SOC-Py Project for Paraguay

August 2018

CyGov for IDB: Nir Peleg, Gal Shmueli
npeleg@cygov.co, gshmueli@cygov.co

Document Administration

Lead Assessors: Nir Peleg, Gal Shmueli

Approved By: Yair Solow

Version	Date	Notes
1	29/06/2018	Drafting
2	19/07/2018	Approved by Cygov
3	30/07/2018	Approved by IDB
4	01/08/2018	Delivered
5	16/10/2018	Corrections after presentations in Paraguay

Table Of Content

Preface

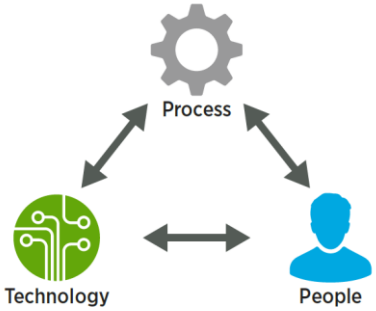
Cyber security The National Secretariat of Information Technology and Communication (SENATICS), is aiming to launch its project of Cyber security Operations Center Paraguay (SOC-Py) as a key piece of the framework in Paraguay's Cyber security Strategy. The **SOC-Py** is considered an important pillar and commitment for implementing the National Cyber security roadmap.

This document of the SOC-Py project is a design and plan advisory team of IDB, performed by the CyGov cyber security firm. This document summarizes the design, plan and recommendations of the CyGov advisory team after extensive discussions with the SENATICS team as well as many other stakeholders in the project.

Security Operation Center Overview

A Security Operations Center (SOC) is a central pillar for improving and implementing continuous cyber security and compliance by consolidating key security personnel, event data and technologies in a centralized location. Security visibility, incident detection and response can be greatly accelerated and enhanced as a result of this consolidation.

Building a SOC is not a trivial project as it requires a substantial investment both upfront and on an ongoing basis in **people, processes and technologies**. However, the benefits of having an improved security posture greatly outweigh the costs. If a security operation center is properly designed and built, it would be the basis for constant improvement towards advanced models of cyber security such as proactive cyber defense and intelligence driven defense.



SOC and Managed Services definitions:

Security operations centers (SOCs) have historically been adopted by large organizations that require centralized and consolidated security operations, primarily for reasons of efficiency and costs. The evolving and expanding threat landscape has changed the cyber security model where prevention on the perimeter is not enough. Cyber defense has shifted from "Prevent" to "Detect and Respond", and the need to design an “adaptive security architecture” for protection against advanced attacks has prompted increased adoption of SOC architectures by a broader base of users. These users are reoriented to focus on the detection, response and prevention of cyber security incidents and threats.

Gartner defines a SOC as a dedicated team, which often operates in shifts, open 24 hours a day and has a dedicated and organized facility to prevent, detect, evaluate and respond to cyber security threats and incidents while evaluating and complying with cyber security policies.

A managed security service (MSS) and managed Detection and Response (MDR) are models which offer shared security services originating in the SOC and provided to other organizations as a **SOC as a Service**.

The Main SOC services include:

- Management and maintenance of security devices
- Analyzing threats, vulnerabilities and alerts
- Monitoring and security audit
- Management of cyber security incident response
- Situation awareness and reporting
- Security compliance management
- Security training
- Security information sharing

There are three main relevant models for building and implementing the SOC-Py project:

1. A dedicated SOC for an organization: This model relates to a dedicated service that manages the cyber security of an enterprise. A good example of

this models are Banks SOCs which manage 24/7 security monitoring of the entire bank systems and networks.

2. A dedicated SOC-MSS: A centralized shared service providing security services for other organizations that are enrolled to the service. A good example is commercial MSS providers who provide a shared security service for customers and offer full security management and compliance as a service.
3. A Dedicated SOC-MDR: A centralized SOC with shared services that are focused on threat detection monitoring and incident response capabilities. In this model the SOC-MDR manages two main services: Detection, situation awareness and incident response as a service. The SOC is not responsible for managing the organization's security (i.e. system and security administration).

Our recommendation is to continue with option 3: Dedicated SOC-MDR.

SOC-Py Project Objectives and Scope:

The SOC Project has the following main objectives:

1. **Managed Detection and Response**: The SOC-Py will offer managed security services focused on detection, situation awareness and response **for the government administrations** based on the dedicated SOC-MDR model. The following services will be planned: Security monitoring, threat and vulnerability management, operating security systems and sensors, incident response (mainly remotely).

2. **Enhance CERT-Py capacities and services**: Work closely and support the CERT-Py to empower its security services and **create security synergy** between **public and private sector**. The concept of the SOC with the CERT is to create critical mass of personnel, knowledge and security operations under the same roof, as the national center for cyber security.

3. **A training center** for professionals' - **Cyber Hub of Knowledge and Training**: Courses and hands on experience from real-life incidents, threats and events analysis experience. Create and maintain a knowledge base for the lessons learned from past events as well as the changes to current standards, policies and procedures. The training center will then train professionals according to those updated materials.

Critical Pre-Conditions for Success:

1. The establishment of the SOC-Py project will include definitions and requirements of the three interrelated pillars of **P**rocess-**P**eople-**T**echnology. **It is a critical to define and establish <u>all the three pillars</u> in order for the critical mass of this project to be operationally successful.**
2. In order for a SOC-MDR to be effective, there are minimum baseline security requirements that are expected from the administrations who are the 'clients' of the service. In addition, a relevant security/IT point of contact (POC) who is committed to work with the SOC team and procedure needs to be defined in each administration.

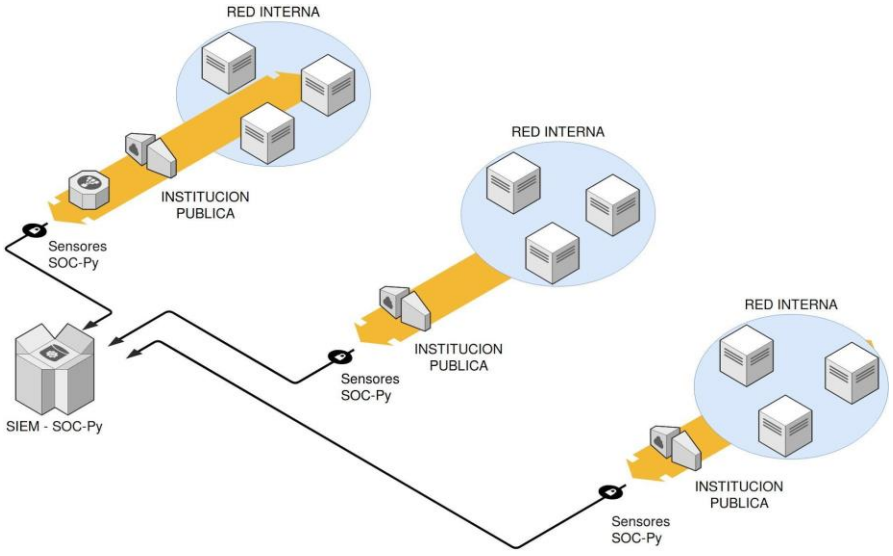
Process Definitions

There are three main processes that need to be defined:

Process 1: Threat Modelling and Visibility Coverage Plan

The SOC-Py aims to defend the government networks and digital assets with advanced detection and response services across the government networks.

The general architecture of the SOC is to deploy sensors/collectors at each relevant government office in order to create continuous visibility and optimal coverage for detection of security events.



The following list summarizes the recommended coverage plan after analyzing the main digital assets (existing and planned) of the government.

The first list relates to collection from the various institutions, mainly with log collectors that will be managed by the SOC. The second part is monitoring central government assets owned or managed by SENATICS. These assets, such as: the government cloud, information highway (IIS) and potentially a central DNS resolver and DNS filter are highly recommended to monitor.

1. **Administration/ Institution: A need to adapt to each institution**
    - IDS/IPS – Network (PfSense as an example)
    - Anti-virus systems logs
    - Window system event logs (collector)
    - Active directory logs (if used)
    - Local Mail-server (if used)
    - Any syslog entries (if generated)
2. **Central / SENATICS:**
    - Government cloud logs
    - Government WEB sites access logs
    - Administrative access (VPN, SSH)
    - Active directory (SENATICS)
    - DNS monitoring central government
    - Mail server logs (anti-spam)
    - E-mail security gateway
    - DDoS Protection system on WEB sites (there are plans to purchase Imperva WAF)
    - Information exchange system logs (SII) – sistema intercambio de informacion
    - Application logs – customization logs

Process 2: SOC-CERT Management

Procedure Definitions

There are several main procedures that need to be defined and take place for the SOC system and services. These procedures should be defined for the both the SOC as

well as for the “customer” end. The definition should be led by the SOC team and shall be coordinated with its clients:

No	Procedure	SOC Procedure
1	Monitoring Procedure	The true value of collecting, correlating, and analyzing log data is that it gives you the ability to find the "signal in the noise". Key indicators of a compromise can be found within user activity, system events, firewall accept/denies etc. In addition, specific sequences and combinations of these events in specific patterns can also signal an event that requires your attention. The key to success in this stage is having a way to classify each event quickly – the 'Triage process', so that you can prioritize and escalate critical events that require additional investigation.
2	Notification Procedure	One of the SOC missions is to produce alerts and notifications to the 'customer's POC. A procedure to effectively communicate with email, mobile, home, chat etc. is needed in order to react fast. **Time is crucial**! There is also a need to log all notifications in a ticketing log system. In addition, a clear priority needs to be defined for each notification. The SOC will manage and maintain contact lists for notifications.

3	Escalation Processes	Escalation usually takes place after Tier 1 **triage process** or as a result of an external incident alert coming to the help desk. Any tier 2 incident handling should be at the discretion of the SOC manager. Escalation from Tier 2 should be managed by the SOC manager.
4	Incident Management	Incident management is the process of managing an incident or a threat by a Tier 2 level analyst. The process of incident management aims to add context to IOCs (indicator of compromise), investigate artifacts and recommend steps to respond, contain and recover from the event. Incident management procedure should also define clearly when the event should be escalated to CERT-Py.
5	Dashboard Creation	Dashboard creation is the process of building customized KPIs (Key Performance Indicators) that serves a real time situation awareness of events, warnings, behaviors and performance security and network assets. The security dashboard should be customized for every customer in order to be productive and efficient.

6	Shift Logging	This procedure is important for the internal management of the SOC and switching between shifts and personnel. It is highly important to manage event logs for smooth handovers in order to maintain high-capacity and continuous operations, consistency, traceability and knowledge management.
7	Reporting	As a primary function, regular reports will need to be generated and provided to different audiences within the organization and with its customers. Usually, a weekly report is prepared for incidents, detailing the activity within the SOC. These reports can be delivered to management and other members on the core escalation contact list as well as other relevant stakeholders.

SOC-Py and CERT-Py Working Together

The recommended implementation model is for the SOC-Py and CERT-Py to work together under the same roof as it will achieve the following benefits:

1. Creating a critical mass of personal, experts and knowledge working together under the same roof that will enable them both to collaborate in tasks and capacity.
2. Building a national and governmental security hub operation center.
3. Information sharing of threats, incidents and best practices between the public sector (government networks) and the private sector (represented by the

national CERT). This will create better collaboration for protection of critical infrastructure.

The Incident handling (Tier 2, Tier 3) of the CERT and SOC should be merged in order to have the adequate capacity to manage several simultaneous events efficiently with the same security professionals and personnel.

We **strongly recommend** that the Tier 1 and Tier 2 personnel allocated to the SOC will be fully committed to security operations only and not for administrative duties or capacity building duties.

Process 3: SOC-Py Services Model

The SOC-Py project is planned to give Managed Detection and Response security services (MDR) to many other government administrations (defined as 'customers'). As such, there is a crucial need to define a contract/agreement between the SOC and its 'customers' in order to set expectations, responsibilities and separation of duties.

The following table will define the recommended roles and responsibilities for the SOC model:

Characteristics	SOC – MDR Responsible	'Customer' Responsible
Security Event Log and Context Sources with Threat Analysis	Yes	POC for alerts

Detection	Yes	POC for alerts
Remote Device Management	No Only SOC sensors	Yes
Incident Response	Yes Mainly remotely	POC for response
Incident Containment	Only recommendations	Yes
Compliance Reporting	No Supportive data and reports	Yes

People

Hiring the **right amount of people with the required qualifications** and skills is critical in building and running a successful SOC. A diverse set of personnel is required, each with different skills, qualifications, personalities and pay grades. It's also important to make sure that on-the-job and **ongoing training occurs**. The SOC personnel need to be collaborative in nature so they can work as a security team to remediate incidents.

Following is the staff definition table:

Role	Description	Skills	Responsibilities
Tier 1 Security Analyst	Event monitoring, triage of events	Sysadmin skills, programming skills	• Reviews the latest alerts and threats to determine relevancy and urgency. • Creates new troubleshooting tickets for alerts that signal an incident and require Tier 2 / incident |response review.
Tier 2 Security Analyst	Incident responder, root-cause analysis	Experienced analysts, incident management skills	• Reviews troubleshooting tickets generated by Tier 1 analyst(s). • Leverages emerging threat intelligence

			(IOCs, updated rules, etc.) to identify affected systems and the scope of the attack. • Reviews and collects asset data (configs, running processes, etc.) on these systems for further investigation. • Determines and directs remediation and recovery efforts.
Tier 3 Expert Security	Subject matter expert, threat hunter	Penetration testing, reverse engineering, system internals	• Reviews asset discovery and vulnerability assessment data. • Uses latest threat intelligence to explore ways to identify stealthy threats that may have found their way inside your network without being detected.
SOC Manager	Operations and	Security expert with strong management	• Supervises the activity of the SOC team.

	management of the SOC	and communication skills	• Recruits, hires, trains, and assesses the staff. • Manages the escalation process and reviews incident reports. • Develops and executes crisis communication plan to CISOs and other stakeholders.

Practical recommendation and cost estimations for SOC-Py:

The following table summarizes our practical recommendations for human resources based on our discussions and data provided by the SENATICS team.

Role	Qty	Month cost[$]	Annual cost[$]*
Tier 1	6	500	39,000
Tier 2	2	850	22,100
Tier 3	2	1,200	31,200
SOC Manager	1	1,200	15,600
Total	**11**		**107,900**

*It is assumed an additional 1month salary every year as an acceptable bonus.

We've made the following recommendation assumptions:

1. The price estimations are based on discussions with SENATICS and local salaries that are relevant to the region and practical recruitment.

2. We recommend to add additional $5K per person per year for training and professional improvement purposes.
3. The plan is to move to 24/7 coverage with a factor of 1x6 staffing for constant Tier 1 watch.
4. There is a need to train the Tier 1 and Tier 2 staff, therefore an internal training period of at least 6 months is estimated before the SOC will be fully operational 24/7.
5. It is important to retain the work force for at least 2 years in order not to sink into an inefficient cycle of constantly training new employees.
6. Tier 3 personnel will be challenging to recruit, therefore there will be a need to hire external professional service experts for Tier 3 duties. This should be planned as part of the project budget.
7. A critical minimum staff of 6 people (Tier 1 (x3), Tier 2 (x2), Manager (x1)) are needed in order to start the initial operations of the SOC.
8. **First phase** of operation should begin with shifts of 8 hours per day, 5 days a week for at least 6 months. **Second phase** should move to being an operational SOC 24/7.

Technology and Architecture

The Central Technology that is the Basis for SOC Operations is the SIEM Platform.

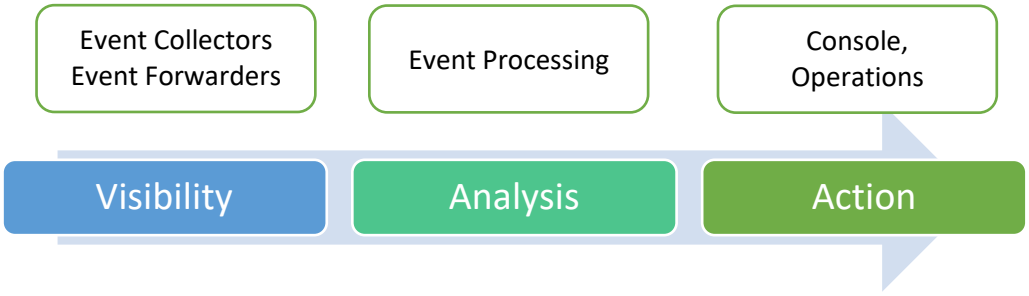
Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events originating from multiple sources.

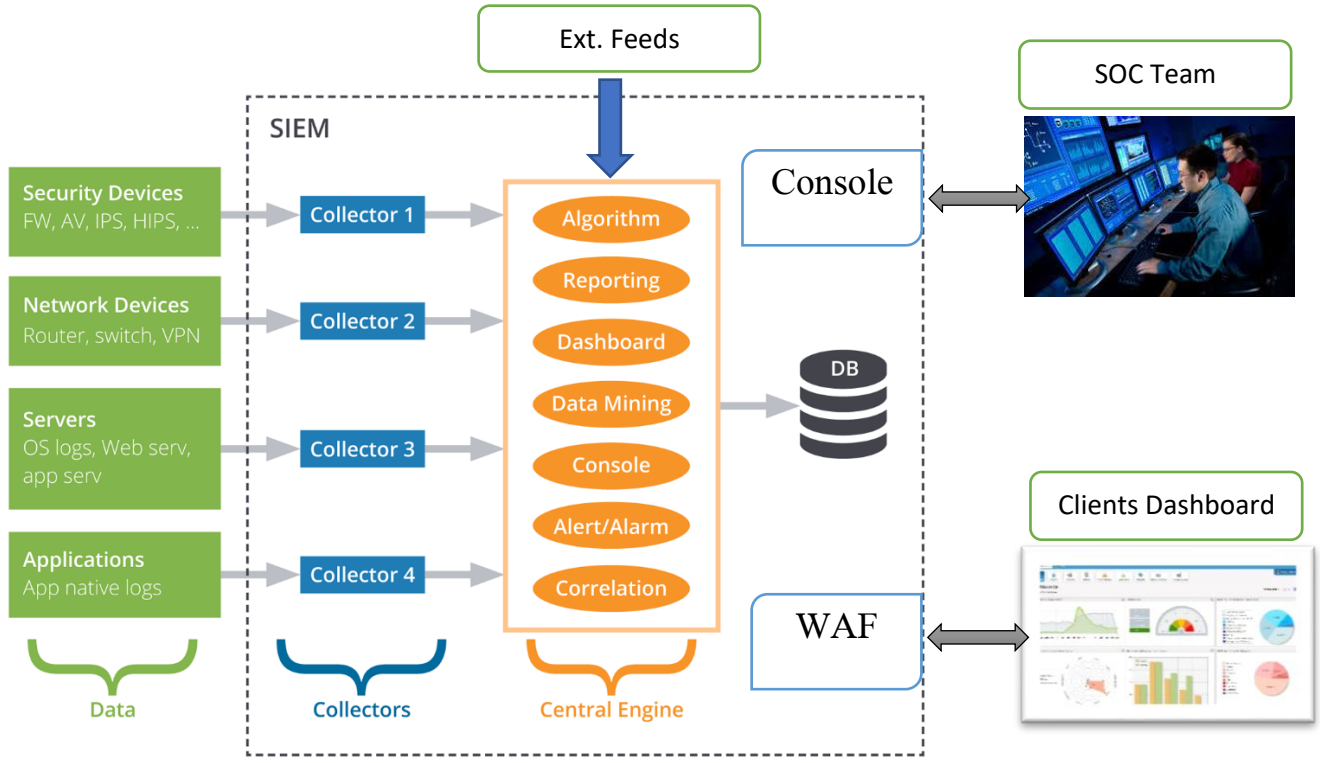
The main features that advanced SIEM platform should contain are as follow:

- **Collect** logs from standard security sources
- **Enrich** logs with supplemental data
- **Incorporate** Global Threat Intelligence (e.g. Black Lists)
- **Correlate** - Find the proverbial needles in the log haystacks

- **Investigate** - Follow up and analysis across all data repository
- **Document** - Standard operating procedures, service level Agreements, troubleshooting tickets
- **Create** - Build white lists, new rules, new content
- **Alerts** management and creation
- **Dashboards** and Visual reports and for situation awareness
- **Automation** of actions, procedures and operations

SIEM General Architecture and flow:





Data Collectors: Virtual software that is installed on the customer's network/segment and collects data from all potential resources. Typically, syslog format is being used as a common format. The data collectors' packs and securely sends the data to the central engine.

Central Engine: The central processor that processes the data in order to produce effective and actionable results, alerts and reports.

DB: Central database for all logs and unstructured data to create central repository.

Console: The main interface for all analysts and administrators working internally in the SOC, command and control, management, scripting and user visual interface.

WAF for WEB publishing: A security interface for web publishing data and dashboards to external users. The Web Application Firewall is crucial in separating external users who should only be exposed to their domain only from internal users that work on sensitive data across multi-domains.

External Feeds: External data of intelligence such as threats, indicators, reputation signatures and reports. These interfaces are usually integrated with the data correlation engines of the SIEM processor, and usually several different sources of threat feeds are recommended.

According to Gartner, there are several leading vendors for SIEM platforms such as: Q.Radar (IBM), Splunk, Alienvault, Logrhythm, Arcsight, etc.

It is important to require the following feature specifications for the SOC-Py implementation beyond the common features that most platforms contain:

1. **A multi-domain platform**: This feature will enable the platform to produce managed services for different and separated entities with customization capabilities.
2. **Scalability and elasticity**: The platform should cover about 100 institutions with changing demands and coverage requirements. The feature of pay as you grow with the same architecture is highly important.
3. **Automation and orchestration**: The ability automate and orchestrate processes with many out of the box tools is highly critical due to limited personnel resources (i.e. ticketing tools, smart algorithms for anomaly detection, etc.).
4. **Flexible API** to manage and connect to third party devices.
5. **Intelligence and information sharing platform**: Tools to manage and digest threat intelligence as well as share the information in an efficient and automated manner.
6. **Privacy-by-design features**: The SIEM contains sensitive data repository with PII (Privacy Identifiable Information) content. There is a need to set the technology features to manage PII. Features include: (1) Obfuscation and masking of PII data; (2) Role based access management of PII data; (3) Auditing and automatic detection of PII in data and logs repository.

Capacity Planning and System Parameters:

The most common approach to determining how much log data will be generated is to use Events per Second (EPS). EPS is exactly what it is called, the number of log or system events that are generated by a device every second.

$EPS = \#\frac{of\ System\ Events}{\text{Time Period in Seconds}}$ Using EPS will help you scope or determine the sizing of the system in two main factors: the processing power, licensing (usually by EPS) and the storage capacity requirements.

Average EPS Vs. Peak EPS: typically we will use the Average EPS for calculations (storage and licensing). However, peak EPS is important for the system processing including hardware demands in order to support peak EPS events that can reach up to 10x the Average EPS.

Log volume storage calculations: Let's calculate the amount of data generated per day and per year.

We usually assume that each log record contains 100 Bytes at average with compression.

$$\frac{GBytes\ of\ Data}{Second} = \frac{(\text{EPS x Bytes Per Event})}{1{,}000{,}000{,}000} = \frac{\text{EPS}}{10{,}000{,}000}$$

$$\frac{GBytes\ of\ Data}{day} = \frac{GBytes\ of\ Data}{Second} X64{,}800 = \frac{EPS\ X\ 64{,}800}{10{,}000{,}000}$$

Estimated parameters for the SOC-Py project:

EPS	Retention period	Storage Estimate
10,000	6 Months	3.9TB
10,000	1 Year	7.8TB
20,000	6 Months	7.8TB
20,000	1 Year	15.6TB

A reasonable estimation would be that an institution with network of about 1,000 employees would consume average of 500 EPS. 10,000 EPS would serve about 20

institutions in the first phase, with the need to increase up to 40,000 EPS for full capacity of 80-100 institutions. Therefore, according to these estimations: Total Storage of at least 30TB is recommended for the system with the flexibility to add storage according to needs.

Data Retention Policy:

There is a need to define the data retention and backup policy as well as the method for the SIEM system and data repository. The following data policies should be defined (with recommended parameters):

1. Retention of data period: **1 Year** is recommended.
2. Backup to disk period policy: Automatic **Daily backup** (with roll back capability).
3. Backup to tape period policy: **Weekly** or bi-weekly.

Other Important System Requirements - SIEM:

1. **Backup of data and configuration**: The SOC system is expected to be a critical operational system. Therefore, there is a need to plan recovery and redundancy architecture to keep the system up and running. A need to create backup to disk (B2D) and backup to tape (B2T - long term) is a recommended practice. The backup should cover all storage data, system configuration and system audit data and should be compressed and encrypted.
2. **Internal System Security and administration**: The SIEM system is expected to be the main system for the SOC team with several role holders and personnel working on it. It is critical to manage the **internal security**

administration and auditing of all system access and data access with Role Based Access Control (RBAC) mechanism. The system should be planned on a dedicated and secured network infrastructure with a high level of security policies and systems. The SIEM system security will be managed and controlled by the SOC manager.

Additional Technology Tools for SOC Operations

In addition to SIEM platform there are several other components and tools that should be considered as addons to the toolbox used by the SOC. Many of them could be based on popular open source platforms:

1. Investigation tools: For network tapping investigations, the 'Bro' open source platform (https://www.bro.org/) that can be installed virtually on a local server is a very effective tool for offline investigation of network traffic. Use of this tool should be monitored.
2. Big data platform for analysis: For data analytics beyond the SIEM, 'Elastic' open source platform (https://www.elastic.co/) is a very good option for unstructured analysis and visualization of data.
3. Asset and configuration management tools: These tools will enable the continuous management of network assets and configuration in order to manage risk-oriented security and manage investigations effectively.
4. Vulnerability assessment tools: Nessus, openVas (http://www.openvas.org/) and other options could be used.

Communication Links Infrastructure

The Security Operation Center needs to have dedicated communication lines with all connected institutions, connecting the sensors and collectors that will be located at each institution to the SOC. The recommendation for SOC connectivity is to plan dedicated out of band virtual lines (VPNs) that will be encrypted end-to-end. As most of the government institutions (if not all) are connected to COPACO ISP (a government owned company), we recommend the establishment of a VRF (Virtual Routing and Forwarding) connectivity to the SOC with COPACO.

Infrastructure Needed

Physical Space

The SOC must maintain its own physical space in a secure location. There is a need to plan space at the data center (2-3 racks) with a redundant power supply. In addition, there should be enough work space for approximately 12 analysts with computer display screen walls (4-6).

Training Center

Just as cyber security is constantly changing and evolving, the SOC operation and personnel must constantly adapt and improve. The SOC should serve as a national knowledge hub for cyber security and as an on-the-job training for internal staff and external partners.

The SOC must provide the appropriate education and constant training to ensure that the skills and knowledge of its personnel evolve with the changing threat environment. Similarly, processes will need to adapt and change to deliver a larger value. Finally, the SOC will need to constantly evaluate itself to determine its relevance and effectiveness against evolving internal and external threats.

The main objectives of the training center should be as follows:

1. **Recruitment and Training** - Basic training for new personnel, including course materials and on-the job-training before they are fully qualified to lead cyber incident research and handling.
2. **Maturity Progress -** Advanced training for security professionals, enabling constant improvement and capacity maturity building.
3. **Education Hub for Partners** - The SOC-Py should serve as an education hub for partners, mainly from other government entities. The hub will offer shared knowledge and language and improved cooperation with other IT and cyber security partners and professional personnel. It will also serve as the de-facto expert for lessons learned and best practices for cyber security incidents.

The definition, creation or purchase of the following materials and courses are important to ensure the professional service in the SOC training center. We

recommend that one of the SOC team (Tier 2 or SOC manager) should be responsible for the training center.

Course	Audiences	Remarks
Cyber Security Essentials: Principles, Standards, Methodologies	SOC Training Partners	SOC Training Course
Tier 1 – Basic Analyst Training, Working with SIEM Tools and Processes	SOC Training	SOC Training Course
Tier 2 – Incident Response Investigation, Using Threat Intelligence	SOC Training Partners	Purchased Course
Development with Scripting Tools and Automation	SOC Training	Purchased Course
Advanced Security Data Analytics and Data Forensics Investigations	SOC Training	Purchased Course

Pricing Estimation Summary Table

The following elements need to be considered for the pricing estimation of the SOC project and scope of work. The SOC project estimations need to be for the **period of 3 years**.

Specific pricing need to be quoted from relevant vendors/integrators.

Establishment - Summary

No	Content	Remarks
1	S/W infrastructure	Storage, WAF for WEB publishing of SIEM, etc
2	H/W infrastructure	Servers, switches, routers
3	SIEM software (20,000 EPS), basic SOC operation with about 100 virtual collectors	Leading vendor
4	Advanced analytics modules	Additional advanced capabilities for analytics, automation, etc.
5	Threat intelligence feed commercial (1-2)	Commercial feed
6	Additional security tools for the central government cloud (WAF, Asset management, vulnerability assessment)	
7	Integration of project establishment	
8	Support and maintenance	For 3 years with optional 2 years extension

9	Course and training material	Online documentation, course materials, training courses
10	Professional services	Customizations, API, rules calibrations, training

Our general estimation is that a **budget of $2M for a period of 3 years is needed** to effectively implement the establishment of the SOC-Py project (H/W+ S/W + Services).

Communication links costs: A need to allocate a separate budget with the relevant government administrations for the dedicated connectivity through the government ISP.

Annual cost estimations for the SOC personnel:

Role	Qty	Month cost[$]	Annual cost[$]*
Tier 1	6	500	39,000
Tier 2	2	850	22,100
Tier 3	2	1,200	31,200
SOC Manager	1	1,200	15,600
Total	**11**		**107,900**
Training	10	5,000	50,000
Total			**157,900**

*We assume 1-month bonus salary for each year, as accepted for local government employees in Paraguay.

*We assume training cost of $5K/person/year.

Our general estimation is that an **annual budget of $160K is needed** to maintain the SOC-Py operations personnel (this budget is only for a sustainable SOC personnel).

Implementation Recommendations

Staged Implementation for Reducing Risk

We recommend implementing the project in the following stages:

Phase	Name	Duration	Focus
1	Establishment	6 months	ARO + Establishment period Recruitment of minimum 6 positions Initial training Connect 10-20 customers
2	Initial Operation Period	6 months	Initial operations SOC (8 / 5) SOC calibration Additional recruitment & training Connect 40 customers
3	SOC Full Operation	Continuous	Fully operational (24 / 7) Training center Connect 80 customers

Procurement Considerations

We recommend the following procurement considerations:

1. H/W should be based on standard servers and storage machines. It is highly recommended to be consistent with other H/W elements and vendors that are currently utilized at the government cloud due to maintenance and flexibility considerations.
2. Most of the project should be implemented on software and virtual installations.
3. A service model of support should be offered for each component (3 years as a minimum).
4. It is highly recommended that the vendors/integrators have local technical representatives to support the project throughout its lifecycle.
5. Knowledge, training and professional services should be acquired as part of the project. It is critical to procure and maintain leading material for the training center.

Stakeholders Engagement

In this type of project, that aims to serve a big community of customers (stakeholders), bringing them on board and winning their cooperation is crucial for the success of the project. Therefore, a group of stakeholders should be part of the design stage from the early phase of the project. This group (5-10 stakeholders) should be the early adopters of the SOC and be part of the initial operations, process definition and feedback. This approach will help the SOC to scale successfully to many other stakeholders.