UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

SECURITY OPERATIONS CENTRE (SOC) BASELINE CAPABILITIES

May 2023 Version 1.0

DISCLAIMER

This document is the sole property of UAE Cyber Security Council and is approved by the UAE Cabinet.

The UAE Cyber Security Council reserves the right to amend, add, or delete any section of this Policy.

Neither the whole nor part of this document shall be reproduced without the prior written consent of the UAE Cyber Security Council.

VERSION CONTROL

Version	0.1
Date:	11 May 2022
Prepared by:	CSC
Amendment Content:	Initial Draft Document

Version	0.2
Date:	25 June 2022
Prepared by:	CSC
Amendment Content:	Updated based on initial feedback

Version	1.0
Date:	30 August 2022
Prepared by:	CSC
Amendment Content:	Updates as per review comments on the draft v0.2 of the document

	Reviewed by	Approved by
Designation:	xxxxxxxxx	xxxxxxxxx
Name:	xxxxxxxxx	xxxxxxxxx
Signature:	xxxxxxxxx	xxxxxxxxx
Date:	xxxxxxxxx	xxxxxxxxx

Table of Contents

Table of Contents

SECTION 1

INTRODUCTION

INTRODUCTION

The evolving threat landscape and plethora of new technologies and business practices necessitates enterprises match the dexterity and skills of their adversaries, while ensuring their detection capabilities stay relevant and constantly advance their ability to respond. A key foundational element toward this is a competent Security Operations Center (SOC), alerting stakeholders of meaningful security events, centralizing alerts into a single functional unit and providing the ability to coordinate a response to emerging situations, thus limiting the impact of security incidents.

Modern day SOCs have at their disposal a wide array of sophisticated prevention, detection and response technologies, cyber intelligence reporting capabilities, and access to a rapidly expanding skilled cyber workforce. It is therefore necessary to outline baseline capabilities for Security Operations Centers within the Critical Information Infrastructure (CII) and propose maturity targets across technology, tools and supporting people and processes.

From the context of building national monitoring capabilities, it is expected that SOCs of CII entities are aligned and feed into the National Security Operations Center (NSOC) to support the UAE’s situational awareness. Supported by a common taxonomy of security events and incidents, it enables coherence in national incident response against cyber-attacks.

The Cyber Security Council has established this baseline to outline minimum requirements for CII Security Operations Centers and define maturity targets to enhance national cyber resilience. This initiative builds upon the UAE’s position as a global leader in cyber security, and further enhances the security posture of organizations and individuals within the UAE.

1.1 Purpose

The purpose of this document is to outline the approach to measure the maturity and capabilities of a CII SOC whilst also providing capability and maturity targets for minimum capabilities across CII sectors. This provides a roadmap for the development and improvement of SOCs across all critical infrastructure in the UAE.

While each organization and sector will need to customize their own level of SOC maturity that factors in their cyber risk tolerance and technology landscape, a minimum baseline capability, as outlined in the document, will contribute to enhancing the national cyber resilience.

1.2 Scope & Applicability

This document provides the mandatory minimum level of maturity for SOCs across each identified Critical Information Infrastructure sector. It further outlines the security capabilities that must be present and integrated across the monitored environment and should be adopted across the CII in the UAE.

The framework also specifies the guidance for implementation of the security capabilities of a SOC and can be used to evaluate the compliance of each individual organization to the requirements. While the document sets out to elaborate the requirements and guidance across various elements of SOC capabilities and maturity, it does so in a technology agnostic manner.

This document is applicable to CII entities that are identified as such in the Critical Information Infrastructure Policy, as well as Managed Service Providers that provide outsourced SOC services to CII in the UAE.

SECTION 2

IMPACT DEFINITION

2.1 Significant Event vs Incident

Information Technology Infrastructure Library (ITIL) defines an incident as the unplanned interruption (or reduction in quality) of an IT service while event can be defined as any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT service. However, these definitions do not lend themselves as neatly to security events and incidents. The earliest stages of an intrusion carry no intrinsic impact, yet they are more relevant than a simple security event. As such, we adopt the following three definitions:

- Security Event. Any observable occurrence that is relevant to information security. Example: A user login into a server via secure shell (SSH).
- Significant Security Event. A security event which is of particular interest to the SOC, as it carries implications of a security threat in the environment.
- Example: Blocked by an antivirus solution, a recently downloaded malware fails to execute.
- Security Incident. A significant security event that either directly implies or carries the significant risk of impact to the organization, its assets or its information.

Example: Ransomware replicating rapidly through an environment.

The key distinction is impact. Impact separates events that while potentially malicious, are ultimately irrelevant to your operations, from the events that warrant the expensive time-consuming disruptions that are necessary to appropriately investigate and resolve security Incidents. A Trojan (backdoor) for example, should be removed from a system, but if it cannot, and never succeeded in calling back to its Command & Control Server (C&C), is it really an incident, or a simple case of cyber hygiene? While the criticality of the asset matters in this question, in most cases, this can be categorized as a significant security event.

2.2 Formal Definition of Impact

Impact is defined as any damage or significant risk to the confidentiality, availability or integrity of information, assets, and operations.

However, in a modern SOC, this definition is expanded beyond the traditional Confidentiality, Integrity, and Availability model (CIA triad). Maintaining control and safety are major imperatives in environments where Industrial Control Systems (ICS), Operational Technology (OT) or Internet of Things (IoT) play a significant role, and require the same level of consideration.

Prioritizing incidents is an important part of the triage process of a SOC. It also defines the level of response, the level of coordination, and frequency of notification to relevant stakeholders during the actual incident. As we differentiate a significant event from an incident, based on its impact or potential impact, impact should be the primary method of evaluating the priority. Note that this approach allows for the exclusion of a separate metric, often called severity, which is often an arbitrary measure associated with the type of threat. To reiterate, the nature of a threat is irrelevant compared to its potential impact. This approach will allow us to forgo any priority/severity matrix which add little value to the management of the incident. Instead, how close a threat actor is to achieving their goal of impacting your organization, will be the deciding criteria.

2.2 Formal Definition of Impact

The following priorities are mapped to steps In the MITRE ATT&CK framework. This mapping allows integration with a hierarchical use case framework, where alerts directed from your Security Incident Event Management (SIEM) or Extended Detection & Response (XDR) to your analyst are already mapped to the following priorities.

Priority	MITRE ATT&CK
Significant Events: Entry Level & Failed Attacks	Reconnaissance, Initial Access, Resource Development
P3: Early Stage	Command and Control, Execution, Persistence, Defense Evasion
P2: Mid Stage	Privilege Escalation, Lateral Movement, Credential Access, Discovery
P1: Late Stage & Critical Assets	Collection, Impact, Exfiltration Note: Alerts on assets that are considered critical should start at this stage
P0: Successful Attacks	N/A Note: This priority is reserved for Incidents that are discovered after the fact, such as in the case of a breach, and Incidents where the cumulative impact is so qualitatively high, that it requires the highest attention.

SECTION 3

MATURITY, CAPABILITY & METHODOLOGY

This framework borrows heavily from the SOC-CMM framework, which in turns borrows from the Capability Maturity Model Integration (CMMI). The CMMI framework was developed by the Carnegie Mellon University and aims at improving processes across project, division and entire organization. It defines maturity levels that can be used to evaluate processes, and leveraged to improve them. The SOC-CMM, developed by Rob Van Os and popularized in the Dutch banking system, extended that concept to the Security Operations Center.

3.1 Maturity

Maturity is experience codified. It is a predictable, reproducible approach at the various processes, and questions related to the operation of a SOC. There are two keys to maturity, documentation and the adoption of that documentation into your organization’s culture. CMMI style frameworks operate on plateaus of achievement, which provide a look at the overall progress toward maturity. Since culture is difficult to evaluate, the framework focuses on the **documentation** aspect.

Level	Name	Description
0	**Non-existent**	At this level, the aspect is extremely ad-hoc or incomplete. Thus, delivery is not assured.
1	**Initial**	The aspect is delivered in an ad-hoc fashion.
2	**Managed**	The aspect is documented and delivered consistently.
3	**Defined**	The aspect is managed using ad-hoc feedback on the quality and timeliness of deliverables. This step is about continual improvement. Document is revisited at least once a year, with the intent of keeping it accurate, and improving it.
4	**Quantitatively Managed**	The aspect is systematically being measured for quality, quantity and timeliness of deliverables. Similar to level 3, the document is revisited at least once a year, however, the difference is what drives the change. It’s now propelled by metrics and KPIs.
5	**Optimizing**	The aspect is continuously being optimized and improved upon. Opportunity to improve are being actively sought and monitored for. Performance is reviewed monthly, weekly, or more, and changes made not only as required, but in an attempt to test out new ways of creating efficiency.

3.2 Capability

Capability is the ability to put will to action. In a SOC, that translates to the ability to communicate, coordinate, prevent, detect, analyses, contain, and remediate. A SOC will utilize many different technologies, methodologies, expertise and processes to accomplish these goals.

Similar to maturity, capabilities are rated on plateaus of achievement, which provide a look at the overall progress toward achieving the fullest extent of the desired capabilities. Since methodology is difficult to evaluate, the framework focuses primarily on the **technological** aspect

Level	Name	Description
0	**Incomplete**	At this level, the aspect is incomplete. Thus, the SOC has insufficient capability to deliver this aspect.
1	**Performed**	There is sufficient capability to deliver the aspect at a basic level. At this level, you have the capability in some form, and it’s applied at the areas you need most.
2	**Managed**	The capability for the aspect is delivered consistently. The capability has reached near-full coverage, and is of good quality.
3	**Defined**	The capability for this aspect is optimized and well-documented and delivers true added value. The capability is of good quality and is frequently (monthly, weekly, etc) improved based on metrics.

3.3 Evaluation Methodology

This framework provides a grid which may be used to evaluate and plan future improvement. It effectively provides a roadmap of all the documents that need to be created, approved, and maintained, and of all the capabilities that a SOC needs to acquire, to count itself among the finest example of its kind.

Principally, this document and the accompanying grid can be used to perform an assessment against an existing SOC and help identify the areas that need to be further developed to achieve the organization’s required, expected, or desired goals. Performing an assessment requires collecting copies of each documents that contains proof of the maturity or capability level of each item being assessed.

For capabilities, this will often require a screenshot or export of the configuration of the associated technology. These must demonstrate that the capability not only exists but is also deployed with the appropriate amount of coverage.

SECTION 4

INDUSTRY TARGETS

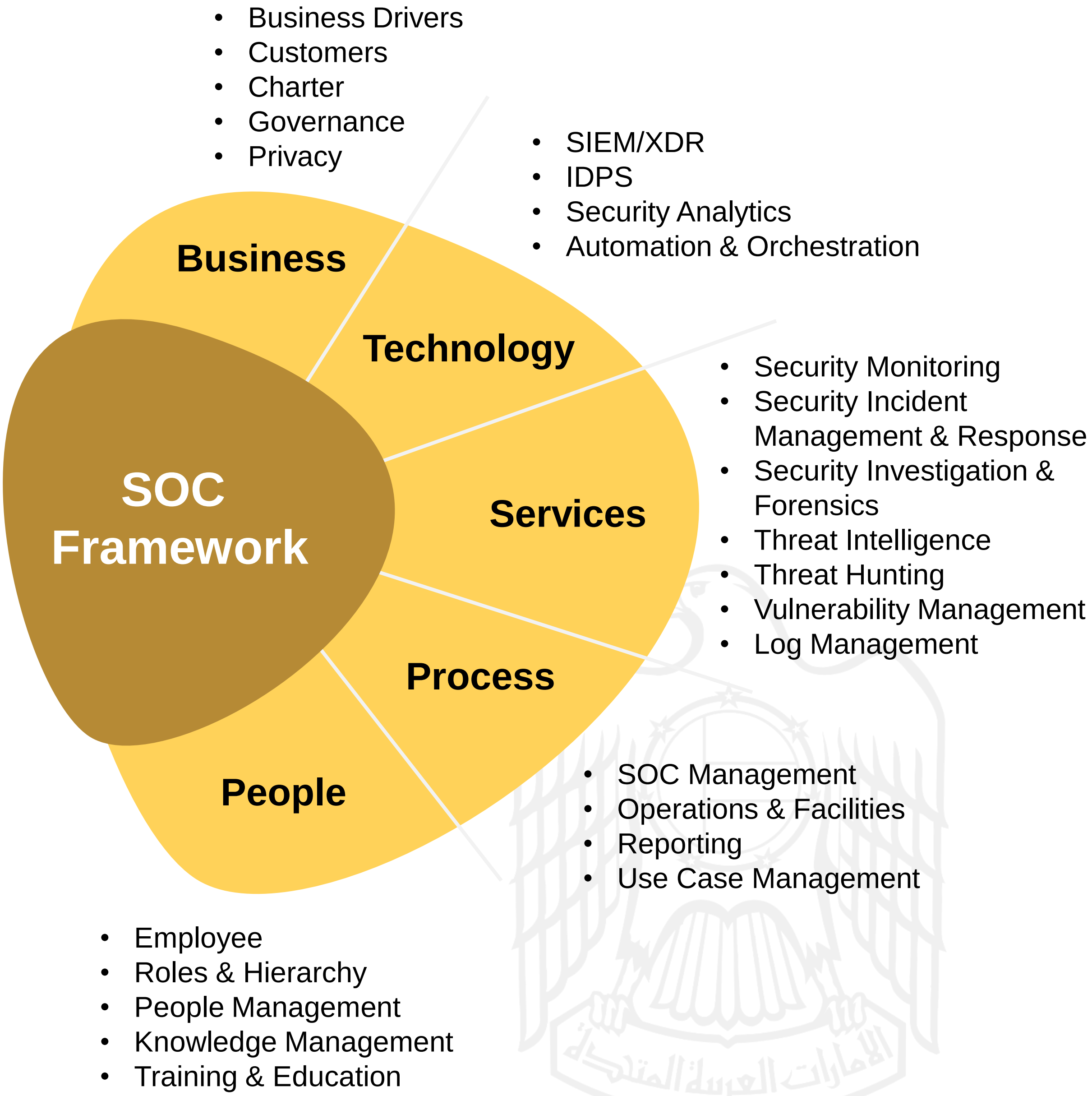
Critical Industries are expected to meet the mandatory targets set in this document within three years of implementation of this baseline. Targets are calculated as the average (mean) of the maturity, and capability score across the total applicable SOC domains.

Industry	Criteria	Mandatory Target	Recommended Target
Energy	Maturity	4	5
	Capability	2	3
Transport	Maturity	3	4
	Capability	2	2
Financial	Maturity	3	4
	Capability	2	2
Health	Maturity	3	4
	Capability	2	2
Electricity & Water	Maturity	4	5
	Capability	2	3
Digital Infrastructure	Maturity	3	4
	Capability	2	2
Government Services	Maturity	3	4
	Capability	2	2
Defense	Maturity	4	5
	Capability	2	3
Education	Maturity	3	4
	Capability	2	2
Space	Maturity	3	4
	Capability	2	2
Food	Maturity	3	4
	Capability	2	2

SECTION 5

SOC FRAMEWORK

The SOC framework relies principally on documentation. Each of the below section can be thought of as a separate document, with version control and stakeholder signature for formal acceptance. It is perfectly acceptable to group many of these sections into a single document, where deemed appropriate. Note that while auditors must rely on paper to provide proof of existence, the aspects captured here must be real and part of the daily life of the SOC.



- Business Drivers
- Customers
- Charter
- Governance
- Privacy

- SIEM/XDR
- IDPS
- Security Analytics
- Automation & Orchestration

- Security Monitoring
- Security Incident Management & Response
- Security Investigation & Forensics
- Threat Intelligence
- Threat Hunting
- Vulnerability Management
- Log Management

- SOC Management
- Operations & Facilities
- Reporting
- Use Case Management

- Employee
- Roles & Hierarchy
- People Management
- Knowledge Management
- Training & Education

5.1 Business

A SOC is first and foremost an organization, and at the core of an organization are the documents that define it. To manage a business, is to coordinate and organize the business activities to achieve its stated goals. While in security, the goals may seem self-evident, the very reasons SOCs and cybersecurity programs are tailored to specific industries, is due to the specific focus these industries require.

5.1.1 Business Drivers

Objective

Identify the key activities, inputs and imperatives that drive the operational requirements of the SOC, document the business drivers thus identified and ensure its continuous appropriateness.

Guidance

The first step is to identify the key activities, inputs and imperatives that drive the operational result of the SOC and capture them in a document. Your organization will have multiple business drivers, and they can change and grow over time. Below is a non-exhaustive list which should be identified along with the business stakeholders.

BD#	Business Driver
BD1	Maintaining the Accessibility of the Information
BD2	Maintaining the Confidentiality of the Information
BD3	Maintaining the Integrity of the Information
BD4	Maintaining Control of the Operations
BD5	Maintaining the Safety of the Users
BD6	Maintaining the Privacy of Users
BD7	Participating in maintaining a timely picture of the overall Cybersecurity posture for the UAE
BD8	Building resiliency against foreign threat actors
…	…

The documented business drivers should be continuously aligned with the organizational strategy and objectives, and the SOC service catalogue should be updated in line with the business drivers.

5.1 Business

5.1.2 Customers

Objective

Identify the customers for the SOC, their needs and expectations, and document formal service level agreements.

Guidance

A SOC typically has more than a single stakeholder. It is important to recognize formally the SOC customers, and document that relationship. The formal documentation with the customers should also align the customers' obligations, the inputs, the outputs, SLAs & contact points.

Typically, the SOC relationship can include, but is not limited to:

- Legal
- HR
- Audit
- Operations Security
- Engineering / R&D
- IT
- Business
- External customers
- (Senior) Management
- Regional SOC
- National SOC

The customer engagement process should be outlined and at a minimum should include regular updates on the service level monitoring, and measurement & monitoring of customer satisfaction.

5.1 Business

5.1.3 Charter

Objective

Document the formal charter for the SOC which outlines its authority and its mission statement.

Guidance

The SOC derives its authority from its charter, which is both a formal grant and a mission statement. It will specify the responsibilities, and specific rights granted to the SOC in pursuit of those duties.

It is particularly important, that this document be regularly updated and include the signature of the stakeholders, and parties that grant their authority to it.

A typical charter can include the following sections:

- Mission: A SOC mission should be established to provide insight into the reason for existence of the SOC
- Vision: This describes long-term goals for the SOC
- Strategy: A strategy should be in place to show how to meet goals and targets set by mission and vision
- Service Scope: Service scope is documented to provide insight into SOC service delivery
- Deliverables: The output provided by the SOC, for example: reports, incidents, investigations, advisories, etc.
- Responsibilities: A list of activities for which the SOC is responsible
- Accountability: A list of activities for which the SOC is accountable
- Operational Hours: The operational hours of the SOC, and its services
- Stakeholders: A list of the organization, roles or individual to who the SOC answers to, and derives its mission and requirements
- Objectives and Goals: Objectives and goals should be concrete and measurable so that they are fit for reporting purposes
- Statement of Success: A statement of success is used to determine when the SOC is successful. Should be aligned with goals and objectives
- Signatures: Signatures of the stakeholders

5.1 Business

5.1.4 Governance

Objective

Document the governance model employed for the SOC, including its high-level interactions, evaluation & monitoring of its mandate and provisioning of resources for its efficient functioning.

Guidance

The SOC's strategic alignment, must be documented. Governance is concerned about the high-level interactions of the SOC, and its long-term planning. Along with the mandate and sponsorship of the SOC, it is required that the SOC evaluate its performance, identify the key reporting metrics, and reporting hierarchy and process. The span of control of federation governance will impact the output, inputs and processes implemented within the SOC.

The following elements should be identified and continuously reviewed:

- Accountability
- Sponsorship
- Mandate
- Vendor and third-party engagement
- Program management
- Continual improvement process
- Span of control
- Alignment with regional, sector and national entities
- SOC KPIs and metrics
- SOC audits and external assessments

Another facet to consider, is budgeting and provisioning of resources. Proper cost management practices should be applied to the SOC, including budgeting and monitoring activities across the following elements:

- People cost
- Process cost
- Technology cost
- Services cost
- Budget forecasting
- Budget alignment
- Return on investment

5.1 Business

5.1.5 Privacy

Objective

Outline a privacy policy for the SOC regarding security monitoring of customers and employees, in line with applicable laws and regulations and cater for any binding privacy requirements.

Guidance

The data collection, handling and processing performed as part of a SOC has direct impact on the privacy of customers, employees and visitors. As any SOC operates within the boundary of not only its organizational policy, but also appropriate laws and regulations, hence care must be taken in precisely documenting the approach at meeting these requirements.

Accordingly, the following privacy related elements should be implemented:

- Identification of applicable laws and regulations and co-operation with entity legal teams
- Procedures for dealing with privacy related investigations
- Identification of information that SOC processes and is subject to privacy regulations
- Privacy Impact Assessment (PIA)
- Privacy controls identified through the PIA (Limit the access to personal data; Data subject consent, where applicable; Data retention guidelines; Data usage scenarios; Data privacy trainings)

5.2 People

People are the principal resource of a SOC. While artificial intelligence is getting better every year, there are still no replacement available for the synthesis and investigative power of a human security analyst. A mature approach at managing people requires well thought out processes of acquisition, optimization and retention of talent. Security is not a commodity industry. The lead time to find quality resources can be particularly painful, as such, care must be taken to motivate, direct, and train existing staff to maximize the SOC's ability to close a particularly wide knowledge requirement.

5.2 People

5.2.1 Employees

Objective

Establish the workforce requirements for efficient functioning of the SOC including the Full-time-Employee (FTE) requirements, skill-set requirements, and talent acquisition processes.

Guidance

The number of resources a SOC requires depends on its hours of operation, the desired capabilities, as well as the size of the overall organization being monitored. 24/7 staffing requires a minimum of 12 resources, to cover the monitoring alone. The shortage of talented, affordable resources in the security industry often results in SOC supplementing their staffing requirements with external contractors. Since dependence on external vendors always represent a dependence and risk, managing the ratio of internal to external Full-time-Employee (FTE), should be an ongoing goal of the SOC. Below you will find some sizing recommendations, note that barebones and minimum should not be considered suitable for critical infrastructure organizations.

Category	Max Org Size	Hours of Operations	Afterhours Support	Analysis FTE	Minimum Emiratization Ratio
Barebones	100	9to5*	1 Resource on Rotation	2	0%
Minimum	500	9to5*	1 Resource on Rotation	6	40%
Recommended	1000	24x7	1 Resources on Rotation for IR	14-16	60%
Preferred	5000	24x7	2 Resources on Rotation for IR	20	80%

All SOC positions should be filled and supporting talent acquisition and recruitment processes should support the SOC workforce requirements. Note that these represent recommendations only, and sector mandates should be at the forefront of any decision around the actual resource composition of the SOC.

Wherever outsourcing is employed, the SOC remains fully accountable to deliver on the expected maturity and capability score provided in **section 4 Industry Targets**. As such, we strongly recommend enforcing vendors to meet the targets that they participate or are solely responsible for delivering through clearly defined contractual terms.

5.2 People

5.2.2 Roles & Hierarchy

Objective

Establish a role-based hierarchy within the SOC organization and outline the responsibilities for each role.

Guidance

The role- based hierarchy within the SOC need to be carefully documented to outline the expectations, including the role description, responsibilities, tasks assigned, technical skills, soft skills, educational level and certificate requirements. The roles should be regularly reviewed and revised, as required.

5.2 People

5.2.3 People Management

Objective

Apply a consistent and defined people management approach to acquire, optimize and retain talent for SOC operations.

Guidance

The employee life cycle should start with a mature talent management process, which is effectively in the anticipation of the required human capital for the SOC. This should be coupled with a recruitment and onboarding process for new hires. It may be required to meet diversity and inclusion mandates of the organization and/ or Emiratization targets which should be carefully considered and applied.

As the shortage of skilled resource will remain a factor for the foreseeable future, training and cross-training resource helps alleviates concerns for future employee turnover, as well as increase the internal-to-external ratio of FTEs.

To further increase employee retention, career path planning and employee satisfaction must be implemented.

Other processes meant to embed security across the employee lifecycle such as screening, job rotation, periodic monitoring and evaluation should be implemented.

5.2 People

5.2.4 Knowledge Management

Objective

Establish formal knowledge management practices for the SOC operations.

Guidance

The broad set of skills and abilities required to accomplish a SOCs mission can be particularly complex to manage. Knowledge management represents the level of mastery the SOC has over it's the sum of knowledge and skills that are desired, and the state of what is currently present within the organization. It will cover how knowledge is gathered, organized, shared and optimized.

A SOC defined skill matrix and periodic assessment covering technical and non-technical soft skills should be used to drive team and personal improvement across the SOC workforce.

A knowledge matrix covering all workforce and knowledge areas should be outlined and used to determine training and education needs.

The extent of the skill & knowledge coverage across available SOC resources and regular update of the skill & knowledge matrix will drive its continued relevance.

Tools should be leveraged to support knowledge documentation and distribution.

5.2 People

5.2.5 Training & Education

Objective

Implement a training and education program for the SOC workforce to address skills and knowledge gaps

Guidance

The SOC’s training program should be role specific, include soft-skills, and considers multiple approach, from training on the job, product specific training and formal education.

Additionally, developing a number of certification track, where each role and levels within your organization is mapped to a necessary set of trainings, to demonstrable knowledge and skills is indicative of a mature SOC organization.

The training and education program should be linked to performance evaluation and career progression. For an effective training and awareness program, reserved budget and reserved amount of workforce time are key enablers, along with ongoing review and update of the training and education program.

5.3 Process

Processes are a series of steps and actions, that achieve a desired outcome, and more importantly, contribute to the stability of the SOC's operations. Designing and implementing the appropriate process architecture are necessary steps toward aligning the downstream processes with the strategic goals of the organization.

5.3.1 SOC Management

Objective

To organize and maintain the various relationship necessary for the functioning of a SOC and accountable for the continual improvement of the operation, by establishing methodologies for the processes for daily operations.

Guidance

There should be a SOC management procedure in place, which clearly identifies the following elements that are required for appropriate SOC management:

- Internal and external relationship management
- Vendor management
- Continuous service improvement
- Project methodology
- Process documentation and diagrams
- RACI matrix
- Service Catalogue
- Service on-boarding procedure
- Service off-boarding procedure
- Compliance monitoring

The SOC management procedure documentation should be regularly reviewed and updated. The procedure may also be shared with relevant stakeholders for alignment.

5.3 Process

5.3.2 Operations & Facilities

Objective

To ensure that services, people, processes, and tools are present at all times to maintain service availability.

Guidance

While the SOC itself may not be responsible for the operations and maintenance of its facilities, it shares in the accountability to maintain its services availability. As such ensuring that the broad spectrum of services, people, processes, and tools are present at all times, is part of a SOC's mission.

Additionally, the following requirements should be addressed:

1. Service delivery standardization - The daily operational activities within the SOC should be clearly documented in an operational handbook, containing all workflows, standard operating procedures, and checklists for recurring activities. Accordingly, security operation exercises should be performed regularly to ensure
2. Process integration – The following processes should be well integrated in the SOC: Change management, configuration management, problem management, incident management and asset management.
3. SOC Facilities – Wherever feasible, the following aspects should be considered for SOC facilities: dedicated physical SOC location with controlled access to the SOC center, dedicated network for the SOC, video wall for monitoring purpose, call center capabilities, and specialized analyst workstations.
4. 4. Operational Shifts – There should be clear shift schedules identified and a shift log maintained (manual or automated, whichever is feasible). There should also be shift handover template which may include, but not limited to:
    - Any on-going issues
    - Any monitoring alerts
    - Critical applications check
    - Incident details
    - Change details
    - Request details
    - Task handover
5. Knowledge Management – The SOC should establish a Document Management system and leverage a knowledge and collaboration platform.
6. Environmental Management – Certain aspects of data center management that are often neglected but are nonetheless vital to a SOC's continued operations are power and Heating, Ventilation and Air Conditioning (HVAC). The process and ownership of these must be documented along with a detail description of the organization's floor plans.

5.3 Process

5.3.3 Reporting

Objective

To ensure reports are produced on a defined frequency based on type of audience/recipient and these reports are reviewed and/or approved, as required.

Guidance

The SOC may produce daily, weekly, monthly, quarterly, and yearly reports depending on audience/recipient. Following may be some examples of the type of reports, audience and frequency, however this may change based on the organization’s requirements.

Report Type	Audience	Frequency
Operational reports	Security Team	Daily/Weekly
Incident reports	Security Team and IT	Daily/Weekly
Technical security reports	Security, IT and Applications teams	Monthly
Trends Report	Security, IT and Applications teams	Monthly
Newsletter or digest	All	Monthly
KPI reports	Security Team, Business teams and Senior Management	Quarterly
Executive security reports	Security Team, Business teams and Senior Management	Quarterly and Yearly

Wherever feasible, reports should use qualitative and quantitative metrics, incident, and case metrics and SLA details.

5.3 Process

5.3.3 Reporting

Additionally, a security incident report should be authored following all P0 to P3 incidents. Since P3 and P2 reporting may be common and frequent, it is important that these reports share a common and simple format and aim to be succinct. A greater attention to detail and content, can always be extended when required, such as in the case of a P0 or P1.

A proper computer security incident report, should feature the following fields:

- Start Date & Time of Incident
- End Date & Time of Incident
- Priority
- Category
- Title
- Detection Date & Time
- Detection or Reporting Mechanism
- Investigative Team
- Description
- Timeline
- Evidence & Analysis
- Remediation
- Summary & Recommendations

5.3 Process

5.3.4 Use Case Management

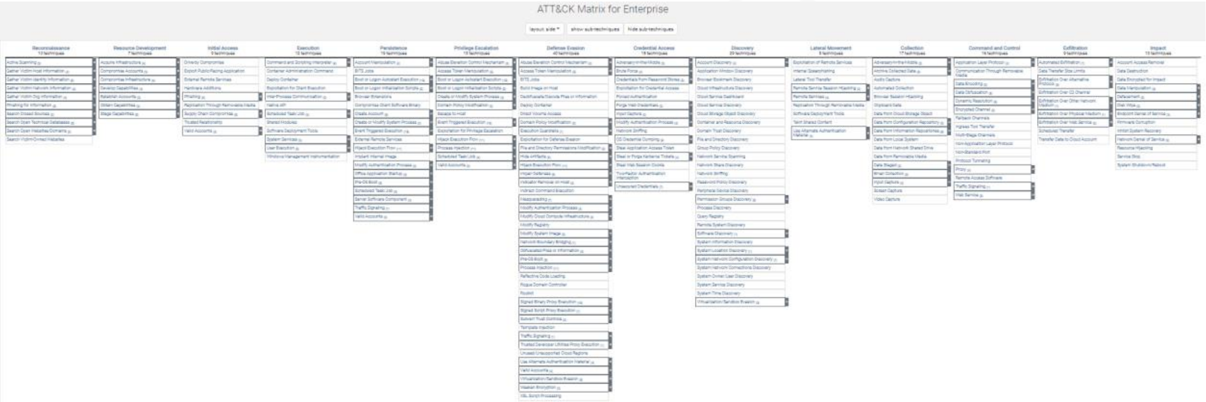
Objective

To provide a structured approach to security monitoring and describe follow-up actions which are tied with business drivers.

Guidance

Formally a use case is more than simple a mechanism of detection, it is the combined technical activities, technologies and processes that transforms an input into a desired output or condition. In the context of a SOC, the overall goal is to move from an unsecured to a secured state. As such, most SOC use case will involve delivering on specific business drivers through the discovery of a suspicious or unwanted behavior, so that it may first be investigated, then reacted upon appropriately.

While describing a full use case management framework falls outside of the stated goal of this document, a proper approach is so critical to the successful operation of a SOC, that some guidelines should be followed. While, as previously noted, processes and technologies factor into it, technical use cases are the focus of this practice. These technical use cases exist primarily inside of your organization's SIEM/XDR, which has a limited capacity and performance, and yet must cover a wide set of abilities to identify Tactics, Techniques, and Procedures (TTPs) from the collected logs. In addition, one cannot ignore the human factor, security analysts have a limited capacity to process alerts.



Use cases should be organized in a hierarchical framework and take a top-down approach at accomplishing the expected detection goals. It is a common trap of SOC to develop one-off use cases that target specific vulnerabilities or malware campaign. It is the strong recommendation of this document that a more comprehensive framework should be adopted.

5.4 Technology

While technology is pervasive, and touches on all the other domains, here we are solely focused on technology that should help accomplish one of the principal stages of the cybersecurity lifecycle: Prevention, Detection, Investigation, Containment, and Remediation.

Technologies are measured for their maturity and capability. Each technology category should be captured by at least 1 separate, unique document that covers the following sections:

- Technical Ownership
- Functional Ownership
- Technical Description
- Functional Description
- Training Status
- Support Status
- Availability & Integrity
- Confidentiality Status

Capabilities must be comprehensive in their coverage. If only a small segment of the network is covered, or the possibility of identifying a particular pattern is low, then it should significantly penalize the level associated with the capability.

5.4 Technology

5.4.1 SIEM/XDR

Objective

To provide log management, and correlation capabilities, which are leveraged to centralize all alerts and signals to a single focal point of management using a Security Information and Event Management (SIEM) or Extended Detection and Remediation (XDR) platform.

Guidance

Security Information and Event Management (SIEM) and Extended Detection and Remediation (XDR) platform are two generations of the same conceptual approach. They are the principal tool of a SOC, through which a SOC maintains a holistic view of the security posture of the organization. SIEM/XDRs are where most technical use cases are developed, often with the purpose of providing dashboard, reporting, and most importantly alerts, which will then be processed by the Security Monitoring Service. It is also the repository of metrics that management will leverage to evaluate services.

The following technology capabilities should be available:

- Aggregation
- Correlation
- Custom parsing
- Threat Intelligence integration
- Subtle event detection
- Automated alerting
- Alert acknowledgement
- Automated threat response
- Multi-stage correlation
- Pattern detection
- Case management system
- Asset management integration
- Business context integration
- Identity context integration
- Asset context integration
- Vulnerability context integration
- Standard rules
- Custom rules
- Network model
- Customized SIEM/XDR reports
- Customized SIEM/XDR dashboards
- Granular access control
- Controlled and monitored maintenance / support
- API Integration
- Secure Event Transfer
- Support for multiple event transfer technologies

5.4 Technology

5.4.2 IDPS

Objective

To enable detection, and automatic blocking of IoCs and behavioural indicators using technology.

Guidance

Traditionally, the term Intrusion Detection and Prevention System refers to a family of devices that can be leveraged to monitor network traffic for suspicious activity, and block this activity through an automatic, or manual intervention. In this document, the definition is broader to contain all technologies that can participate directly into the detection, and automatic blocking of IoCs and behavioural indicators:

It contains, but is not limited, to the following classes of devices:

- Network-Based IDPS
- Wireless IDPS
- Network Behaviour Analysis (NBA) System
- Host-Based IDPS & Antivirus Solution
- Anti-DDoS Solutions
- Pack Capture Engine
- Network Access Control (NAC) Systems
- Application Whitelisting Software
- Data Leakage Protection (DLP) System and Software
- Web Application Firewall
- Endpoint Detection & Remediation (EDR)
- Network Sandboxing
- Network Detection and Response instead of NBA
- Email and Web filtering

There are 3 major approaches that are common to all IDPS solutions:

- Signature-based
- Anomaly-based
- Protocol-based

5.4 Technology

5.4.2 IDPS

Aside from participating in reducing the exposure, and risk profile of the organization, the IDPS stack represents the principal means of intervening during an incident for the SOC.

The following technology capabilities should be available:

- Network-based intrusion detection
- Host-based intrusion detection
- File integrity checking
- Application whitelisting
- Honeypots
- Custom signatures
- Anomaly detection
- Automated alerting
- Central Management Console
- Full Packet Capture for inbound / outbound internet traffic
- Full Packet Capture for high-value internal network segments
- Full Packet Capture for other internal networks
- Granular access control
- Controlled and monitored maintenance / support
- SIEM/XDR integration
- API integration
- Threat Intelligence integration
- DDoS Protection
- Application DoS Protection
- Web Application Firewall
- Email and Web Filter
- EDR
- Cloud capabilities (CASB, CSPM, CWPP)

5.4 Technology

5.4.3 Security Analytics Tooling

Objective

To accomplish use cases that may be too large in scope, or too complex for a traditional SIEM solution, by using the adequate security analytics solution (such as Big Data Analytics) and threat intelligence.

Guidance

At its most advanced stages, this technical capability can be significantly expensive, and may not be suited to smaller SOC. It is, however, indispensable to high data environment such as Internet Service Provider (ISP), transport network and data center, which can leverage their privileged accesses to uncover malicious infrastructure. This also, in part, the differentiator between a SIEM and an XDR, the latter which covers several of the functionality listed here.

The following capabilities should be maintained by the overall technology deployment:

- Scalable analytics engine
- Automated data normalization
- Pattern-based analysis
- Integration of security incident management
- Integration of security monitoring
- External threat intelligence integration
- Advanced searching and querying
- Data visualization techniques
- Data drilldowns
- Detailed audit trail of analyst activities
- Historical activity detection
- Structured data collection
- Unstructured data collection
- User baselines
- Application baselines
- Infrastructure baselines
- Network baselines
- System baselines
- Central analysis console
- Security data warehouse
- Flexible data architecture
- Granular access control
- Controlled and monitored maintenance / support
- API Integration

5.4 Technology

5.4.4 Automation and Orchestration

Objective

To enable automation as a method of connecting disparate security tools into a single integrated solution.

Guidance

It is typical for a SOC to become overwhelmed by large volume of low-level significant events and incidents. Security automation then takes root in performing tasks on behalf of a human analyst, simply alleviating the load in some case, or resolving the event entirely independently. Typically, this is embodied in a product called a Security Orchestration, Automation and Response (SOAR). While not limited to this scenario, the SOAR will often be actioned by a SIEM/XDR use case triggering. It will then action a playbook, that capture the workflow of that use case resolution. These playbooks can be fully automated, or partially automated, where a human analyst intervention is deemed necessary.

Acquiring, developing and improving these playbooks, should be a strong qualitative measure of the performance and readiness of this technology.

The following capabilities should be maintained by the overall technology deployment:

- SIEM/XDR Integration
- Threat intelligence integration
- Asset management integration
- User management integration
- Vulnerability management integration
- Historical event matching
- Knowledge base integration
- Risk-based event prioritization
- Firewall integration
- IDPS integration
- Email protection integration
- Malware protection integration
- Sandbox integration
- Active Directory / IAM integration
- Ticket workflow support
- Granular access control
- Controlled and monitored maintenance / support
- Performance tracking

5.5 Services

All SOC domains exist in support of creating the services the SOC provides. They are the true expression of the value the SOC represents to the organization. They are defined as high level activities that together put into action the ability to protect the environment under the SOC's mandate.

Services are measured for their maturity and capability. Each service should be captured in a separate, unique document that covers the following sections:

- Key performance indicators
- Quality indicators
- Service dependencies
- Service levels
- Hours of operation
- Service customers and stakeholders
- Purpose
- Service input / triggers
- Service output / deliverables
- Service activities
- Service roles & responsibilities

Capabilities must be comprehensive in their coverage. If only a small segment of the network is covered, or the possibility of identifying a particular pattern is low, then it should significantly penalize the level of maturity associated with the capability.

5.5 Services

5.5.1 Security Monitoring

Objective

To establish a process of collecting and analysing logs and signals, to identify potential security incidents, which are then validated, triaged, and escalated to the incident management service.

Guidance

Most incidents handled by the incident management service are in fact initiated from the security monitoring service. The focus of the service is on visibility, and the key to visibility is detection and maintaining continuous near-real time alerting.

The following capabilities should be maintained by this service:

- Early detection
- Intrusion detection
- Exfiltration detection
- Subtle event detection
- Malware detection
- Anomaly detection
- Real-time detection
- Alerting & notification
- Status monitoring
- Perimeter monitoring
- Host monitoring
- Network & traffic monitoring
- Access & usage monitoring
- User monitoring
- Application & service monitoring
- Behaviour monitoring
- Database monitoring
- Data loss monitoring
- Device loss / theft monitoring
- Third-party monitoring
- Physical environment monitoring
- False-positive reduction
- Continuous tuning
- Coverage
- Cloud monitoring
- Mobile device monitoring

5.5 Services

5.5.2 Security Incident Management and Response

Objective

To establish processes and procedure that are utilized to resolve significant security events, security incidents and post-breach investigations to reduce the impact, provide clarity into the occurrence, remediate the compromised assets, and provide recommendations to avoid similar events in the future

Guidance

Security Incident management is the process of reacting and coordinating response to security threats that reasonably could or have caused impact to the organization.

The following capabilities should be maintained by this service:

- Incident logging procedure
- Incident resolution procedure
- Incident investigation procedure
- Escalation procedure
- Evidence collection procedure
- Password change procedure
- IR Training
- Table-top exercises
- Red team / blue team exercises
- RACI matrix
- Response authorization
- Incident template
- Incident tracking system
- False-positive reduction
- Priority assignment
- Severity assignment
- Categorization
- Critical bridge
- War room
- Communication plan & email templates
- Backup communication technology
- Secure communication channels
- (dedicated) information sharing platform
- Change management integration
- Malware extraction & analysis
- On-site incident response
- Remote incident response
- Third-party escalation
- Evaluation template
- Reporting template
- Incident closure
- Lessons learned extraction for process improvement
- External security incident support agreements
- Exercises with other incident response teams
- Root Cause Analysis

5.5 Services

5.5.3 Security Investigation and Forensics

Objective

To provide security monitoring with the ability differentiate false from true positive, the ability to establish forensically sound timelines to incident management service and expand the knowledge of an incident to the resolution of fundamental questions such as what, why, who, when, where, and how.

Guidance

Security analysis includes disk and memory forensics, as well as the advanced analysis of binaries. Once a suspected threat is identified, it must undergo testing, to first determine whether it’s a false positive or a malicious event, and then to identify the nature of the threat. Once that is accomplished, it will be possible derive the necessary insight to discover additional compromise within the organization, if any exist. The service represents the sum of the analytical capabilities of the SOC, from advanced manual review of the log, to advanced big data analytics processing.

The following capabilities should be maintained by this service:

- Event analysis
- Event analysis toolkit
- Trend analysis
- Incident analysis
- Visual analysis
- Static malware analysis
- Dynamic malware analysis
- Tradecraft analysis
- Historic analysis
- Network analysis
- Memory analysis
- Mobile device analysis
- Volatile information collection
- Remote evidence collection
- Forensic hardware toolkit
- Forensic analysis software toolkit
- Dedicated analysis workstations
- Security analysis & forensics handbook
- Security analysis & forensics workflows
- Case management system
- Report templates
- Evidence seizure procedure
- Evidence transport procedure
- Chain of custody preservation procedure

5.5 Services

5.5.4 Threat Intelligence

Objective

To provide with the ingestion, processing, management, analysis, and reporting of Indicators of Compromise (IoCs) through threat feeds, (that can include IP, Domains, File Hashes, or even behavioural indicators) and to establish closer links to other organizations and participate in the voluntary or compulsory sharing of information.

Guidance

The most mature threat Intel program will work closely with the security analysis and threat hunting services to generate their own threat intelligence.

The following capabilities should be maintained by this service:

- Continuous intelligence gathering
- Automated intelligence gathering & processing
- Centralized collection & distribution
- Intelligence collection from open / public sources
- Intelligence collection from closed communities
- Intelligence collection from intelligence provider
- Intelligence collection from business partners
- Intelligence collection from mailing lists
- Intelligence collection from internal sources
- Structured data analysis
- Unstructured data analysis
- Past incident analysis
- Trend analysis
- Automated alerting
- Adversary movement tracking
- Attacker identification
- Threat identification
- Threat prediction
- Threat intelligence SOPs
- Roles and responsibilities
- Monitor & report vulnerabilities
- TTP extraction
- Deduplication
- Enrichment
- Contextualization
- Prioritization
- Threat intelligence reporting
- Forecasting
- Sharing within the company
- Sharing with the industry
- Sharing outside the industry
- Sharing in standardized format (e.g., STIX)

5.5 Services

5.5.5 Threat Hunting

Objective

To enable a proactive, iterative search through networks and assets to discover evidence of undetected threats.

Guidance

While security monitoring is the primary input to the incident management process, a solid threat hunting service can be a close second. Threat hunting can be performed manually by sifting through logs, or machine assisted. Threat hunting can be adhoc or structured. The more mature services will follow a well-established threat hunting framework, such as the TaHiTi framework.

The following capabilities should be maintained by this service:

- Hash value hunting
- IP address hunting
- Domain name hunting
- Network artefact hunting
- Host-based artefact hunting
- Adversary tools hunting
- Adversary TTP hunting
- Inbound threat hunting
- Outbound threat hunting
- Internal threat hunting
- Outlier detection
- Hunting coverage
- Leveraging of existing tooling
- Custom hunting scripts and tools
- Dedicated hunting platform
- Continuous hunting data collection
- Historic hunting
- Automated hunting
- Hunt alerting
- Vulnerability information integration
- Threat intelligence integration

5.5 Services

5.5.6 Vulnerability Management

Objective

To minimize the attack surface by identifying, evaluating, remediating and reporting on vulnerabilities.

Guidance

Vulnerabilities are weaknesses that can be leveraged by a threat actor to misuse a product or a service. This misuse can be relatively benign or translate into allowing an unauthorized user to cross network and privilege boundaries. Vulnerabilities are the building blocks of security incidents, often chained together by threat actor to achieve their ultimate objective. They are manifested, often, as a mistake in the code base of an application, one of its libraries, or as a misconfiguration. As a result, organization are often dependent on vendors to identify vulnerable versions of their application and provide patches or temporary work around.

Vulnerability management is not only about patching, but about maintain visibility on risk in the organization.

The following capabilities should be maintained by this service:

- Network mapping
- Vulnerability identification
- Risk identification
- Risk acceptance
- Security baseline scanning
- Authenticated scanning
- Incident management integration
- Asset management integration
- Configuration management integration
- Patch management integration
- Trend identification
- Enterprise vulnerability repository
- Enterprise application inventory
- Vulnerability Management procedures
- Scanning policy tuning
- Detailed Vulnerability Reporting
- Management Reporting
- Scheduled scanning
- Ad-hoc specific scanning
- Vulnerability information gathering & analysis

5.5 Services

5.5.7 Log Management

Objective

To ensure activities related to the continuous gathering, processing, storing and post-processing of the logs, performing regular quality analysis of the logs and tuning of derived parameters.

Guidance

Log Management has direct implication to achieving and maintaining the visibility required for the security monitoring service to operate correctly

The following capabilities should be maintained by this service:

- End-point log collection
- Application log collection
- Database log collection
- Network flow data collection
- Network device log collection
- Security device log collection
- Centralized aggregation and storage
- Multiple retention periods
- Secure log transfer
- Support for multiple log formats
- Support for multiple transfer techniques
- Data normalization
- Log searching and filtering
- Alerting
- Reporting and dashboards
- Log tampering detection
- Log collection policy
- Logging policy
- Data retention policy
- Privacy and Sensitive data handling policy

SECTION 6

FEDERATION & NSOC

6.1 National Security Operations Center

The vision for the National Security Operations Center (NSOC) is to create centralized visibility, coordination and accountability for the UAE defense against cyber security threats. The NSOC will provide assistance to each Sector SOC and organizational SOCs by offering services, and by driving collaboration between government, Industry and academia.

The NSOC acts as a center of information collection, analysis and dissemination and operates at the highest standards of this document. It is responsible for the national cyber awareness system, from which organizational and sector SOCs receive visibility on the overall state of cyber security in the UAE.

The NSOC maintains the UAE cybersecurity framework and policies. It periodically assesses compliancy within the Sector SOCs to this framework and policies on behalf of the CSC. The Sector SOC's will in turn assess the compliancy of their reporting organizations.

While the NSOC will directly support the most critical organizations in the UAE, its mission is also to protect, build and advise the cyber security readiness of the wider public and commercial sector. The NSOC strives to build the local security community, helping raise awareness, and offering education to organizations that need it. It is dedicated to establishing partnerships, providing resources and a feedback mechanism for all organizations within the UAE.

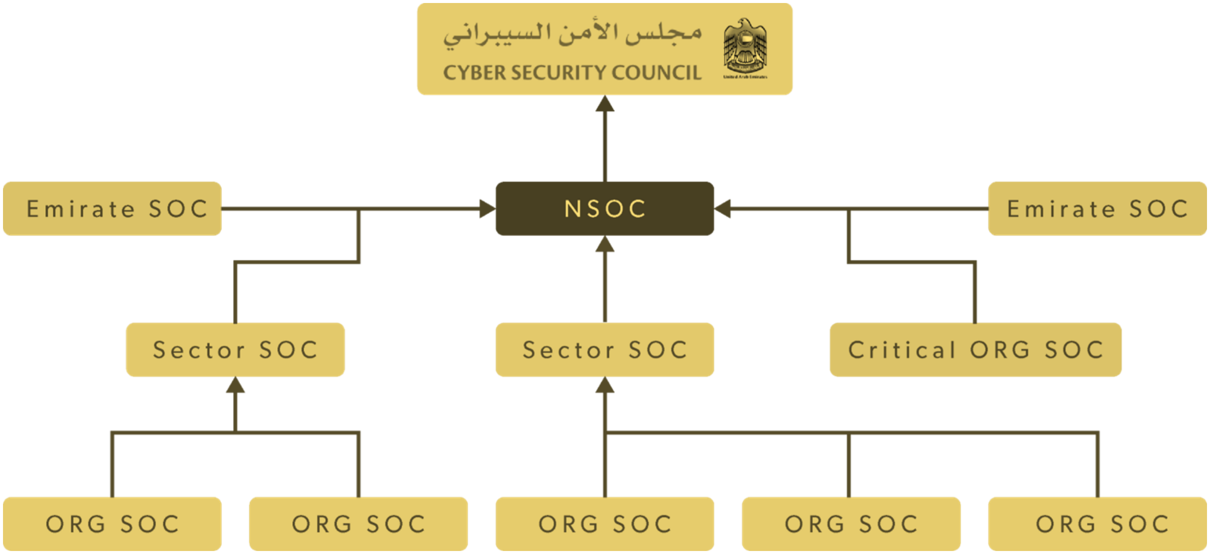
In all, the NSOC provides the following services:

- Situational Awareness
- Malware Reverse Engineering
- Security Analysis and Forensics
- Threat Intelligence
- Compliancy Assessment
- Cyber Security Advisory
- Cyber Security Education
- Incident Response Management
- Crisis Coordination
- Penetration Testing & Red Teaming
- Vulnerability Management
- Security Monitoring
- Threat Hunting

In case of significant cyber security incidents, the NSOC provides support on request to any organization that requests it.

6.2 Federation

Federation is principally about 2-way communication. Information must flow up, and guidance flow down. Sector SOCs and organizations that report directly to the NSOC will be expected to notify of all incidents they are aware of. In turn, all organizations reporting to a Sector SOC are obligated to report all Incidents they experience.



All incidents notification must contain:

- Local Priority
- Assigned Category Level
- Title
- Description
- Current Status
- Artefacts

These notifications must be communicated as the investigations unfold, and updates provided at an appropriate frequency. Expected notification time are from the moment the incident is detected.

6.2 Federation

Expected Notification Time

Incident Category	Mean-Time-To-Notify (MTTN)
Sector Emergency	30 min
Sector Incident	60 min
Localized Incident	1440 min

Expected update times

Incident Category	Mean-Time-To-Update (MTTU)
Sector Emergency	60 min
Sector Incident	120 min
Localized Incident	1440 min

To enhance detection capabilities of the NSOC, the following data will be shared with the Sector SOCs, and in turn with the NSOC

- Perimeter Firewall
- Internet facing Proxy
- Domain Name Resolution
- BGP Routing Information

SECTION 7

APPENDICES

7.1 Reporting Metric & Monitoring

Achieving the higher stages of maturity and capabilities requires a focus on metrics and Key Performance Indicators (KPIs). Only by developing, maintaining, and frequently reviewing the right metrics, can an organization engage in the type of continual improvement loop present in the optimizing level (5) of maturity and the defined level of capability (3). Here we focus on the KPIs attached to the key services and technologies found in a SOC.

Security Monitoring Metrics

KPI	Description	Purpose
# Assets Monitored	The number of assets that are witnessed in the logs, and security events	Identifies broadly the scope of activity that is being monitored. Potentially identifies issue in Change Management, or other technical issue if the number changes unexpectedly.
% Asset Database Completeness	The number of assets monitored, compared with the number of known assets in the asset management database.	Identifies delta in monitoring, or in the asset inventory.
# Events Monitored	The total number of security events monitored by the team. This includes any relevant security action, such as logging into an endpoint with a user account. These are not inherently suspicious events; they are the building blocks for use cases to extract the insight that leads to significant events and incidents.	Precisely identifies the scope of activity that is being monitored. This is the tide by which all other metrics should rise.
MTTD Mean-Time-To-Detect	The time before a significant security event is found, identified and alerted to the SOC	Monitors the security stack's ability to detect and relay the information to the end user.
MTTA Mean-Time-To-Acknowledge	The time between the moments a significant event is detected, and before a SOC analyst has acknowledged the alert, or a preventive measure has been automatically applied.	This identifies responsiveness. This may identify if the SOC monitoring is too busy, not attentive enough, or otherwise lack the urgency desired by the organization.
# Escalated False Positive	The number of significant security events that were identified as incidents.	This value can be indicative of independence and maturity your procedure and playbooks. However, this value can be overinflated by false positives that are easy to close, and present a problem at the use case management layer. This also indicates the organization's ability to stop threats in their early stage of development.

7.1 Reporting Metric & Monitoring

Security Monitoring Metrics

KPI	Description	Purpose
MTTN Mean-Time-To-Notify	The time between the moments a significant event has been acknowledged, and the time a notification is sent out to the relevant stakeholders. This applies only in cases where a notification is necessary, or an incident identified for escalation.	This is the metric by which the efficiency of the monitoring team is measured.
# Significant Security Events Processed	The number of significant security events that are identified, analyzed, triaged, and either resolved, or escalated.	This represents the analytical load on the monitoring team, in other words, how busy they are.
% Significant Security Events Closed	The number of significant security events that were eventually resolved by the monitoring team, without escalations.	This value can be indicative of independence and maturity your procedure and playbooks. However, this value can be overinflated by false positives that are easy to close, and present a problem at the use case management layer. This also indicates the organization's ability to stop threats in their early stage of development.
# Incidents Identified	The number of significant security events that were identified as incidents.	This value can be indicative of independence and maturity your procedure and playbooks. However, this value can be overinflated by false positives that are easy to close, and present a problem at the use case management layer. This also indicates the organization's ability to stop threats in their early stage of development.
# Escalated False Positive	The number of significant security events that were identified as incidents.	This value can be indicative of independence and maturity your procedure and playbooks. However, this value can be overinflated by false positives that are easy to close, and present a problem at the use case management layer. This also indicates the organization's ability to stop threats in their early stage of development.

7.1 Reporting Metric & Monitoring

Security Incident Management Metrics

KPI	Description	Purpose
# Incidents, categorized by Priority	The number of security events that were identified as incidents.	This represents the analytical load on the incident management team, in other words, how busy they are.
Mean Incident Dwell Time by Priority	The time between the moment the incident begun, and the time the affect asset is contained or remediated.	This represents the time the threat actor spent in your environment, and your organization’s actual exposure to that incident. The goal is always to reduce this particular figure.
MTTU Mean-Time-To-Update	Each incident may require communications and coordination checkpoints. This measure how accurate the incident management team is at keeping these checkpoints.	This is a measure of efficiency and completeness. Communication, particularly to stakeholders should be frequent and mandatory in critical case.
MTTR Mean-Time-To-Remediate	This the time between the moment an incident is declared, and the time to contain, or remediate the impact of that incident.	This can be the most misleading stats available to a SOC. Unlike IT incident, where prioritization can lead to reduce down time, the more critical a security incident is, the longer it may take to resolve. This metric should still be monitored, as it gives a view at the overall efficiency of the SOC at mitigating impact, but should be considered in context of the actual events.

7.1 Reporting Metric & Monitoring

Cyber Security Analysis & Forensics Metrics

KPI	Description	Purpose
# Sample Collected by type	The number of samples of any type, file, memory, disk image, packet capture, etc., that is collected for storage or processing	Precisely identifies the load and scope of activity that is being performed. This is the tide by which all other metrics in this category should rise.
# Sample Analyzed	The number of samples of any type, file, memory, disk image, packet capture, etc., that is collected for storage or processing	This is one of two values that represents the analytical load on the service, in other words, how busy the team responsible is. When compared to the overall sample collected, it provides visibility in the investigative depth permitted by resource restriction.
# IoCs Generated	The number of IoCs that are discovered through the analysis of samples	This is the measure of the value brought on by the security analysis service.
# Reports Generated	The number of reports created, outside of incident report.	This is one of two values that represents the analytical load on the service, in other words, how busy the team responsible is.
# Chain of Custody Failures	The number of times a review of the chain of custody reveals discrepancy, or the number of times such event is self-reported.	This provides a measure of quality and precision of the work performed by the analysts.

7.1 Reporting Metric & Monitoring

Threat Intelligence Metrics

KPI	Description	Purpose
# Feeds monitored	The number of feeds monitored, across all devices, whether centralized or not.	More is not always better, but maintaining visibility is important.
% Feeds Centralized	The percentage of feeds centralized, to monitor and protect across the entire security stack	Indicative of maturity of the threat intelligence team. This represents making the best use of all the data ingested.
# False Positive, by Feed	The number of times an IoC has led to a false positive significant event, or incident	This influences the confidence in the data source, and may be used to make educated decisions on how to benefit from using, or not using the feed.
# IoCs monitored, by Feed	The number of IoCs monitored across the security stack	This measures how much intelligence you are actively using
Mean Time To Age Out, by Feed	The length of time each IoCs is typically maintained in the feed.	IoCs relevance are based on time. Feeds that maintain shorter aging time, are usually more mature and useful.
# Incidents Identified	The number incidents that were identified from IoCs.	This value is indicative of the value of your threat intelligence program.
# IoCs Generated	The number of IoCs that were created as a result of the threat intelligence program.	A mature threat intelligence team will produce their own intelligence. This is a great metric of the value returned by the service.
# Recommendations Generated	The number of improvements to the overall security posture generated by the service.	This is value represents the value returned by the service.

7.1 Reporting Metric & Monitoring

Threat Hunting Metrics

KPI	Description	Purpose
# Threat Hunt Performed	The number of hunts performed	This represents the analytical load on the hunting team, in other words, how busy and productive they are.
Mean-Time-To-Hunt-Completion	This the time between the moments a hunt is started, and the time it is considered completed.	Similar to the MTTR, this can be misleading Hunts with larger scope will take longer, successful hunts may lead down long paths of pivoting and iteration. This metric should still be monitored, as it gives a view at the overall time spent on hunting, but should be considered in context of the actual events.
# Incidents Identified	The number incidents that were identified from threat hunts	This value is indicative of the value of your threat hunting program.
# Recommendations Generated	The number of improvements to the overall security posture generated by the service.	This is value represents the value returned by the service.

7.1 Reporting Metric & Monitoring

Vulnerability Management Metrics

KPI	Description	Purpose
Internal Patching Cadence	The number incidents that were identified from threat hunts	This value is indicative of the value of your threat hunting program.
Mean Vendor Patching Cadence	The number of improvements to the overall security posture generated by the service.	This is value represents the value returned by the service.

7.1 Reporting Metric & Monitoring

Perimeter Facing Vulnerability

Assets that are accessible directly from the internet, or otherwise sit in the DMZ require particular attention from a vulnerability management program. As a threat actor can run vulnerability scans, or attempt to exploit these assets directly, it is crucial that these vulnerabilities, particularly critical vulnerabilities, are patched with a higher urgency than non-perimeter facing vulnerabilities.

KPI	Description	Purpose
# Open Vulnerability, by criticality	The number vulnerabilities currently open across the organization, categorized by criticality.	This value is indicative of your existing exposure, and how busy your vulnerability management.
# Open Critical Vulnerability	The number of critical vulnerabilities currently open across the organization. This is an important subset of the previous metric.	This value represents the number of emergency issues that must be addressed.
# Recently Closed Vulnerability	The number of vulnerabilities that were closed over the last examined time period, typically a month.	This value represents the accomplishments of the vulnerability management team. It can be evaluated to provide an estimate of the effort, and return on that effort.
Monthly Delta, by categories	A running sum of the amount of positive, or negative change on the total count of vulnerabilities.	This derivative shows the overall progress of the vulnerability management program. Is the organization progressing toward a more, or less secure posture?
Weekly Delta	A running sum of the amount of positive, or negative change on the total count of vulnerabilities, on a smaller scope.	This derivative allows to anticipate the direction of progress, and to readjust more nimbly, to ultimately influence the previous metric.
Mean-Time-To-Remediate, by Criticality	The arithmetic average of the time between the moments a vulnerability is identified, to the moment it is remediated or patched.	This represents your true exposure time. It is the key metric of the service, and the one that must be constantly optimized.

7.1 Reporting Metric & Monitoring

Non-Perimeter Facing Vulnerability

KPI	Description	Purpose
# Open Vulnerability, by criticality	The number vulnerabilities currently open across the organization, categorized by criticality.	This value is indicative of your existing exposure, and how busy your vulnerability management.
# Open Critical Vulnerability	The number of critical vulnerabilities currently open across the organization. This is an important subset of the previous metric.	This value represents the number of emergency issues that must be addressed.
# Recently Closed Vulnerability	The number of vulnerabilities that were closed over the last examined time period, typically a month.	This value represents the accomplishments of the vulnerability management team. It can be evaluated to provide an estimate of the effort, and return on that effort.
Monthly Delta, by categories	A running sum of the amount of positive, or negative change on the total count of vulnerabilities.	This derivative shows the overall progress of the vulnerability management program. Is the organization progressing toward a more, or less secure posture?
Weekly Delta	A running sum of the amount of positive, or negative change on the total count of vulnerabilities, on a smaller scope.	This derivative allows to anticipate the direction of progress, and to readjust more nimbly, to ultimately influence the previous metric.
Mean-Time-To-Remediate, by Criticality	The arithmetic average of the time between the moments a vulnerability is identified, to the moment it is remediated or patched.	This represents your true exposure time. It is the key metric of the service, and the one that must be constantly optimized.

7.1 Reporting Metric & Monitoring

Log Management

KPI	Description	Purpose
% Coverage, by log source	What percentage of all devices generating these particular log source, is collected?	This represents the overall visibility of downstream SIEM/XDR solution
Accuracy, by log source	Percentage of logs that are being produced as expected, and with the correct data.	This represents the reliability of the logs being ingested. It is not uncommon for logs of different manufacturer to differ in their interpretation of an RFC. Over time, issues can also cause the log to become inaccurate, such as when a data source's internal timer becomes inaccurate.
Log Ingest Availability, by log source	Percentage of time the data is collected and processed on time, within the acceptable delay.	Prompt an accurate security monitoring depends on the availability and timeliness of the information. As such, this represents a key indicator for the log management service as a whole.

7.1 Reporting Metric & Monitoring

Use Case Management

KPI	Description	Purpose
# of Use Case	Overall Number of Use Case in deployment	While more is not always better, this is particularly useful metric while actively developing UCs toward a level of desired readiness. On the opposite end of the spectrum, it can help identify a scenario where too many UCs may imply a lack of efficiency in the overall management.
True Positive Rate, by UC	The number of true positive events divided by the sum of true positive and false negatives. This is sometime referred to as the Sensitivity.	This measure gives the hit rate of the UC. How confident are we that if an event occurs, we will detect it?
False Positive Rate, by UC	The number of false positive events divided by the sum of false positive and true negatives. This is sometime referred to as the Specificity.	This measure gives the miss rate of the UC, or its false positive tolerance. How confident are we in our interpretation of the event is correct? How much false positives are we willing to accept, to decrease the likelihood of ignoring a true event?
UC Periodicity	The number of UC running at a certain category of periodicity: Near Real-Time (<5min) # ~15 min # ~Hourly # ~Daily # ~Weekly # ~Monthly	This measure helps plan out the performance impact of the UCs

7.1 Reporting Metric & Monitoring

SIEM/XDR

KPI	Description	Purpose
SIEM/XDR Capacity (Disk Space)	The percentage of disk utilization	This measure is an indication of the capacity of the infrastructure to support incident detection.
SIEM/XDR Performance (RAM)	The percentage of RAM utilization	This measure is required to plan out the periodicity and efficiency of UCs. This measure also helps anticipate upgrade requirements
SIEM/XDR Performance (CPU)	The percentage of CPU utilization	This measure is required to plan out the periodicity and efficiency of UCs. This measure also helps anticipate upgrade requirements
License Utilization	The percentage of license utilization	This measure helps anticipate upgrade requirements
SIEM/XDR Availability	The percentage of uptime for the SIEM/XDR platform	This measure is directly reflective of the ability to perform security monitoring.

7.1 Reporting Metric & Monitoring

IDPS

KPI	Description	Purpose
True Positive Rate, by Security Device	The number of true positive events divided by the sum of true positive and false negatives. This is sometime referred to as the Sensitivity.	This measure gives the hit rate of the Security Device. How confident are we that if an event occurs, we will detect it?
False Positive Rate, by Security Device	The number of false positive events divided by the sum of false positive and true negatives. This is sometime referred to as the Specificity.	This measure gives the miss rate of the Security Device, or its false positive tolerance. How confident are we in our interpretation of the event is correct? How much false positives are we willing to accept, to decrease the likelihood of ignoring a true event?

7.1 Reporting Metric & Monitoring

Security Orchestration, Automation and Response (SOAR)

KPI	Description	Purpose
Total # Playbooks	The number of soar playbooks	This represents how many procedures are either partially or fully automated.
# of Fully Automated Playbooks	The number of soar playbooks that do not require manual automation	This represents how many procedures are fully automated. This is a measure of how automated the environment is.
Successful Action Rate, by Playbook	The percentage of time the soar performed an activity correctly, when activated to do so.	This measure indicates how well-maintained playbooks are, and how reliable the SOAR has been.

Operational Reports

Operational reports should include daily and weekly iterations covering all relevant metrics listed. The intended audience is technical, and is expected to make use of the data to identify and address issues with the overall Security Operations Centre.

Executive Reports

Executive reports should paint a clear, succinct picture of the past, current and future state of security for the organization. They should cover the following:

- Vulnerabilities - What are we exposed to?
- Security Events & Monitoring - What malicious activity did we observe?
- Incidents - What did we do about it?
- Threat Intelligence - What should we be ready for?

Incident Reports

Covered in Section 5

7.2 Cloud Considerations

The growing popularity of cloud deployment, and the clear financial advantages they propose, make it difficult to ignore as a common variable in SOC planning and compliancy. However, the cloud is a complex subject. Cloud computing covers multiple service models (SaaS, PaaS, IaaS, etc.) and multiple deployment approaches: private, public, hybrid and community. Each models and service bring their own security concerns and particular architectural challenges. This has a couple of implications given the typical Shared Responsibility Model implemented in these environments, splitting the security risks and responsibilities between cloud providers, and their customers.

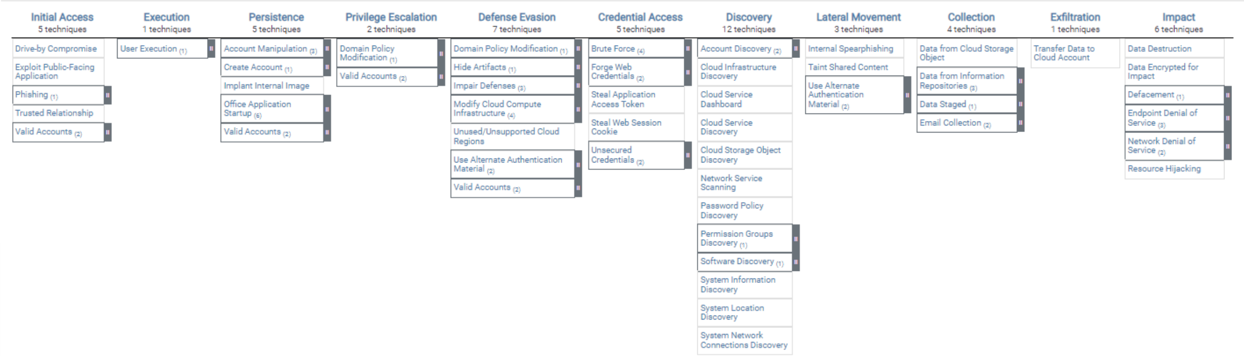
While the provider is ultimately responsible for the security, risk and exposure of the infrastructure, data and applications, the accountability for the security of the code, the implementation of the application, and the implementation of strong authentication, rests with the customers. Major security concerns particular to cloud deployment include:

- **Insider Threat:** While perhaps one of the most common threat vectors in any environment, it is particularly challenging in a cloud environment where physical access to the data is surrendered to the provider.
- **Data Isolation Failure:** As infrastructure is shared between customers in a cloud deployment, the possibility that data could be viewed by another customer, remains a significant concern.
- **Hypervisor Compromise:** While mostly anticipatory, the concern exists that a compromise of the hypervisor in a cloud infrastructure provider, would lead to full access to organization private data.

7.2 Cloud Considerations

From a SOC perspective, the challenge with the concerns above is the lack of visibility, and the dependence on the cloud provider for response. Forensic capabilities are significantly degraded, if not typically non-existent in a commercial cloud deployment. There is typically no access to raw disk or live memory capture for deeper technical analysis. As such it is important to carefully select data that will uploaded to cloud infrastructure outside of the direct control of the organisation, and to consider the deployment an untrusted or semi-trusted zone, to which all access is monitored through a single capture and monitor point, such as a Cloud Access Security Broker (CASB). A CASB is a software that sits between the Customer's Edge and the Cloud Edge, capturing, enforcing and monitoring communications between the two environments.

The logs from the CASB, will provide one of the most valuable data sources to a SOC. It will also provide the SOC the ability to enforce or terminate communications to a cloud deployment, representing perhaps the best. Where cloud is deployed Use cases should be aligned to the MITRE ATT&CK Cloud Matrix.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	1 techniques	5 techniques	2 techniques	7 techniques	5 techniques	12 techniques	3 techniques	4 techniques	1 techniques	6 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Data Destruction
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery	Taint Shared Content	Data from Information Repositories (3)		Data Encrypted for Impact
Phishing (1)		Implant Internal Image		Impair Defenses (3)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data Staged (1)		Defacement (1)
Trusted Relationship		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Steal Web Session Cookie	Cloud Service Discovery		Email Collection (2)		Endpoint Denial of Service (3)
Valid Accounts (2)		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Unsecured Credentials (2)	Cloud Storage Object Discovery				Network Denial of Service (2)
				Use Alternate Authentication Material (2)		Network Service Scanning				Resource Hijacking
				Valid Accounts (2)		Password Policy Discovery				
						Permission Groups Discovery (1)				
						Software Discovery (1)				
						System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

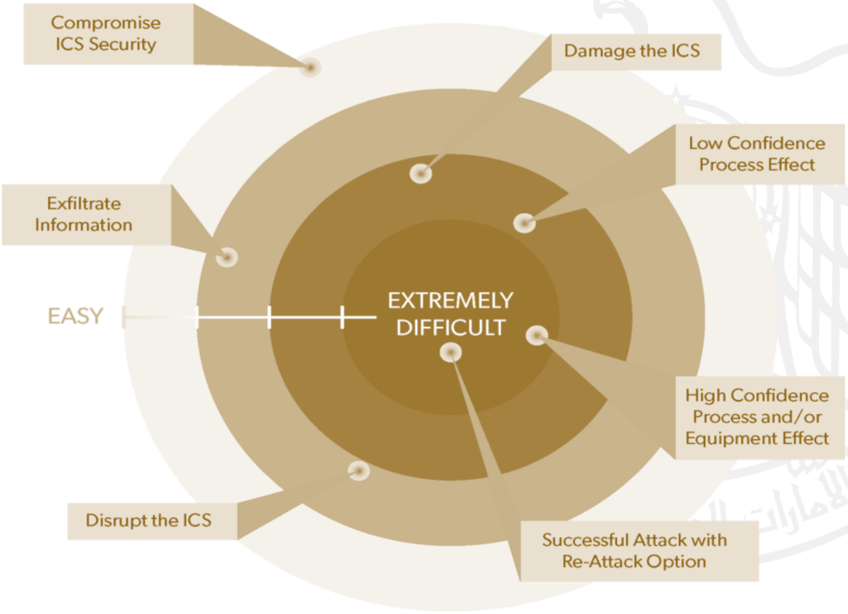
7.3 ICS/OT Considerations

The growing prevalence of industrial control systems (ICS) and other operational technologies (OT) is making it difficult to continue treating it as a separate niche space, particularly as more and more organizations seek to connect these systems to their traditional IT, exposing them to remote threat actors. A modern SOC must recognize both the similarities in monitoring and protecting an ICS/OT network, and its differences.

The space for forensic and detection technologies directly geared for the ICS/OT is young and sparse in capabilities. As such, the most cost-effective approach is often to isolate and better control access to the ICS/OT network itself, leveraging the SOC's large arsenal of traditional IT security capabilities. In addition, knowing and tracking the ICS/OT's network implementation becomes paramount.

One misunderstood aspect of ICS/OT attacks is that they are in fact quite complex due to the bespoke nature of all deployments. While the market for PLCs is concentrated to a few large players, there are over 250+ ICS protocols, and vast number of different types of sensors and actuators. Architectures and implementation are most often customer specific, with interactions between the various parts of the overall system, difficult to fully comprehend.

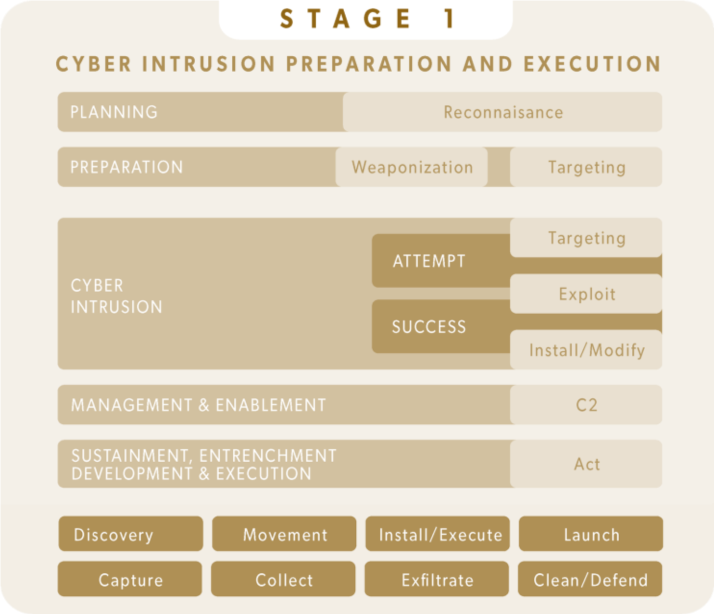
The pain this complexity creates is shared by both defenders and threat actors alike. Any threat actors which intend on leveraging their access must spend a large amount of time inside of the network studying its function and composition, before an attack can be planned, tested and then carried out successfully.


Compromise ICS Security
Damage the ICS
Low Confidence Process Effect
Exfiltrate Information
EASY
EXTREMELY DIFFICULT
High Confidence Process and/or Equipment Effect
Disrupt the ICS
Successful Attack with Re-Attack Option

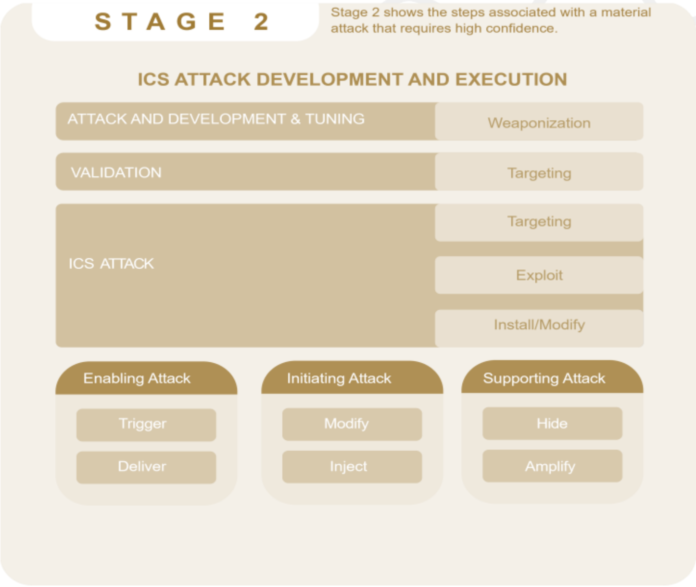
ICS Attack Difficulty

7.3 ICS/OT Considerations

As such, we can conceptualize ICS attacks into two separate phases, with distinct kill chains:



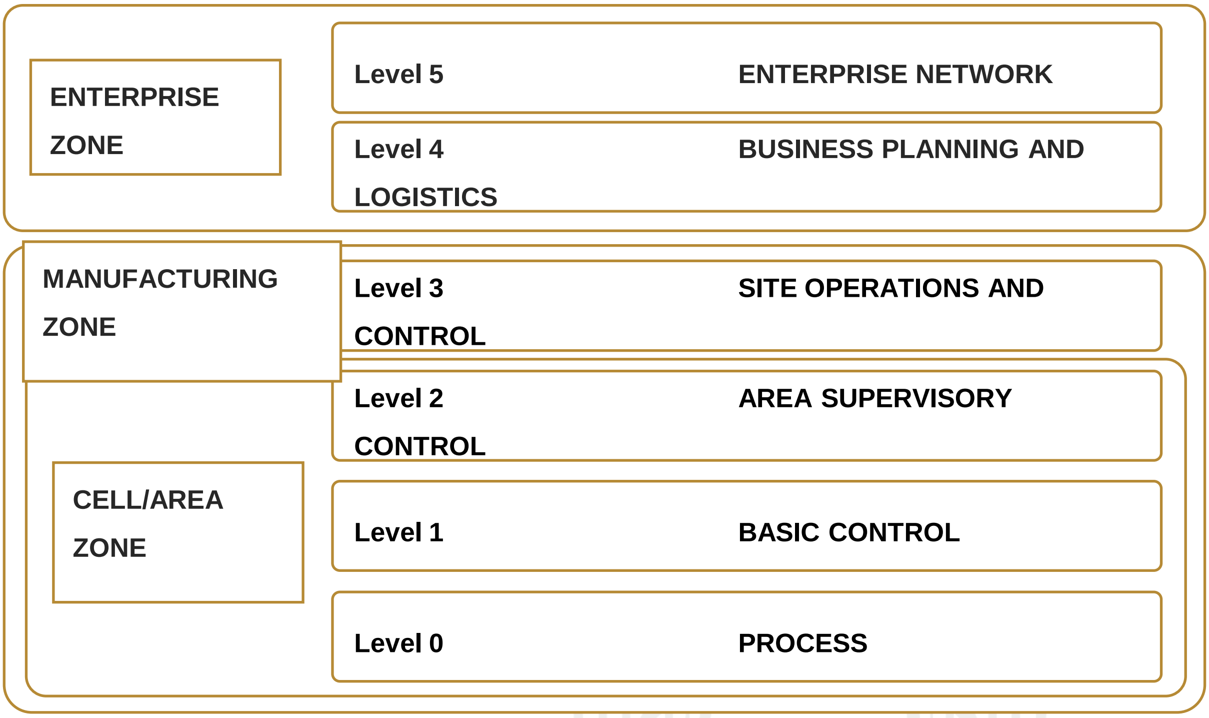
The first phase represents a standard IT security incident, where a threat actor establishes their access to the ICS/OT network, and then proceed to study and plan their next phase of attack. This offers the best chance of intercepting and stopping the attack. It is also the least complex challenge, as this aligns with the traditional detection and protection stack, and with the existing process and services of the SOC.


Stage 2 shows the steps associated with a material attack that requires high confidence.

7.3 ICS/OT Considerations

The second phase is more of a challenge, as it introduces the limitations and particularities of the ICS/OT environment into the detection and incident management approaches. In this phase, the threat actor is leveraging their undiscovered access to observe, modify or destroy the system.

Another advantage SOC have when dealing with ICS/OT networks is that they are relatively static. Once deployed, they do not change with the same frequency that a normal IT network does. As such, gathering an accurate baseline of network traffic, and node configurations becomes an essential. It is an expectation that all critical infrastructure related ICS/OT deployment, invest in a professional ICS asset identification tool. This step is also strongly recommended for non-critical infrastructure deployment, with open-source projects available as an alternative.



ENTERPRISE ZONE

Level 5 ENTERPRISE NETWORK

Level 4 BUSINESS PLANNING AND LOGISTICS

MANUFACTURING ZONE

Level 3 SITE OPERATIONS AND CONTROL

CELL/AREA ZONE

Level 2 AREA SUPERVISORY CONTROL

Level 1 BASIC CONTROL

Level 0 PROCESS

7.3 ICS/OT Considerations

A Modern SOC should tailor each of its traditional services to their ICS/OT deployment, with the following considerations:

Security Monitoring

- Data collection points & network chokepoints must be developed and closely monitored.
- Changes in configurations or architecture of the ICS/OT network must be closely monitored.
- Transition into the Incident Management Process should be limited and go through approval of senior management. Incident response on ICS/OT environment is particularly time consuming and may cause potential interruption to the system. As such, this decision should be taken more carefully than on an IT network.
- Arguably, it may not be recommended to place monitoring devices inline on ICS/OT network due to the inherent risk to operations. Great care should be exercised in approaching this question.

Incident Management

- The forensic tooling for ICS/OT network is very limited as the space is still heavily researched
- Programmable Logic Controllers (PLCs), sensors and actuators all contain small live memory, and hard disk size, which simplify hardware requirement
- Attempts to acquire data will likely crash the device and should be assumed to cause interruption whenever attempted.
- The vast majority of incidents occur directly on the Human-Machine Interface (HMI) systems. As this is typically a legacy windows operating system, it opens the door for traditional incident response

Threat Intelligence

- Specialty ICS/OT threat feeds should be acquired
- Identifying and limiting the exposure of information on the ICS/OT deployment on the internet is critical in increasing the dwell time of a threat actor.

7.3 ICS/OT Considerations

Threat Hunting

- Customized kill chains must be developed for the specific ICS/OT deployments
- Threat hunting should be performed on these kill chain, with greater frequency than on normal IT networks
- One of the key outputs of threat hunting becomes the identification of baselines, and the anticipated deviation that a TTP would cause.
- In environments critically sensitive to interaction, creating a replicate environment (or reference network) in a virtualized Cyber Range becomes essential to threat hunting exercises.

Vulnerability Management

- Greater care must be taken when planning and reporting on patching in these environments. An estimated 80% of ICS vulnerabilities are not actionable, or unnecessary due to a more serious condition such as an inherent lack of security from a particular device. For example, remote execution flaws are irrelevant on a device that allows anonymous authentication by design. Since patching often implies potentially dangerous interruption to the system, the vulnerability management service should carefully identify only the most critical case and the case where the value return is greater than the risk and availability loss to the system.
- Attack path management, an approach focused on identifying the natural chokepoints in the pathway to a successful attack, is particularly relevant to OT environments. This approach allows to limit the scope and complexity of patching and hardening, required to build a more robust infrastructure. An OT-ready SOC, MDR or Fusion Center must implement this approach to efficiently manage the exposure of their environment.

Use Case Management

- Use cases need to be extended to cover the ICS/OT MITRE Att&ck framework
- Use cases must also be designed to include the rapidly changing smart sensor / IoT device environment within OT networks

7.4 Reference Documents

International Standards

The following table outlines the international sources referenced in this document.

Authority/Body	Document
SOC-CMM	SOC-CMM
MITRE	ATT&CK

7.5 Abbreviations

Usage	Description
SOC	**Security Operations Center**
CII	Critical Information Infrastructure
NSOC	National Security Operations Center
C&C	Command & Control Server
CIA Triad	Confidentiality, Integrity, and Accessibility
ICS	Industrial Control Systems
OT	Operational Technology
IoT	Internet of Things
SIEM	Security Incident Event Management
XDR	Extended Detection & Response
CMMI	Capability Maturity Model Integration
SLA	Service Level Agreement
KPI	Key Performance Indicator
PIA	Privacy Impact Assessment
FTE	Full-time-Employee
HVAC	Heating, Ventilation and Air Conditioning
TTP	Tactics, Techniques, and Procedures
IDPS	Intrusion Detection and Prevention System
IoC	Indicators of Compromise
NBA	Network Behavior Analysis
NAC	Network Access Control
DLP	Data Leakage Protection
EDR	Endpoint Detection & Remediation
API	Application Programming Interface
DDoS	Distributed Denial of Service
WAF	Web Application Firewall
CWPP	Cloud Workload Protection Platform
CASB	Cloud Access Security Broker
CSPM	Cloud Security Posture Management
ISP	Internet Service Provider
SOAR	Security Orchestration, Automation and Response
IAM	Identity Access Management
IR	Incident Response
RACI	Responsible, Accountable, Consulted, and Informed
TTP	Tactics, Techniques & Procedures
SOP	Standard Operating Procedures