FINANCE AND TECHNOLOGY SUMMIT

Building and Managing Effective SOC (Security Operation Center)

Vusal SALMANLI MSc, CISA, CISM, CEH
Information Security Expert

May 2019
Baku, Azerbaijan

AGENDA

- **About me**
- **SOCs within organizations across the globe**
    - Overview of current SOCs
    - Existing Challenges
    - Need for an effective SOC
- **How to build an effective SOC?**
    - Triad of Security Operations
    - People
    - Technology
    - Process
- **7 tips to manage a SOC effectively**
- **Next steps and recommendations**

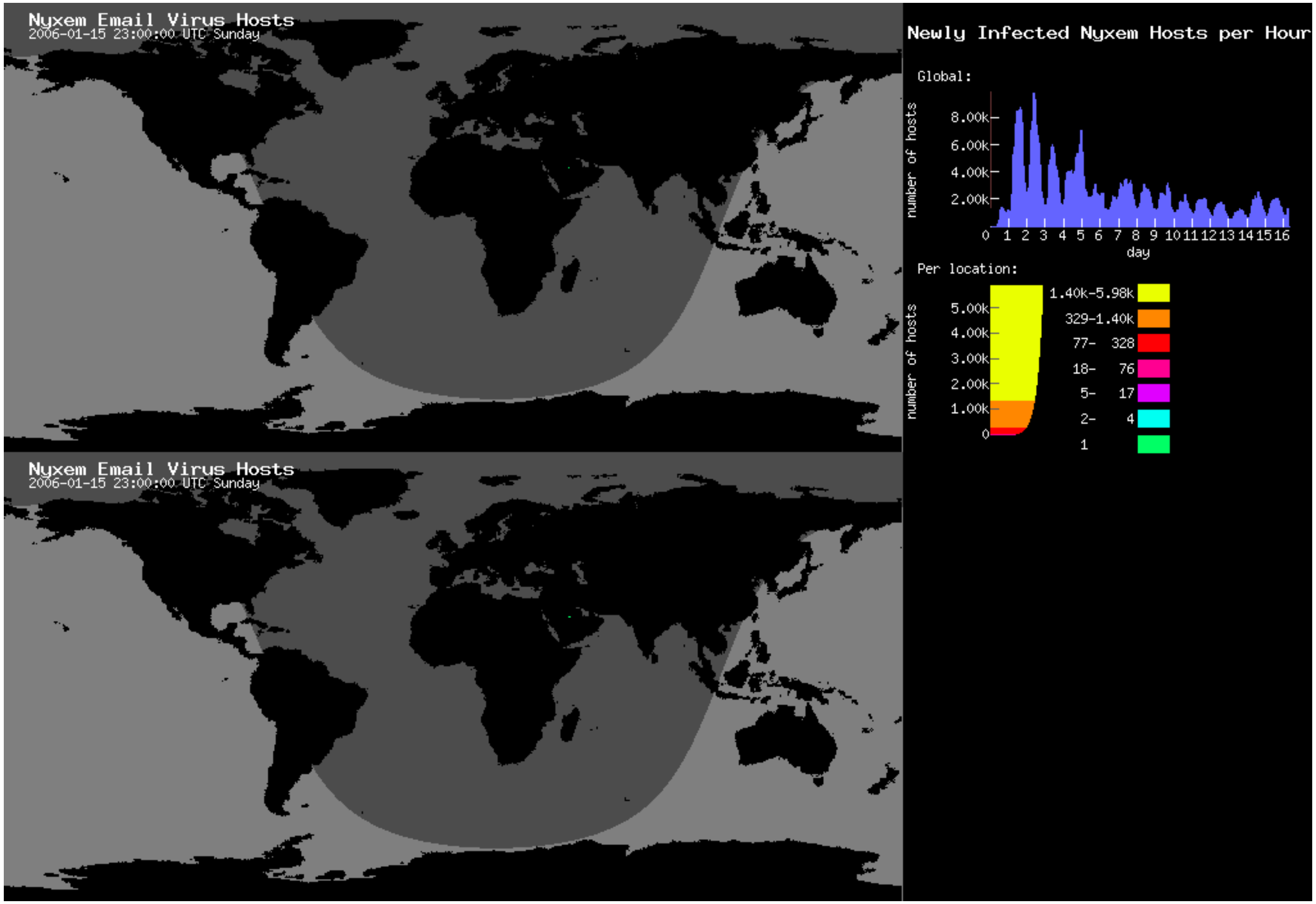
ABOUT ME

Currently working for Sirius as a Principal Consultant of Managed Security Services including:

- **Managed SIEM Service**
- **Managed FW/IPS Service (on-premise & cloud)**
- **Managed global SOC Service**

Sirius is one of the largest solutions provider in North America. For more information: www.siriuscom.com

- ✓ **Former Head of Information Security unit at Azerconnect LLC**
- ✓ **Former Manager of Information Security unit at Azerfon LLC**
- ✓ **Former Visiting Lecturer at SABAH groups, Azerbaijan Technical University**
- ✓ **10+ years experience in ICT sphere**
- ✓ **MSc, Information Security**
- ✓ **OCP, OCE, MCP, CCSA, CEH , CISA , CISM Certificates**
- ✓ **Silver member of ISACA**



SOCs
Within Organizations
Across The Globe

OVERVIEW OF CURRENT SOCS

- Metrics are used in only about half (54%) of SOCs.
- Only 30% had a positive depiction of the coordination between the SOC and NOC.
- Asset discovery and inventory tool satisfaction was rated the lowest of all technologies.
- Most meaningful event correlation continues to be highly manual.
- The most common architecture is a single, central SOC (39%); 29% have “informal/not defined” SOCs.
- 31% of SOCs are staffed with 2–5 people, 36% of SOCS are staffed with 6 to 25 SOC personnel, while 11% had 26 to 100 SOC staff members.
- 62% cite lack of skilled staff, 53% cite inadequate automation/orchestration as the most common self identified shortcomings.

SANS

A SANS Survey

The Definition of SOC-cess?

SANS 2018 Security Operations Center Survey

EXISTING CHALLENGES

Main obstacles security managers face in deploying and maintaining SOCs:

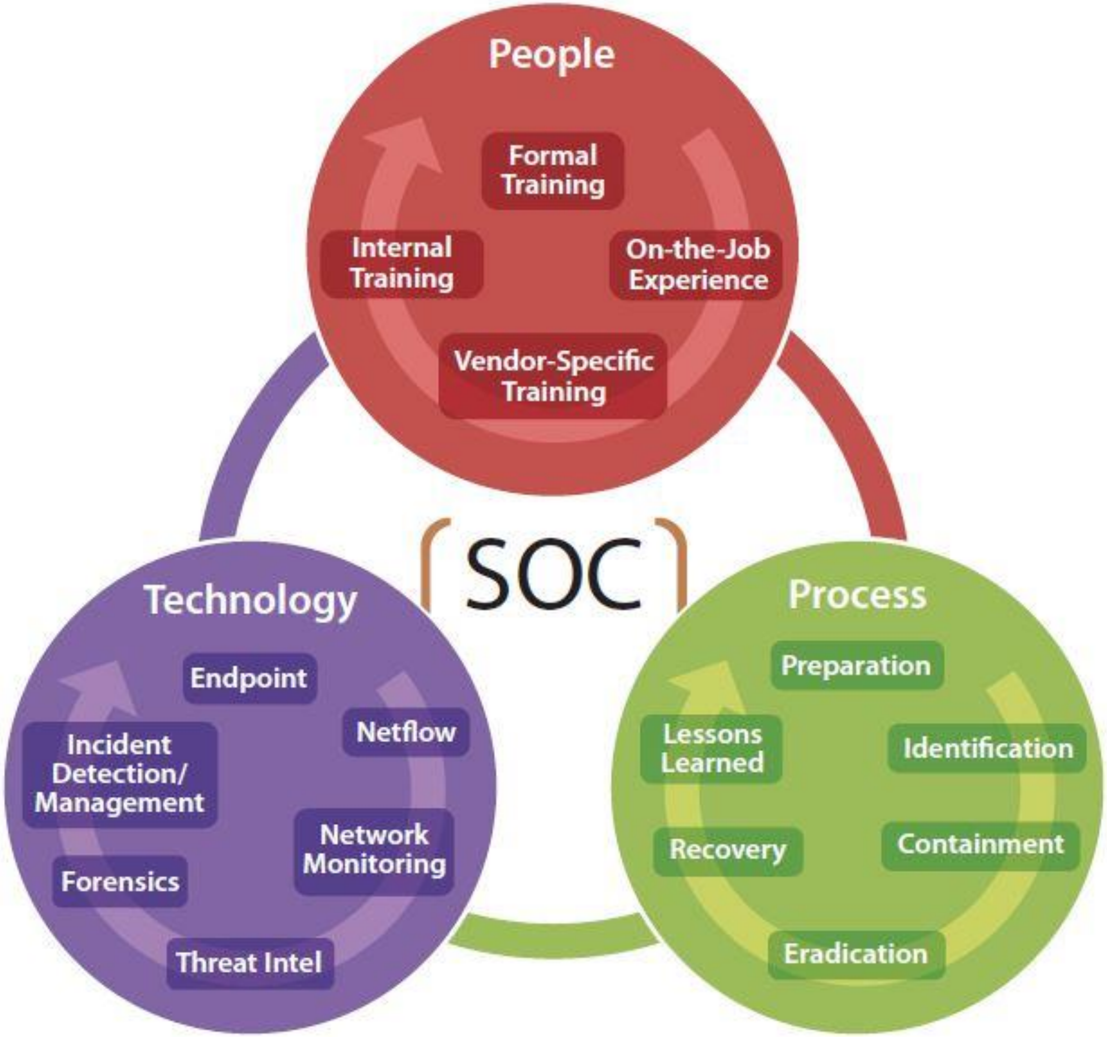
- Defining a meaningful SOC metrics
- Lack of effective and integrated tools
- Lack of effective asset and inventory tools
- Organizational silos and barriers
- Lack of staff and key skills
- Ineffective automation, particularly in correlation

NEED FOR AN EFFECTIVE SOC

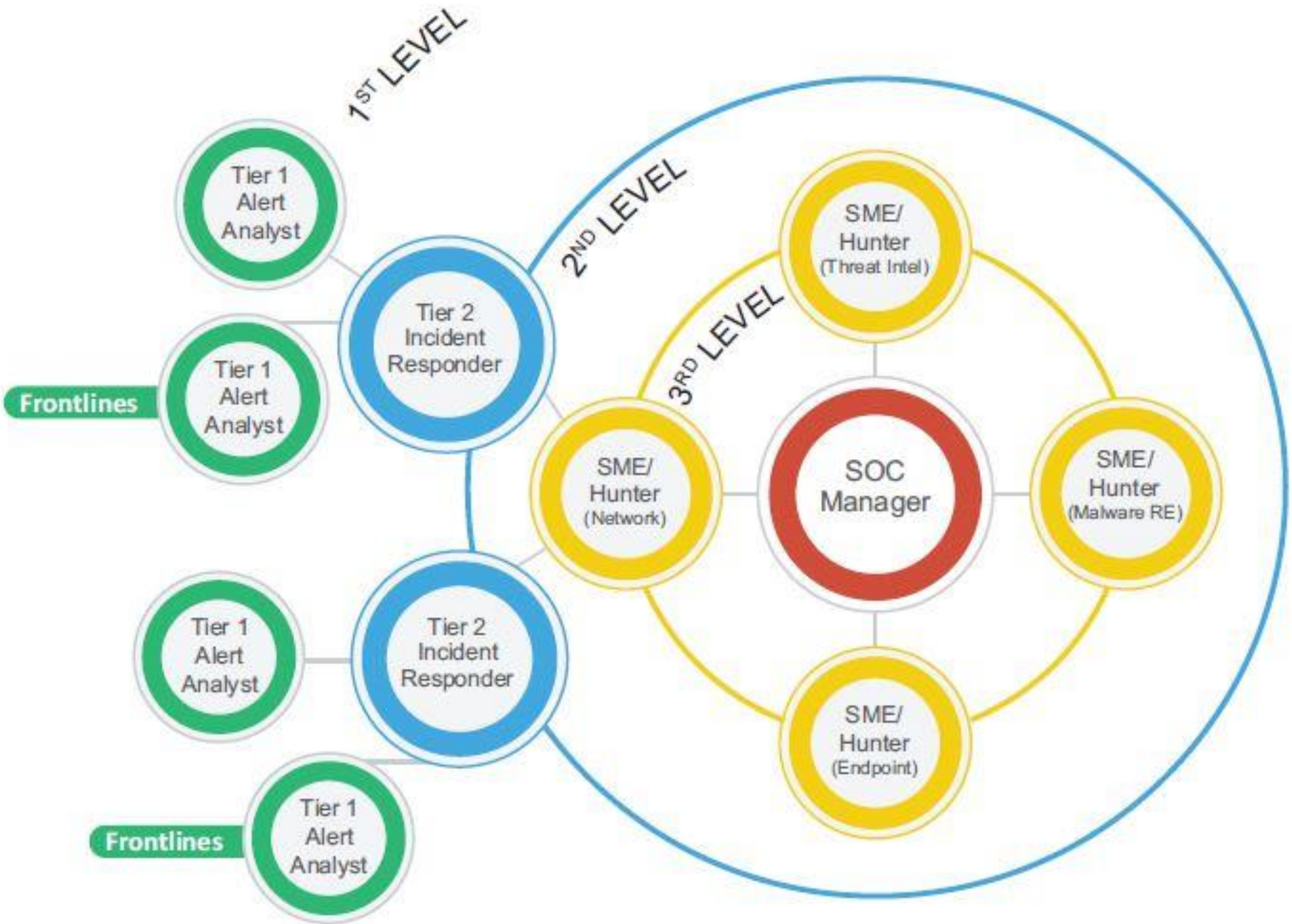
A leading indicator of a security program's capability to effectively and efficiently protect the business is the existence of a functional and mature security operations center.

HOW TO BUILD AN EFFECTIVE SOC?

TRIAD OF SECURITY OPERATIONS: PEOPLE, PROCESS AND TECHNOLOGY

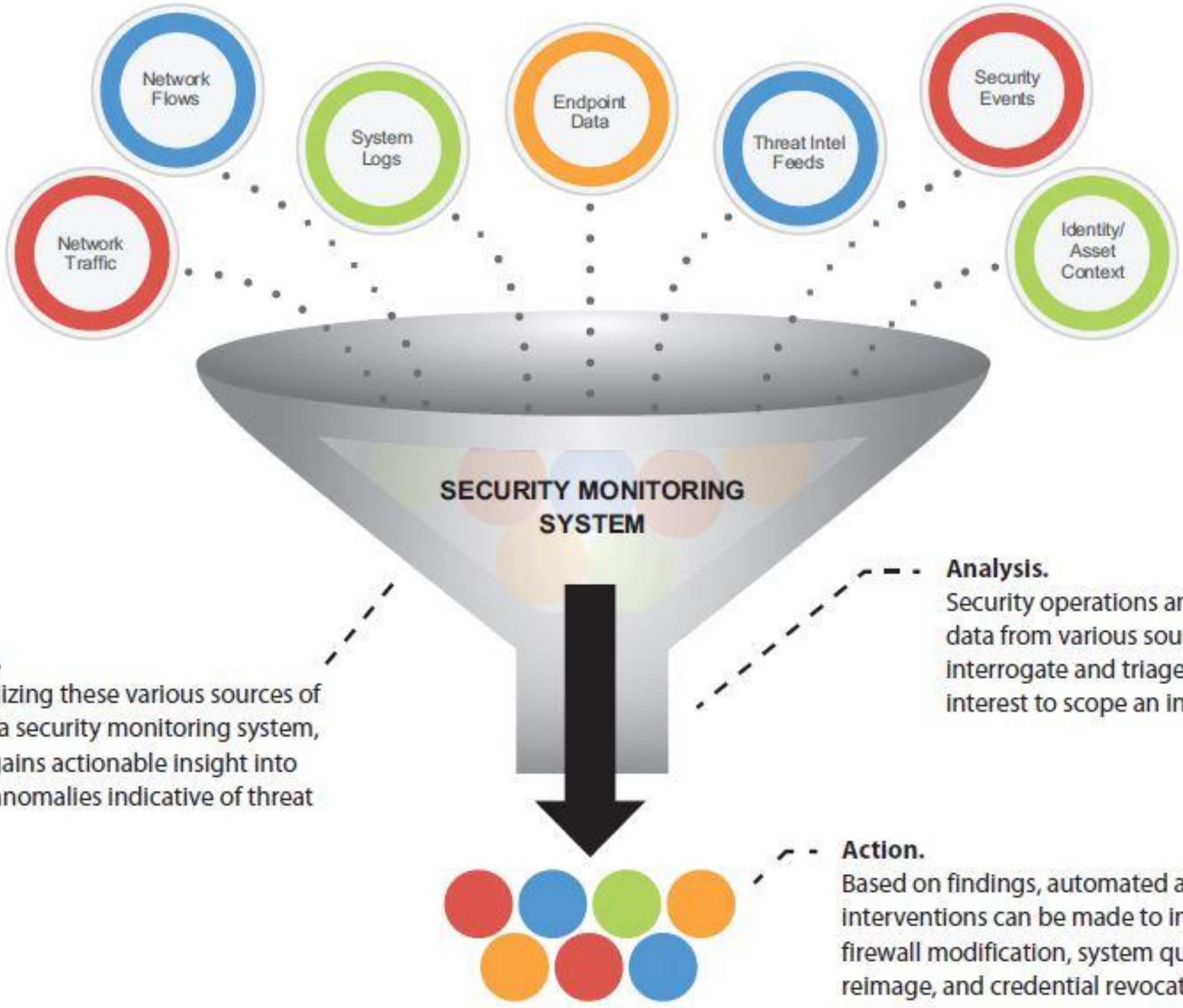


PEOPLE



Organization of the SOC

TECHNOLOGY



Visibility.
By centralizing these various sources of data into a security monitoring system, the SOC gains actionable insight into possible anomalies indicative of threat activity.

Analysis.
Security operations analysts can analyze data from various sources and further interrogate and triage devices of interest to scope an incident.

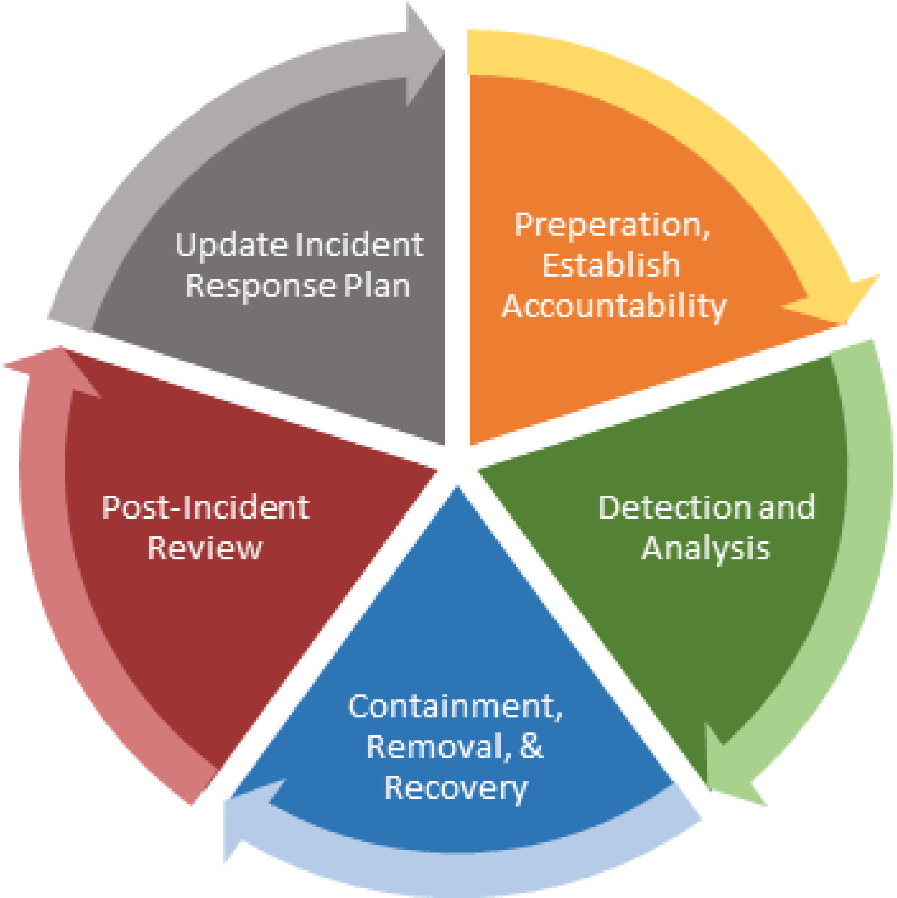
Action.
Based on findings, automated and manual interventions can be made to include patching, firewall modification, system quarantine or reimage, and credential revocation.

Compatible Technologies

PROCESS

Basic procedures required for maintaining a SOC:

- Monitoring Procedure
- Notification Procedure
- Escalation Process
- Transition of Daily SOC Services
- Shift Logging Procedures
- Incident Logging Procedures
- Compliance Monitoring Procedure
- Report Development Procedure
- Dashboard Creation Procedure
- Incident Investigation Procedure


Preperation, Establish Accountability
Detection and Analysis
Containment, Removal, & Recovery
Post-Incident Review
Update Incident Response Plan

One of the most frequently used incident response process models is the DOE/CIAC model, which consists of six stages: **preparation, identification, containment, eradication, recovery and lessons learned.**
In addition, NIST SP800-61 Revision 2, “Computer Security Incident Handling Guide” provides excellent guidance in developing IR procedures

7 TIPS
TO MANAGE A SOC EFFECTIVELY

7 TIPS TO MANAGE A SOC EFFECTIVELY

1. Hire Smart
2. Visibility
3. Take and review notes
4. Prepare management reports
5. Evaluate and apply threat intelligence
6. Team engagement
7. Communication within parties

NEXT STEPS AND RECOMMENDATIONS

- Reconsider your recruitment strategy
- Implement a performance-based incentive program for SOC analysts
- Identify and evaluate all sources of threat intelligence.
- Practice your incident response(IR) plan from A to Z
- Prepare a pretty report template for upper management and ensure it includes useful metrics.

THANK YOU!