted, and d) the likelihood of service charges or penalties if the system or service is under a contractual obligation of a Service Provider management. Thus, as you can see the overall picture is bleak.

The recently announced vulnerability – 'Meltdown' and 'Spectre' on reputable and known CPU brands, such as Intel, AMD [1,2] demonstrates that vulnerability can be uncovered in most assets, and therefore, the best approach to cybersecurity is to augment preventive controls with detection, response and recovery controls. This is because protective and preventative controls will fail at some point, and some have already failed, e.g. TLS exploit [3,4] and SSL POODLE attack and 'Heartbleed' [5,6], therefore the best approach is a layered defence in depth, combining protection, detection, response and recovery. This is the crux of the NIST's Framework for Improving Critical Infrastructure Cybersecurity, popularly known as NIST's Cyber Security Framework [7], which identifies five core controls that allow a measured approach to defence in depth in cybersecurity.

In our previous contribution [8], we argued that, to adequately protect an organisation's critical services, networks, systems and infrastructure an approach is to augment the protection afforded by the protective and preventative controls with continuous and protective monitoring of the organisation's assets (e.g. ICT and applications, and including the protective and preventative controls themselves), which is provided through a Cyber Security Operations Centre (CSOC). This is so that should a security breach occur, or should the protective controls fail to stop an exploit or an attack, the incident can still be detected, while incident response and recovery plans are invoked to mitigate the security breach.

In this paper, we propose CoCoa – an ontology-based CSOC analysis process, and knowledge-graph ontology based on the application of CoCoa, which was used to map relationships to aid understanding of how cyber incidents may be detected or realised on the monitored environment. CoCoa maps the CSOC vital aspects of the cyber analysis process and their relationships. The processes considered in CoCoa include *source*, *sense*, *detect*, *respond* and *recover*, which aligns to the NIST's CSF.

The remainder of the paper is organised as follows: Section II discusses concepts used in this paper, and related work. Section III describes the proposed CoCoa analysis process ontology, while in Section IV ontology-based knowledge graph of Cyber Incident is discussed, and finally, the paper is concluded, and including future work, in section V.

II. Concepts and Related Work

A: Concepts

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 [9]. In this paper, we adopt the definition of

a SOC provided in [8] 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** to *deter* computer misuse and policy violation, and *detect* cyber-attacks, security breaches, and abuse, and *respond* and recover from cyber incidents. The terms SOC and CSOC are used to denote the same meaning in this paper.

A *playbook* is defined by the Cambridge dictionary [10] as "*a set of rules or suggestions that are considered to be suitable for a particular activity, industry or job."* In this paper, we define, and use the definition for a playbook (either for incident response playbook, or recovery playbook) as a *set of predefined and agreed actions, steps* and *responses* to be carried out by identified stakeholders in a timely manner to successfully manage (contain, counter and recover) an incident from the moment it is detect through to resolution and recovery.

Sources – these are threat intelligence and network information outlays that allow intelligence gathering and event collations from myriad points, internally and externally, of an organisation. *Log Source* – is any device, asset, ICT system, endpoint, network infrastructure, application and its subsystem that is configured to generate (or produce) transactional logs or events, which are usually stored within the asset's logging faculty, buffer, file or directory. *Security Enforcing Function* (SEF) – these are a category of assets that perform security enforcement and protection of the network or hosts, such as Firewalls, Intrusion Detection/Prevention Systems, Anti-Virus Systems, etc. These types of systems belong to the protective and preventative controls category. *Flow* – is defined as a set of IP packets passing an *observation point* in the network during a certain time interval. An *observation point* is a location in the network where IP packets can be observed, e.g. a line to which a probe is attached, a shared medium such as an Ethernet-based LAN, a single port of a router, or a set of interfaces (physical or logical) of a router [RFC 3917]. Flow provides information about a communication, e.g. the port, directionality of the communication, how long that communication has been active, and with these information, flows can be useful in detecting policy violation and breaches. For instance, if a communication is initiated from a server to an endpoint, a flow will reveal this, and if the policy is that all communications must be from the endpoint to the server, then this behaviour can be flagged up as a breach to security policy. Flows can be deployed in several ways such as *sflow, netflow* and *jflow* etc. *Session* – is the control-plane communication between a sender and a receiver that explore the 3-way TCP handshake. For instance, a session is established when a TCP 3-way handshake is negotiated and the receiver accepts to communicate to the sender. Session information allows vital communications parameters to be derived and profiled, such as how long has that communication being ongoing? What information is contained in the payload?

Threat Intelligence – is the capability to observe, track and gather relevant and actionable information and intelligence a.k.a. indicator of compromise (IOC) from multiple sources about threats, such as IP Address of the threat source, domain, email address, exploit targeted by the specific threat, vulnerability being exploited, techniques being used, and threat group or organisation involved, and the target of the potential exploit in order that the threat can be detected, which in turn allows time for the exploit to be mitigated.

Log collection is the generic term used to describe the central repository, (a.k.a. collector, logger etc) where systems event logs and applications transactional logs generated from ICT systems across the stack e.g. infrastructure, network, middleware, application and databases are stored [8].

Analysis – is defined as "the studying of the nature of something or of determining its essential features and their relations [11]". This definition resonates to the CSOC analysis process, which is a process ontology that determines the essential features and their relationships of the CSOC activities, ranging from intelligence gathering from pertinent sources through to the detection of incidents, resolution and recovery.

B: Related Work

Cybersecurity operations centres remain a vital aspect of any robust cyber programme, because CSOC performs core functions of cybersecurity monitoring, including detection, response and recovery. According NIST CSF [7], *identify*, *protect*, *detect*, *respond* and *recover* are the five core functions that are required for any organisational cyber programme regime.

Cybersecurity ontologies exist in the literature. Many of the contributions focus on ontologies for cybersecurity definitions, cybersecurity issues, and cybersecurity specific aspects, such as the ontology for malware analysis lexicon [12], intrusion detection systems [13], ontology for threat intelligence, e.g. STIX [14], TAXII [15], CybOX [16], ontology for vulnerabilities [17], ontology for malware, e.g. MAEC [18], and cybersecurity incident classifications [19]. Most recently, we recognise a broad effort by Syed et al. [20] to unified cybersecurity ontology, called Unified Cybersecurity Ontology (UCO).

These contributions are fundamental because they form the building blocks for cybersecurity ontology; unfortunately none of these contributions is for the CSOC analysis process. To the best of our knowledge, there do not exist any specific CSOC ontology mapping specifically CSOC analysis processes. So the contribution in this paper is original, and one we hope, not only provides insights into the analysis process of a CSOC, but also, necessitates further ontological research into the CSOC domain.

III. CSOC Analysis Process Ontology

In this section we introduce the ontology-based analysis process of the CSOC; we start from the overarching end to end process as shown in Figure 1 to the detailed ontology shown in Figure 4.

A: CSOC Analysis Process

CSOC operations in a nutshell are as shown in Figure 1.

The focus of the CSOC operations should be centred on proactive, protective and continuous security monitoring. This is the ability to gather, collect and collate, in realtime, actionable intelligence so that threats and cyber-attacks can be detected, and in turn appropriate response and recovery plans put in place to contain, counter and mitigate cyber incidents, and recover from any consequential impacts of a data breach, as follows:

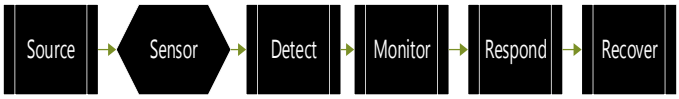

Figure 1: Basic and Foundational CSOC Analysis Process

a) *source* provides threat intelligence and information as discussed in Section B below. The operations process allows sources of threat intelligence to be received, consumed and processed. The sources can be both internal and external, for example, internal log sources may generate logs, events and alerts, while external sources may provide actionable intelligence feeds containing indicators of compromise (IOC). b) *Sensor* allows the threat intelligence and information provided by the sources to be collated and analysed to detect IOCs and suspicious behaviours symptomatic of an attack. The sensor receives and processes the information and threat intelligence from the sources, and this processing initially may include a couple of pre-processing such as normalisation and ingestion of logs, events, network information, IOC and other metrics. c) *Detect* is the process and mechanisms through which an attack is detected, and d) *monitor* is the operational monitoring, e.g. dashboard. Monitoring is performed in realtime (at worst near realtime), and in the event of an alert or alarm being triggered, or in a worst case scenario, an incident. e) *Respond* involves appropriate executable mitigation plans, actions, processes and procedures as documented in the incident response playbook that allows incident response to be invoked, and including stakeholder engagement. f) *Recover* encompasses the measures put in place to contain and continue in the event of a breach. *Recover* ensures service continuity and survivability, and this includes the playbook that outlines containment and continuity measures such as disaster recovery, forensics etc. as discussed in the recently published NIST guide for cybersecurity event recovery, SP800-184 [21].

This entire process is expanded and discussed in detail in subsequent sections throughout this paper.

B: Threat Intelligence Gathering, Log and Network Information Collection

With threat intelligence gathering, log and network information collection, we identified five types of sources (see Figure 2) that should be received and analysed for CSOC.

The sources are classified as follows: **type 1** – *events and logs*, **type 2** – *network information*, **type 3** – *structured digital feed*, **type 4** – *semi-structured and un-structured feed*, and finally, **type 5** – *threat intelligence*, see Figure 2.

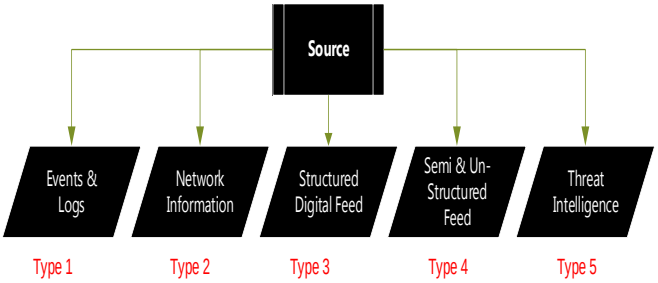

Figure 2: Source Classification and Categorisation

It is pertinent to note that our classification of sources offers a comprehensive and thorough ontology for, first identifying sources, and second, for understanding what actionable information are received from that source, and finally and most fundamentally, it distinguishes the capability the CSOC can offer by being able to consume information and intelligence from these sources. To the best of our knowledge, our model is the first to organize an ontology-based classification of sources of information and intelligence for CSOC analysis.

Our source classification and categorisation model (see Figure 2) can be used as a benchmark to assess the technical maturity model of a CSOC operations technological capability of the analysis process. For example, CSOC technology that is able to ingest, receive and consume all the five types of sources will be best able to detect an inflight threat than one that is able to receive and analyse only *events and logs* (i.e. source type 1).

As shown in Figure 3, threat intelligence and information sources for the CSOC comprises:

- *Events and logs*, which can be of the types e.g., raw log, Syslog (IETF 5424), windows event (Win event), alerts and alarms, which are prioritised event logs, and audit log (logs produced when system audit policy is enabled).
- *Network information*, which can be of the types e.g. SNMP (IETF 5343), traffic flow (i.e. netflow), session information, heartbeat and traps.
- *Structured Digital Feed*, which can be of the types e.g. streaming data, such as Packet Capture (PCAP), Configuration and Management Database (CMDB), which is used to map assets in the environment, National Vulnerability Database (NVD), which is used to assess vulnerabilities related to the assets, scans, which is a prioritised scan against vulnerability and severity, etc. It is pertinent to note that the structured digital feed must to be electronically and automatically integrated for analysis, and this is the only way it can be useful for the realtime detection of threat. Again, it is because of the underlying automation behind the ingestion of the structured feed that it is called ‘digital’ to imply the need for integration, automation and realtime ingestion.

- *Semi and un-structured feed*, which can be of the types e.g. trace, manual input such as unstructured data of physical access controls e.g, ID card reader and audit trails, and wetware (a.k.a. human communications logs), for example, intelligence received via email, phone and photographs etc.
- *Threat intelligence*, which can be of the types e.g. IOC, and as we have seen previously, IOC contains intelligence about the IP address of the threat, the threat source, threat infrastructure and where they are hosted, cryptographic hashes of the threat, vulnerability the threat are to exploit and domain names and emails used by the threat.

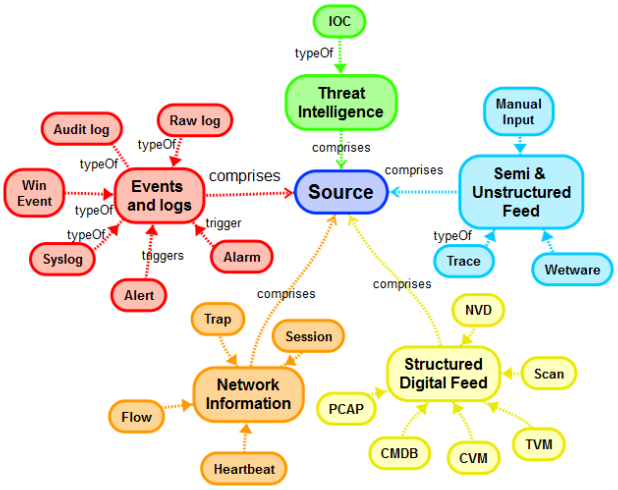

Figure 3: Source Categorisation Ontology

It is relevant to note that ICT events and logs collection has been regarded for years as the singular most important aspect of security monitoring [22]. Unfortunately, events and logs, at best, is a reactive provision that offers very little with regards to detecting inflight, emerging and sophisticated cyber-attacks, and at worse, satisfies only a compliance requirement. We argue for the augmentation of events log collection with network information and threat intelligence obtained from a variety of sources as shown in Figure 3, which allows the CSOC to receive intelligence in real-time, and immediately observe information on the fly and to detect embedded in-line threats that can only be detected via other sources, e.g. flow and session data. For example, flow and session data provide information and intelligence about behaviors that cannot be immediately deduced from events and logs, and similarly, IOCs allow for the identification of threats that could not ordinarily have been detected through events and logs. We call for a re-think in the approach to threat intelligence gathering and log collection. Log collection only is totally inadequately in detecting emerging and sophisticated cyber-attacks. Further, without gathering information and threat intelligence from the right sources, it will be challenging to detect in-flight threats, intrusion attempts, or freshly identified threats. A CSOC relying solely on analysis of event logs will certainly be behind the curves in threat detection, which ultimately limits the effectiveness of that CSOC.

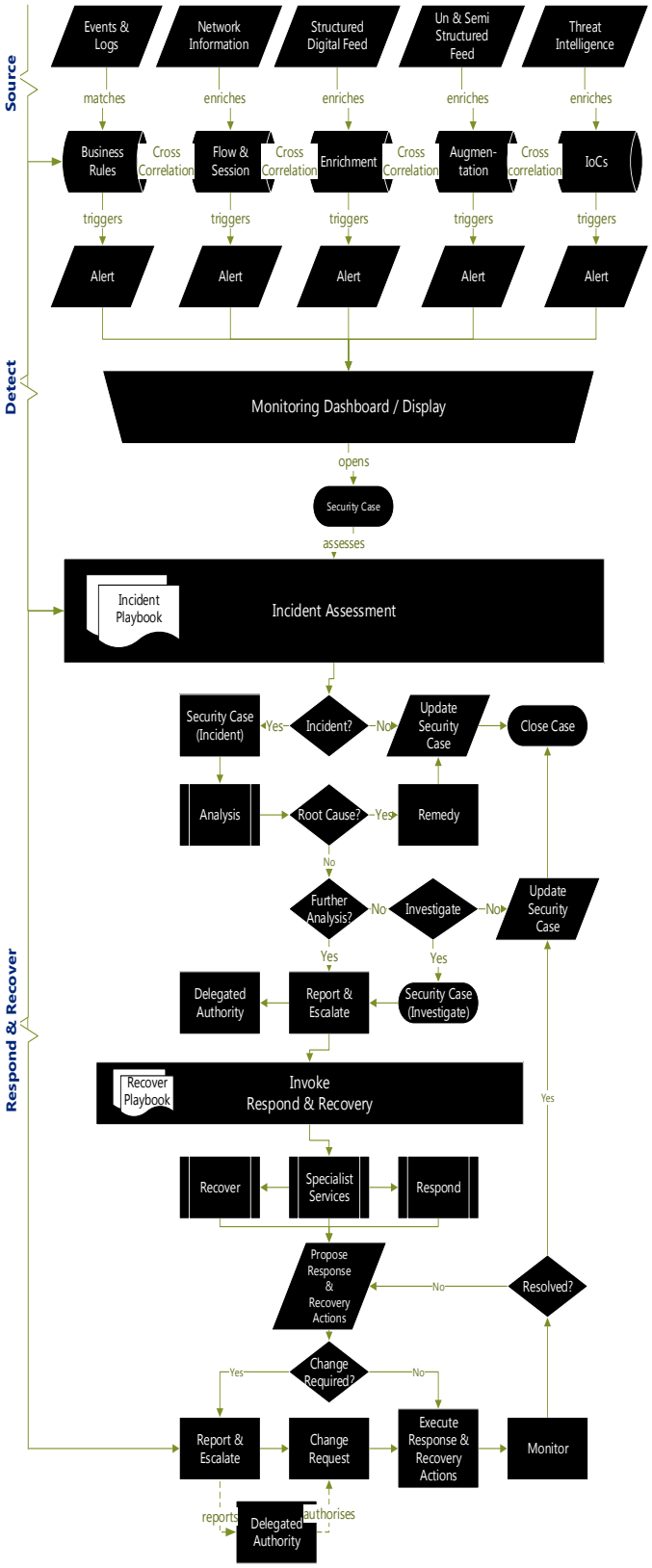

Figure 4: CoCoa – CSOC Ontology for Analysis

Figure 4 shows the proposed CSOC Analysis Process Ontology (a.k.a. CoCoa). It is organised in four main tiers, namely – source, detect, respond and recover. Source has been discussed in the sections above, while detect, respond and recover are discussed in the subsequent sections.

C: Detect

Threat detection starts, for the CSOC, firstly, in having the capability to gather threat intelligence and information from the five source types (*events & logs, network information, structured digital feed, Semi and Un-structured feed and threat intelligence*).

Intelligence (e.g. events, logs, IOCs, data and network information) gathered from the sources will be matched against pre-defined business rules to detect known threats; while some sources will provide enrichment, others will provide augmentation to already known or existing intelligence, and collectively, offer enhanced and richer intelligence picture (situational awareness) to detect and identify unknown and freshly identified threats.

For example, *events and logs* may contain, say IP address of the threat (e.g. the source that originated the traffic), but this piece of information on itself may be good enough to trigger a predefined rule, in the case where a known IP is blacklisted, but in other cases, may not be enough to conclusively identify an incident. In this situation, flow information will be used to enrich the intelligence, for example, if it is observed that the same IP address is still contacting assets in the organisation. The trust in the observation may be further enhanced when threat intelligence feed that provide IOCs, which may contain IP address, domain name, file hashes, hostname etc., these intelligence are then used to correlate against the monitored environment to detect any realisation of the threat in the monitored environment. For instance, to identify if any of the endpoints are communicating (beaconing) a Bot, or may have been 'taken-over' by a Botnet, infected, or otherwise.

To gain better situational awareness of the monitored environment, cross correlation of the threat intelligence and information sources occur, and through this, enhanced situational awareness is gained, and symptomatic manifestation of threats may be identified and detected, which could not have been detected through analysing a single source type.

An alert is raised when an incident is detected. Alerts (a.k.a. alarms, in the case of audible alerts) will be immediately observed on the monitoring dashboard, which allows the cyber security analyst to follow up, open an incident ticket, and following agreed and predefined incident playbook to invoke an incident investigation as shown in Figure 4.

Operational monitoring (a.k.a. 'eyes on glass') is the monitoring carried out by the CSOC, where security analysts (usually, Security Analysts Tier 1) in particular, continuously monitor the screens, dashboards, and displays (see Figure 4) in order to identify and assess when an alert is raised by the sensors or technical controls put in place to detect and identify security breach, policy violation or compromise. The CSOC security analysts (usually Security Analysts Tier 2) provide level 2 supports to the Tier 1, and carry out complex and specialist investigation and security triage, including proactive and retrospective tasks such as trending, that is, analysis of historically logs and intelligence in order to identify trends, understand patterns, and to make future predictions of the evolution of threats, and patterns of occurrence of future attacks. Security Analysts Tier 3 will normally carry out threat hunting and perform incident responder functions, and including mentoring of Tier 1 & 2 analysts. They may provide training to Tier 1 & 2 analysts on key aspects of the SOC operations, and also help to develop CSOC operations and monitoring contents and artefacts.

D: Respond

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* will a security breach occur, and of *what* magnitude? [8], and this realisation has changed where emphasis and efforts should be refocused with the overall organisational cyber programme.

As shown in Figure 4, incident response is triggered by the incident playbook during the initial incident assessment (a.k.a. incident triage). This incident assessment process is to determine if the event is a false positive or a true negative, and if it a false positive, then the security case (incident) is updated and closed, and this will lead to lessons learned, and serve for continuous security improvement exercise.

However, if the event is a true negative, then part of the assessment is not only to determine severity, impact, attack surface, and consequential impact, but also, to assess how the incident can be controlled, contained, and countered. Incident response is triggered as documented in the incident playbook, and each process is dependent on the type of play, the severity of the incident and the impact. For example, if the incident is a high severity incident (say a *Priority 1* incident requiring immediate action due to consequential impacts and losses), then the response time will be different, and the immediacy will be different, too, and hence the incident response plan as documented in the playbook will dictate.

Analysis and investigations will need to be conducted to determine root cause (RCA), and ensure appropriate countermeasures are put in place to contain and mitigate the attack.

Further analyses are required if a root cause could not be substantiated or established through the initial assessment, and specialist investigation may be enlisted as approved by the organisation (a.k.a. authority or its delegate); and throughout this process, the security case is updated accordingly (as shown in Figure 4).

E: Recover

Recovery is the underpinning of cyber resilience. There is absolutely little benefit in responding to cyber-attack if the organisation is not prepared for recovery, because the same vulnerability could be exploited again, if not mitigated, to attack the organisation, and the circle continues. Accordingly to NIST guidance to cybersecurity event recovery [21],

organisations must be fully prepared to recover from significant cyber events[1] that impact their core business operations and services and their ability to support their mission.

As shown in Figure 4, recovery is as documented in the recovery playbook, which includes but not limited to the organisation approach to recovery, stakeholders who will be involved, approach to communications, planning, and agreeing and understanding of recovery objectives, interdependencies among resources and tooling.

Recovery may be not fully achieved by the organisation itself, which could be due to a number of factors such as resource capacity, skills capability, etc., hence the need to establish prior engagements and protocols becomes absolutely important, such as the need to procure call-out service of specialist incident responders, and through their assistance appropriate recovery can be achieved.

It is relevant to note that recover plan must take concerted effort to determine, assess and agreement on SLA, OLA, business impact assessment, and dependency maps [21]. Prior recovery planning should include simulations, and testing of the agreed processes and procedures to determine if they work, and whether improvements are needed when a real incident occurs. As shown in Figure 4, it is equally useful that organisations understand their change request and change management protocols to be invoked during a major incident as following a 'normal incident management process' will certainly be inappropriate, and may delay recovery, and put the recovery plans into peril.

Cyber incident may dictate that emergency changes are carried out in order to recover quickly and swiftly from a cyber attack, and such changes do not have to follow the normal change management process, but carried out through a prior agreed, expedited and quicker change process (a.k.a. emergency change process). Certainly, every major cyber incident must follow the expedited emergency change process.

The emergency change process must be agreed prior, and documented, and including the named individuals who must be involved and their deputies to signoff the change in the event of a major cyber incident.

[1] Cyber event in the NIST guide (NIS SP 800-184) is used interchangeably with cyber incident, and means one and the same thing.

IV. Ontology-based Knowledge Graph of Cyber Incident

An ontology-based knowledge graph has been used to map the interrelationships and interconnections to understand how cyber incidents can be detected or/and may be realized on a monitored asset, as shown in Figure 5. All the entities are displayed and connected by arrow lines that show their relationships. The knowledge-graph is laid in hierarchy, and shows the connections from each layer (hierarchy) to the other. Among the layers are:

- the *detection logic* (e.g. business rules, contextual information, audit policy, profile and anomaly). This layer focuses on detecting the incident, and they do so, by triggering an alert, alarm, inform a situation by offering contextual information, or evidence symptomatic of an attack.
- the *sources* (e.g. PCAP, logs and events, trap, alert, flow, session and IOC). This layer offers the rich set of evidence, which when analysed matches some pre-defined set of rules, which then triggers an alert. They may enrich existing evidence, which then helps in detecting correct the nature and impact of the attack, or may inform a policy violation.
- the *controls* (e.g. Tap, Scanner, Probe, SEF, Sensor, PAM[2], Web Analytics and threat intel). This layer focuses on offering preventative and proactive safeguards that automatically stops the attack or detects its presence. For example, a firewall may stop an attack by blocking the port, and may also generate a log of the action, which then will be analysed later in other to understand better the situation, especially when combined with other intelligence sources.

There are five main entities below the three layers: collector, vulnerability, network infrastructure, threat and asset and config DB (as shown in Figure 5).

A *Collector* stores scan outputs, and also has the ability to query external database, e.g. vulnerability databases (CVE[3] and NVD[4]) in order to identify the associated vulnerabilities in relation to the scan report. *Network infrastructure* connects to the monitored estate/environment, and consists of Apps, hosts, databases, services, networks and middleware, and the collections of these, the data they hold and their configurations are held in the asset and config database (asset & configuration DB). *Threat* associates to malware, as an example, and relates to a geography, which is deduced via the geographic IP database (GeoIP, e.g. Maxmind[5]) in order to map threat source, and threat will exploit vulnerabilities that may exist in the monitored environments, e.g. Apps, hosts etc.

[2] PAM – Privilege Access Management
[3] CVE – Common Vulnerabilities and Exposures - https://cve.mitre.org/
[4] NVD – National Vulnerability Database - https://nvd.nist.gov/
[5] Maxmind - https://www.maxmind.com/en/home

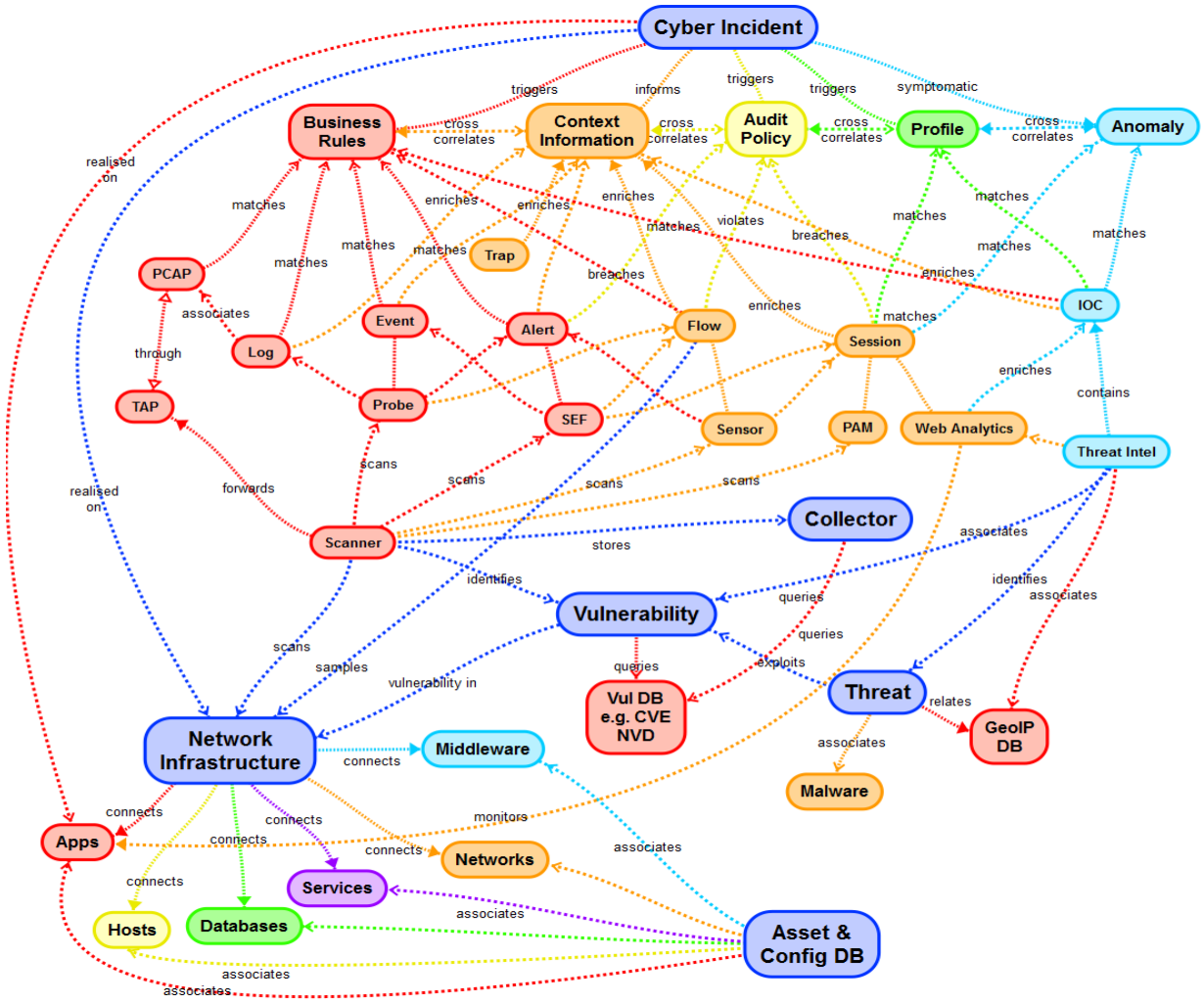

Figure 5: CSOC - Cyber Incident Ontology-based Knowledge Graph

A: Use Case Study

Here, we demonstrate how the ontology-based knowledge graph may be used to detect a cyber incident.

Take for example, threat intel as shown in Figure 5.

a) *Threat intel* contains IOC, and the IOC associates to a GeoIP, which identifies the threat and its geographic location.
b) The *Threat* may be associated to a particular *vulnerability*, and the vulnerability may exists in the monitored *network infrastructure*, e.g. Apps, hosts, services, middleware or networks.
c) Using the IOC an *anomaly* may be identified, which offers some symptomatic evidence of a *cyber incident*. The IOC may match a predefined *profile*, and may offer *contextual information* enrichment.
d) While each aspects provide some vagueness to the detection of an incident, but then when the *contextual information* is cross correlated with *profile* and *anomaly*, then suddenly a clearer picture of the cyber incident appears to emerge, and situational awareness of the incident is gained.
e) Further, where the incident may be realised will be known because the associated vulnerability is mapped to the asset it may exist in within the network infrastructure space, and that the threat targets to exploit.

V. Conclusion

The importance of the CSOC cannot be overemphasised, especially considering their vital importance in cyberspace, more so, on the evidential premise that cyber incident and cyberattacks are unavoidable, and therefore a rethink of the current cyber protection efforts are required, and the adoption

of a defense in depth and measured approach to cybersecurity of identify, protect, detect, respond and recover.

With the CSOC performing the three core aspects of detect, respond and recover. The CSOC function becomes even more critical as highlighted by the US NASA [23] of the lack of a coordinated operational technical agency approach to prevention, detection, response and recovery, and this applies to most of organisations.

The fundamental contributions of this paper, amongst others are:

a) The identification, classification and categorisation of the five source types for threat intelligence and information collection and collation for the CSOC. As we have suggested in the text, this aspect can be used as one of the core criteria for assessing the technological maturity model of any SOC function or capability.

b) The proposed comprehensive analysis process of the CSOC (a.k.a. CoCoa), which not only captures a SOC analysis process, but also, provides a repeatable and consistent framework that can be reused to rollout a CSOC function for an organisation, and finally,

c) The ontology-based knowledge graph of cyber incident, which allows the CSOC analysts to gain better situational awareness of the monitored assets, the threats that may target them, the vulnerabilities they might exploit, and the compromise path and attack surface.

Future work

We plan to make CoCoa publicly available online at C-MRiC.ORG and on GitHub to encourage reuse, collaboration and knowledge sharing.

References

[1] NIST National Vulnerability Database (NVD), https://nvd.nist.gov/vuln/detail/CVE-2017-5754

[2] Meltdown and Spectre Vulnerability - https://meltdownattack.com/

[3] Homeland Security (2017), "Daily Open Source Infrastructure Report", 05 January 2017, [Accessed 23rd Jan 2018] https://www.dhs.gov/sites/default/files/publications/dhs-daily-report-2017-01-05.pdf

[4] US-CERT (2017), "Transport Layer Security (TLS) Vulnerability", Vulnerability Note VU #144389. CERT/CC, December 13, 2017, [Accessed 23rd Jan 2018] https://www.us-cert.gov/ncas/current-activity/2017/12/13/Transport-Layer-Security-TLS-Vulnerability

[5] US-CERT (2016), "Alert (TA14-290A) SSL 3.0 Protocol Vulnerability and POODLE Attack", September 30, 2016, [Accessed 23rd Jan 2018] https://www.us-cert.gov/ncas/alerts/TA14-290A

[6] US-CERT (2014), "Heartbleed OpenSSL Vulnerability", 10 April 2014, [Accessed 23rd Jan 2018] https://www.us-cert.gov/sites/default/files/publications/Heartbleed%20OpenSSL%20Vulnerability_0.pdf

[7] NIST (2014), "Framework for Improving Critical Infrastructure Cybersecurity", version 1.0, February 12, 2014, accessed on https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[8] C. Onwubiko (2015): "Cyber Security Operations Centre: Security Monitoring for protecting Business and supporting Cyber Defense Strategy", Proceedings of the IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015), joint and co-located with Cyber Science 2015 conferences, London, UK, June 8-9, 2015.

[9] R. Bidou (2000), "Security Operation Centre Concepts & Implementation" [Accessed] via http://iv2-technologies.com/SOCConceptAndImplementation.pdf 7th March 2015

[10] Cambridge Dictionary, "Playbook" - https://dictionary.cambridge.org/dictionary/english/playbook

[11] Dictionary.com, "Analysis" - http://www.dictionary.com/browse/analysis

[12] D. A. Mundie and D. M. Mclntire (2013), The MAL: A Malware Analysis Lexicon, Technical Note: CMU/SEI-2013-TN-010, CERT Program, SEI https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_40250.pdf

[13] F. Abdoli and M. Kahani (2009), "Ontology-based Distributed Intrusion Detection System", 14th IEEE International CSI Computer Conference, 2009

[14] STIX – Structured Threat Information eXpression, https://oasis-open.github.io/cti-documentation/ (Accessed 16th Jan 2018)

[15] TAXII – Trusted Automated eXchange of Indicator Information, https://taxiiproject.github.io/ (Accessed 16th Jan 2018)

[16] CybOX - Cyber Observable eXpression, https://cyboxproject.github.io/ (Accessed 16th Jan 2018)

[17] H. Booth and C. Turner (2016), "Vulnerability Description Ontology (VDO)", Draft NISTIR 8138, September 2016, - https://csrc.nist.gov/csrc/media/publications/nistir/8138/draft/documents/nistir_8138_draft.pdf (Accessed 16th Jan 2018)

[18] MAEC – Malware Attribute Enumeration and Characterization, https://maecproject.github.io/ (Accessed 16th Jan 2018)

[19] S. A. Elnagdy, M. Qiu and K. Gai (2016), "Cyber Incident Classifications Using Ontology-Based Knowledge Representation for Cybersecuirty Insurance in Financial Industry", 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing, DOI 10.1109/CSCloud.2016.45

[20] Z. Syed, A. Padia, T. Finin, L. Mathews and A. Joshi (2016), "UCO: A Unified Cybersecurity Ontology", AAAI Workshop on Artificial Intelligence for Cyber Security, February 2016

[21] M. Bartock, J. Cichonski, M. Souppaya, M. Smith, G. Witte and K. Scarfone (2016), "Guide for Cybersecurity Event Recovery", NIST Special Publication 800-184, December 2016.

[22] K. Kent and M. Souppaya (2006), "Guide to Computer Security Log Management" SP 800-92, National Institute of Standards and Technology (NIST), September 2006

[23] J. Wang (2010) "Anatomy of a Security Operations Center", GFirst 2010, NASA, [Accessed 31st Jan. 2018] https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110011188.pdf