SMART NETWORK AND SECURITY OPERATIONS CENTRE

TAN Shyh Hae, LEE Kok Thong, SEOW Nyi Matthew, TAN Choon How

ABSTRACT

This article shares the rationale and benefits of combining the conventional Network Operations Centre (NOC) and Security Operations Centre (SOC) into an integrated Network and Security Operations Centre (NSOC). By re-engineering operational processes and augmenting them with technologies such as end-to-end IT visualisation and analytics, NSOC provides IT managers and operators with end-to-end situational awareness and a streamlined incident management process.

With NSOC, IT incidents can now be managed more holistically and efficiently and this helps in reducing service recovery lead time and minimising additional head count while increasing the operational availability of IT systems.

Keywords: NOC, SOC, NSOC, Network and Security Operations Centre, Converge

INTRODUCTION

The Singapore Armed Forces (SAF) operations of today are becoming more complex due to increasing network-centric operations, operations-other-than war and cyber threats. There is a need to enhance the monitoring of IT systems performed by the SAF's existing Network Operations Centre (NOC) and Security Operations Centre (SOC) as well as streamline the incident management process so that IT incidents can be quickly detected and efficiently managed. This would enable services to be restored promptly and increase IT system resiliency.

BACKGROUND OF NOC AND SOC

NOC and SOC are synonymous with the smooth and secure running of today's IT landscape. They are critical IT nerve centres of public and private enterprises throughout the world. Historically, NOCs and SOCs functioned as separate entities fulfilling different missions.

NOCs play a pivotal role in infrastructure availability and are often measured by uptime Service Level Agreements (SLA). NOC operators utilise a range of management tools to actively monitor and manage the performance and status of various IT infrastructure equipment such as routers and switches, with increasing expansion of scope to include servers, storage and data centre facilities. Through the use of these tools, NOC operators are able to perform fault management and coordination of service recovery efforts.

On the other hand, the emergence of increasingly advanced cyber threats has created a new dimension of challenge that goes beyond the capabilities of NOC management tools. SOCs were hence established with specialised tools to provide capabilities such as security information and event management as well as malware analysis that enables cybersecurity analysts to focus on the deep investigative and forensic work required to accurately detect and respond to cybersecurity incidents.

Working in tandem, NOCs and SOCs ensure the availability and integrity of IT systems, functioning similar to a human's central nervous and immune systems that detect and respond to infections.

SYNERGIES BETWEEN NOC AND SOC

As IT infrastructures grow in size and complexity to meet users' increasing operational needs, NOCs and SOCs will need to work closely together to provide a holistic infrastructure and security view of the IT system. This will enable better sensemaking and situational awareness which will allow the NOC and SOC to remain effective in addressing monitoring and service recovery challenges amid infrastructure growth and complexity.

Fusion of Situational Views across NOC and SOC

A NOC will need to be enhanced with manager-of-managers[1] (MoM) capabilities to fuse together information from the various NOC and SOC tools and provide a holistic infrastructure and security view. This view will provide the operator with timely situational awareness on the interdependencies between various infrastructures and security equipment and facilitate more accurate impact analysis and service recovery prioritisation. For example, the MoM can automatically pinpoint the potential root cause of an infrastructure outage to an open door that caused the room temperature to rise and equipment to overheat, instead of the traditional approach of overwhelming the operator with separate door sensor, temperature and device failure alarms. In a heavily virtualised cloud environment, the MoM can also automatically determine the potential root cause of slow application processing instead of the traditional display of numerous independent performance counters for the operator to self-correlate.

Addressing Overlapping Infrastructure Faults and Cyber Threats

The line between infrastructure faults and cyber threats is becoming increasingly blurred as more powerful and deceptive cyber attacks tend to autonomously jump between different infrastructure equipment in order to cover their tracks and launch their attacks. For example, the infamous Stuxnet computer worm entered a closed network via a USB infection and exploited the Siemens Step-7 programmable logic controller software application to cause the Iranian centrifuges to overspin and become damaged and unserviceable. To be able to more effectively detect such threats, one possibility is to have NOC and SOC collaborate, cross-correlate and potentially identify the common patterns from their respective tools instead of the traditional approach of looking at infrastructure faults and security events in silo. These anomalous patterns can then be further investigated by specialists to diagnose and pinpoint the nature of the infrastructure incidents more accurately.

Enriching Security Insights

Information gathered by the NOC will be able to enrich the SOC investigative and forensics work. With an end-to-end monitoring system cross-referencing infrastructure faults and behaviour anomaly with cyber incidents as well as trending and insights from analytic tools, operators will better understand the extent of the cyber threat being analysed. They can also determine the indicators or signatures to look out for and easily correlate seemingly unrelated events. This can help to provide greater insights into low signature security events which may normally be ignored by cybersecurity analysts focusing on higher volume and higher signature events.

CONVERGENCE OF NETWORK AND SECURITY OPERATIONS CENTRES

NOCs and SOCs generally have similar operational structures with both using tiered monitoring and incident response teams. Junior operators usually form Tier 1 and are responsible for work orders, system monitoring, call handling, preliminary investigation and triage of detected and reported events. Events that are unable to be triaged are escalated to senior Tier 2 specialists for more detailed review and resolution. Tier 3 subject matter experts serve as the final escalation point for the most complex of issues.

In addition, there are commonalities in NOC and SOC infrastructures and operations. NOCs and SOCs both require analyst workstations, call routing and management systems and facilities, service level agreements, standard operating procedures, workflow and trouble ticketing.

To enable NOCs and SOCs to work closely together for better sensemaking and situational awareness as well as remain effective in addressing next-generation infrastructure monitoring and service recovery challenges, an innovative approach is to combine the conventionally separate and independent NOC and SOC into a common Network and Security Operations Centre (NSOC). This is achieved by consolidating operations and re-engineering processes. This integrated approach is also currently being explored by companies such as American Systems, General Dynamics, HP and IBM.

Moreover, this approach helps to save on valuable data centre real estate and corresponding power and cooling facilities as NOC and SOC components require significant resources to run. It also helps to minimise the monitoring load placed on the infrastructure equipment as one common information aggregator can collect all the data required and then share it with NOC and SOC tools instead of each operations centre collecting data separately. In addition, a common NSOC will have the integrated processes and structures in place to allow NOC and SOC operators to communicate and coordinate seamlessly as well as tap each other's skillsets and experiences to identify, manage and resolve incidents effectively.

Technology as a Key Enabler for NSOC

Traditional Network Management Systems (NMS) have difficulties performing the role of a MoM as the majority of them do not have out-of-the-box equipment adapters to correctly interpret information from the different brands and models of infrastructure equipment in use, along with their corresponding management tools. Those that have the equipment adapters are handicapped by the need to manually create rules to map out the interdependencies between components which creates sustainability and scalability issues.

However, the reference architecture behind NSOC is now achievable with the advancement of enterprise network management technologies.

Standardisation and Compatibility

With the maturing of network system management technology, many infrastructure equipment today are leveraging common standards such as SNMP[2], SYSLOG[3], REST[4], JSON[5] and XML[6] to communicate with the management tools. This standardisation enables the enterprise NMS to easily communicate with the disparate infrastructure and security management tools to understand the information being presented. For legacy systems that are still using proprietary communication methods, enterprise NMS now comes with a number of predefined equipment adapters and this makes it easy to reach out to these legacy systems without needing to self-customise.

Data, Cybersecurity and Infrastructure Analytics

Traditionally, a major challenge in enabling end-to-end situational awareness is the inability to map out the relationship between various infrastructure equipment and their performance statistics and trends. The typical approach is to manually define relationship rules to link the various equipment together as well as manually inspect and correlate statistics. This approach is laborious, prone to human error and unsustainable.

Analytics capabilities found in today's enterprise NMS are able to form the overall infrastructure topology and dependencies automatically from information obtained from the various infrastructure equipment to provide the operator with a real-time automated end-to-end holistic view of infrastructure performance statistics and trends.

For example, in a virtualised cloud environment, the enterprise NMS is able to automatically show on which physical host a virtual machine is running, as well as the underlying network and storage connections, without needing manual human intervention. This topology awareness simplifies the need to perform manual rules creation and maintenance significantly while providing the operator with a real-time and up-to-date, end-to-end topology view that facilitates situational awareness. This capability enables the operator to pinpoint the various bottlenecks in the infrastructure quickly and make the necessary adjustments, potentially before actual degradation occurs. To investigate the cause of slow application processing, the operator will no longer need to manually look at the current and historical performance statistics for all the supporting infrastructure equipment and attempt to correlate and identify a pattern. This holistic topology view also enables automated end-to-end root cause analysis that speeds up the identification of the actual cause of a fault.

At the same time, by analysing the network inventory and configuration data, the NSOC will be able to automatically alert the operator on potential security vulnerabilities in the infrastructure and locate components that are not compliant with organisational security profiles.

Data and Software Integration

These new capabilities form the bedrock of an NSOC's operation by fusing together the various NOC and SOC tools and providing the NSOC operator with a holistic end-to-end view of the interdependencies between the various infrastructure equipment as well as security incidents. This timely situational awareness facilitates greater and faster accuracy in service impact analysis. This is important in assessing the actual health and performance of the application and corresponding service recovery prioritisation.

The integration of technology also maximises cost effectiveness in building and maintaining the underlying management infrastructure as well as pave the way for refining incidents and problem management processes.

Processes

The establishment of an integrated NSOC facilitates the ease of information sharing and enables close collaboration between the previously separate NOC and SOC teams.

Streamlining and Automation

Disparate processes can now be streamlined and better automated. For example, instead of manning two separate incident response hotlines with two different teams performing their own work, one single hotline that handles both NOC and SOC incidents can be created as illustrated in Figure 1. The hotline operator can perform first level diagnosis using the integrated NSOC tools to identify if there is an infrastructure fault or cyber incident and route the incident to the respective service recovery teams. If the cause of the incident is not straightforward, it can be escalated to second level NOC and SOC specialists to perform more in-depth investigation. Commonly occurring incidents can also be automatically identified and routed to the service recovery teams without the need for operator involvement.

Centralising Case Management

All the incidents are tracked via a common case management system that automatically monitors the progress status and flags out cases for escalation if service recovery will breach the established service level agreement. The case management system also reconciles the incident resolutions into a common knowledge base that operators can refer to when incidents of similar natures occur, hence further improving triage accuracy and reducing service recovery lead time.

Design for Support

The integration, streamlining and automation enabled by NSOC makes it easier for operators to perform their jobs and focus on incident management and service recovery tasks as less system training and maintenance is required.

People

The availability and sustainability of suitably trained operators is an increasing concern in today's manpower landscape as the skilled engineering pool is decreasing over the years. This is an issue that needs to be systematically addressed.

Beyond the technological enhancements, process streamlining and automation in NSOC, opportunities are created to optimise manpower headcount and at the same time make operators feel more engaged with higher value tasks.

For example, NOC operators are experienced in servers, desktop and network support and will have good troubleshooting skills and TCP/IP protocol suite knowledge. The same set of skills are also necessary for SOC tasks. Hence, instead of engaging two persons to perform overlapping tasks, better synergy can be achieved by cross training the staff such that he or she can perform first level tasks for both the NOC and SOC. In this way, it gives a more holistic meaning to the staff's job while at the same time allowing for the creation of a leaner team.

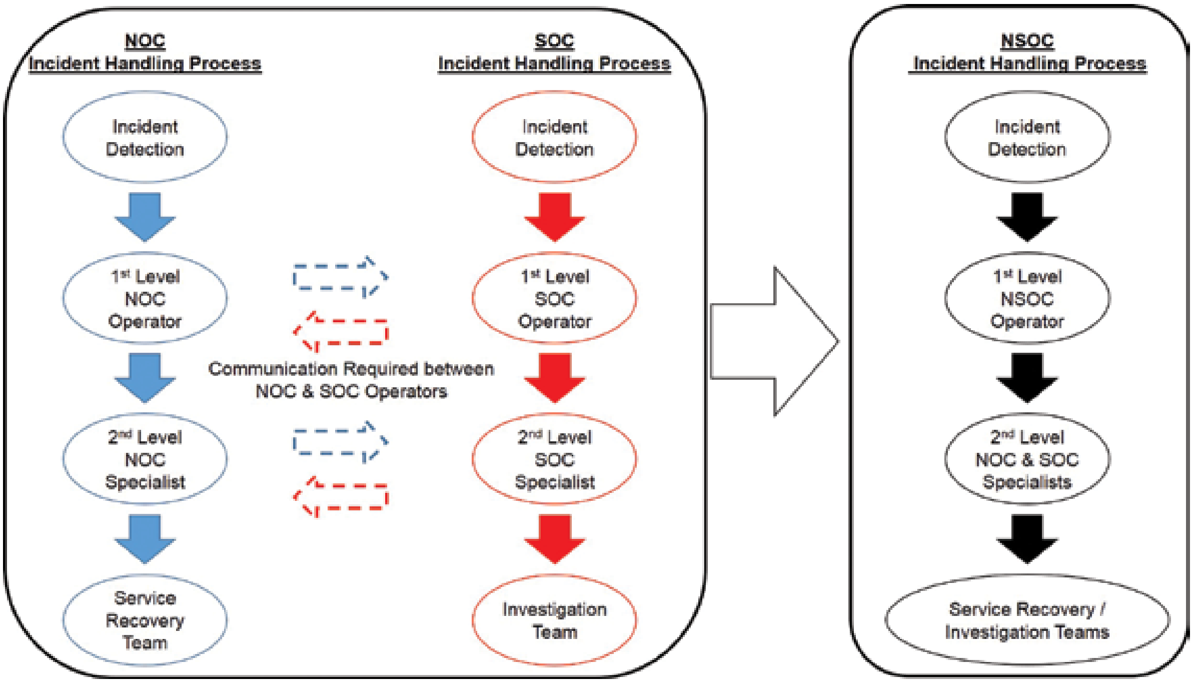

Figure 1. Streamlining of incident management processes

REFERENCE AND SYSTEM ARCHITECTURE FOR NSOC

The reference and system architectures for NSOC consist of three layers (see Figure 2 and 3).

Data Source Layer

This comprises the infrastructure equipment in use. Raw instrumentation data such as performance counters, health status and logs are used by the respective NMS in the System Management Layer for individual monitoring and management purposes. These data are also piped into the Service Management Layer via the Logs and Events Consolidator for further processing.

System Management Layer

NMS performing the FCAPS[7] monitoring and management for the IT infrastructure are grouped under this layer. Alarms, events and statistics from these systems are fed into the Service Management Layer via the Logs and Events Consolidator for further processing.

Service Management Layer

The capabilities in this layer form the 'brain' of the NSOC. It provides the holistic situational picture and decision support functions for NSOC managers and operators to assess the operational impact of the IT infrastructure incident and perform the required recovery actions. The Logs and Events Consolidator aggregates and indexes information from the System Management and Data Source Layers into a centralised data warehouse for the various Service Management Layer tools to perform searching, analysing and reporting tasks.

Performing Service Impact Analysis

The Service Management Layer reconciles related historical and current events from various infrastructure equipment to identify and advise the NSOC operator on the potential root causes of the IT infrastructure incident, the equipment involved and the sequence of events and activities leading to the incident. It also assesses the actual impact of the incident on the IT infrastructure availability by factoring in infrastructure redundancy and criticality parameters. Furthermore, it provides the NSOC operator with recommendations on the corresponding service recovery prioritisation.

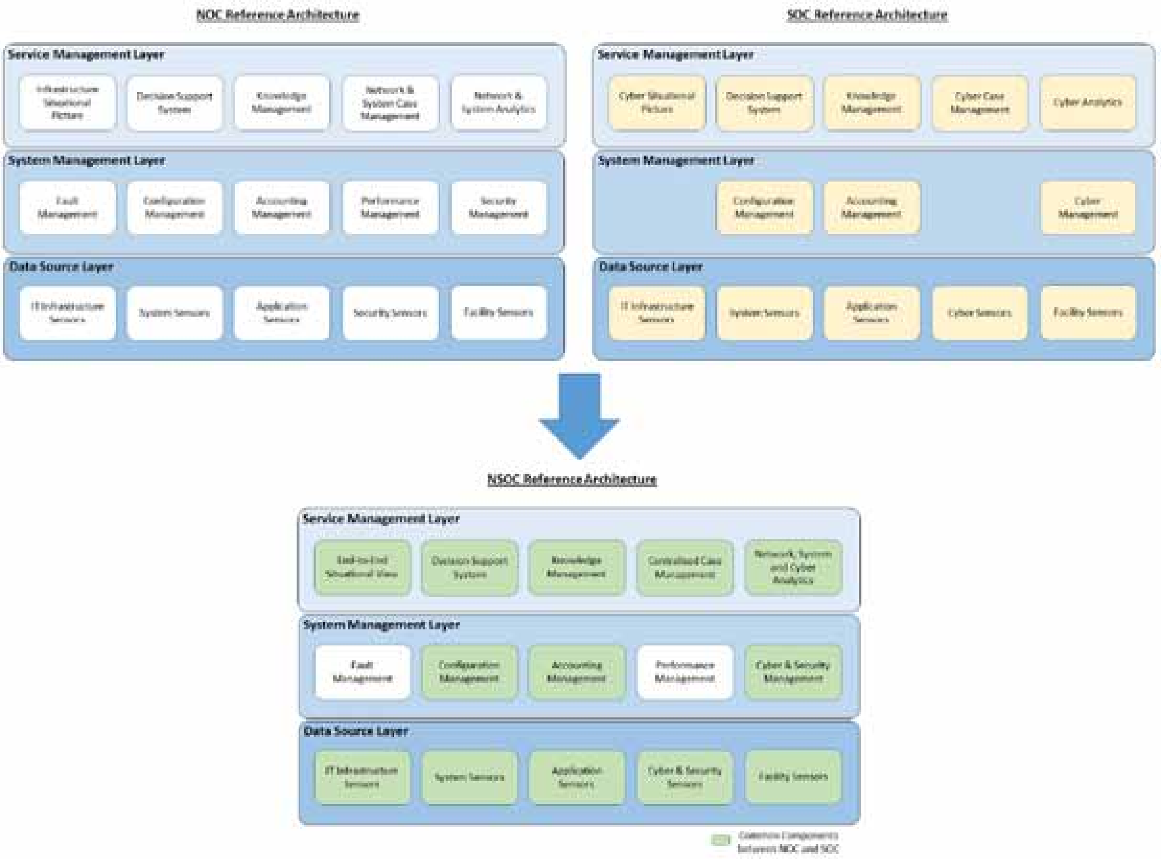

Figure 2. NSOC reference architecture

Detecting Infrastructure Anomalies and Forecasting Capacity Growth

By performing analytics on historical performance trends, the Service Management Layer flags out infrastructure behaviour deviations for further investigation into potential cybersecurity threats or infrastructure faults. This information is further extrapolated to estimate infrastructure growth requirements and prompts the NSOC manager to make necessary adjustments before degradation occurs.

Assessing Infrastructure Vulnerability and Compliance

The Service Management Layer assists the NSOC operators in auditing and ensuring alignment with organisation policies as well as identifying potential security issues and bugs. This is done by performing active network scanning of the infrastructure equipment to determine if it is exposing known vulnerabilities and automatically analysing infrastructure inventory and configuration information as well as if vulnerable software components are installed.

Facilitating Incident and Problem Management

A case management system is provided within the Service Management Layer to centrally track all IT infrastructure incidents. This system comes with workflow automation, SLA monitoring and knowledge management functions that enable NSOC managers and operators to perform swifter and more informed decision making while reducing human error. At the same time, it identifies regularly recurring incidents and prompts the NSOC operator for further investigation and escalation so that the actual root cause can be identified, hence increasing future system availability.

CHALLENGES

The consolidation of conventionally separate and independent NOC and SOC into a common NSOC enables incidents to be addressed more holistically and efficiently to increase system resiliency and maintain operational effectiveness. However, there are three inherent challenges that need to be addressed in order for NSOC to materialise.

Foremost on the list are ownership and skillset issues. Typically, NOCs and SOCs each have their own system owners. When merged, there is a need to iron out issues such as who will be the owner and final decision maker for the NSOC. For example, a NOC operator may interpret a device outage event as an indicator of equipment failure while a SOC analyst may interpret that same event as a compromised equipment indicator. At the same time, beyond the fundamental infrastructure and system technical skills, SOC skillsets are investigative in nature while NOC skillsets are more focused on troubleshooting and recovery. The NOC and SOC staff will need to cross train and adjust their mind sets and mental models. They will also need to expand their range of skills more rapidly and react faster to the increased number of technologies involved.

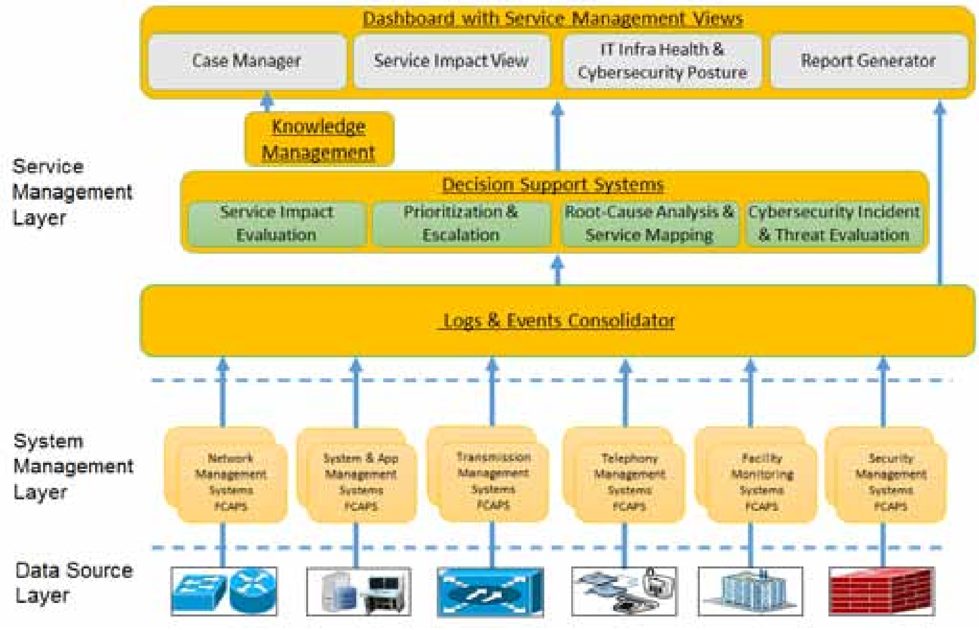
Dashboard with Service Management Views
Case Manager
Service Impact View
IT Infra Health & Cybersecurity Posture
Report Generator
Knowledge Management
Service Management Layer
Decision Support Systems
Service Impact Evaluation
Prioritization & Escalation
Root-Cause Analysis & Service Mapping
Cybersecurity Incident & Threat Evaluation
Logs & Events Consolidator
System Management Layer
Network Management Systems FCAPS
System & App Management Systems FCAPS
Transmission Management Systems FCAPS
Telephony Management Systems FCAPS
Facility Monitoring Systems FCAPS
Security Management Systems FCAPS
Data Source Layer

Figure 3. NSOC system architecture

Next would be the need to balance between NOC and SOC operations. The NOC's objective is to perform service recovery and enhance resiliency rapidly while the SOC's objective is to investigate and create countermeasures. This tension between a NOC needing faster recovery and SOC activities resulting in slower recovery will make it difficult for the NSOC operators to make a sound judgement on which approach to take in the event of an unknown incident.

Lastly, when the NOC and SOC components are built around each other in an integrated NSOC, the components become intrinsically intertwined. As the NSOC system scales with more components, the compatibility and interoperability dead weight increases and may affect overall system performance as well as the ability to rapidly add new components to address emerging concerns.

CONCLUSION

While differences exist between NOCs and SOCs, the convergence of both centres can be both practical and beneficial, combining the awareness and control of an enterprise's nervous system (i.e. the NOC) with the defence and response of its immune system (i.e. the SOC).

Efficiency gains can be realised through the introduction of a single and integrated point-of-contact for all IT infrastructure and security events. Service levels and system resiliency can also benefit through improved communication and increased situational awareness. Incident response time is reduced as a unified operations centre owns both the capability and responsibility for enacting mitigating measures.

REFERENCES

Babu Veerappa Srinivas. (2014). *Security operations centre (SOC) in a utility organization*. Retrieved from http://www.giac.org/paper/gslc/8336/security-operations-centre-soc-utility-organization/138736

Ennis, S. (2009). *A phased approach for building a next-generation network operations center: A planning guide*. Retrieved from http://www.eirteic.com/wp-content/uploads/2013/11/whitepapers_phased-approach-for-building-a-next-generation-network-operations-center.pdf

EY. (2013). *Security operations centers against cybercrime: Top 10 considerations for success*. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY_Security_Operations_Centers_against_cybercrime/$FILE/EY-SOC-Oct-2013.pdf

Goodchild, J. (2009, November). *Network and security operations convergence*. Retrieved from http://www.networkworld.com/article/2237963/compliance/network-and-security-operations-convergence.html

Imbert, C. (2015). *Knitting SOCs: Designing and developing the staff of a security operations center*. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/knitting-socs-35975

Jenkins, D. (n.d.). *Secure your operations through NOC/SOC integration*. [Powerpoint slides]. Retrieved from http://uk.idc.com/downloads/events/sec06_jenkins.pdf

JSON. (n.d.). In *Wikipedia*. Retrieved July 23, 2015, from https://en.wikipedia.org/wiki/JSON

Meierdirk, A. (2012). *Best practices for developing and implementing the right monitoring framework: Next-generation network operations center*. [Powerpoint slides]. Retrieved from http://www.remotemagazine.com/conferences/wp-content/uploads/2012/09/INOC.pdf

Metzler, J. (2008). *The next generation network operations center: How the focus on application delivery is redefining the NOC*. Retrieved from http://www.webtorials.com/main/resource/papers/NetQoS/paper13/NextGenerationNOC.pdf

REST. (n.d.). In *Wikipedia*. Retrieved July 23, 2015, from https://en.wikipedia.org/wiki/Representational_state_transfer

Simple network management protocol. (n.d.). In *Wikipedia*. Retrieved July 23, 2015, from https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Syslog. (n.d.). In *Wikipedia*. Retrieved July 23, 2015, from https://en.wikipedia.org/wiki/Syslog

Walker, M. (2009). *Manager of managers architectures: Providing enterprise situational awareness to the user*. [Powerpoint slides]. Retrieved from http://sunset.usc.edu/GSAW/gsaw2009/s5/walker.pdf

XML. (n.d.). In *Wikipedia*. Retrieved July 23, 2015, from https://en.wikipedia.org/wiki/XML

ENDNOTES

[1] The user interface provides a single, integrated view of the system and network, thereby allowing management of existing and distributed network managers from one interface.

[2] Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks.

[3] SYSLOG is a widely used standard for message logging.

[4] Representational State Transfer (REST) is the software architectural style of the World Wide Web.

[5] JavaScript Object Notation (JSON) is an open standard format that uses human-readable text to transmit data objects consisting of attribute–value pairs.

[6] Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable.

[7] FCAPS is the ISO Telecommunications Management Network model and framework for network management. FCAPS is an acronym for the fault, configuration, accounting, performance and security management categories into which the ISO model defines network management tasks.

BIOGRAPHY

TAN Shyh Hae is a Manager (InfoComm Infrastructure) working on the requirements development and architecting of the next-generation Network and Security Operations Centre (NSOC) concept for the Ministry of Defence (MINDEF) and the Singapore Armed Forces (SAF). He also led project teams that pioneered the implementation of mobile messaging and secure removable storage solutions for MINDEF and the SAF. Under the DSTA Undergraduate Scholarship, Shyh Hae graduated with a Bachelor of Engineering (Computer Engineering) degree from the National University of Singapore (NUS) in 2006. He further obtained a Master of Science (Computing and Security) degree from King's College London, UK, in 2011 under the DSTA Postgraduate Scholarship.

LEE Kok Thong is concurrently Head Command, Control and Communications (C3) and Ops Systems (Networked Systems) as well as Director (C3 and Ops Systems) of the Ops-Tech Group in the Ministry of Home Affairs (MHA). Kok Thong is primarily responsible for providing engineering support to MHA and the Home Team departments. He was previously Head Capability Development (Operations Infrastructure) in the InfoComm Infrastructure Programme Centre, where he was in charge of developing the SAF Integrated Knowledge-based Command and Control IT infrastructure. Kok Thong also served as Head of DSTA's Defence Technology Office (Europe) to manage defence technology relations with overseas partners. A recipient of the Public Service Commission Scholarship, Kok Thong graduated with a direct Master of Engineering (Electrical Engineering) degree from Ecole Foundation EPF, France, in 1997. He further obtained a Master of Science (Telecommunications) degree with Distinction from King's College London, UK, in 1997 as part of the European Schools Exchange Programme. Under the DSTA Postgraduate Scholarship, Kok Thong also graduated with a concurrent Master of Science (Defence Technology and Systems) degree from Temasek Defence Systems Institute, NUS, as well as a Master of Science (Information Assurance) degree with Distinction from the Naval Postgraduate School, USA, in 2003.

SEOW Nyi Matthew is Head Transmission and Core Network (InfoComm Infrastructure) who oversees the design, acquisition, implementation and system management of wide-area critical infrastructures for MINDEF and the SAF. He also contributed to the Infocomm Development Authority of Singapore's Service-wide Technical Architecture between 2007 and 2011. A recipient of the Public Service Commission Scholarship, Matthew graduated with a Bachelor of Engineering (Electrical and Electronic Engineering) degree with Honours from Nanyang Technological University in 1995.

TAN Choon How is a Senior Engineer (InfoComm Infrastructure) who is involved in conceptualising the next-generation NSOC. He was also part of the team that spearheaded the design and implementation of the Network Monitoring and Diagnostics System used by the SAF Network Operations Centre. Choon How graduated with a Bachelor of Technology (Electronics Engineering) degree with Honours from NUS in 2004.