Agenda

- Cyber Security Benefits & Challenges
- Cyber Security Operations Centre
- Challenges to Cyber Security Onboarding
- Rethinking Cyber Security Onboarding
- Recommendations
- Conclusions
- Q&A
Building a CSOC comprises two key aspects:

1. Cyber Security Onboarding
2. Cyber Security Monitoring
Cyber Security Monitoring

- Metrics
- Threats
- Vulnerabilities
- Risks

LAN

SOC Analysts

WAN

On Premises Data Centre

- Events & Logs
- Windows Server
- Database Server
- Firewall
- Storage

Cloud Data Centre

- Workloads are migrated to Cloud, e.g. AD, DB etc

INTERNET

- Events & Logs
- Windows Server
- Database Server

AWS

C-MRiC.ORG
Centre for Multidisciplinary Research, Innovation and Collaboration
Functional Representation of SOC
# Cyber Security Onboarding Reframing Matrix

<table>
<thead>
<tr>
<th>CSOC Perspective</th>
<th>Client Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not enough feeds to monitor</td>
<td>Lack of funds</td>
</tr>
<tr>
<td>Poor quality of onboarding e.g. missing parsers &amp; plugins</td>
<td>Wrong funding model</td>
</tr>
<tr>
<td>Incomplete documentation</td>
<td>Lack of return on security investment (ROSI)</td>
</tr>
<tr>
<td>Too many dashboards</td>
<td>Time consuming</td>
</tr>
</tbody>
</table>

**Cyber Onboarding is ‘Broken’**

<table>
<thead>
<tr>
<th>Onboarding Perspective</th>
<th>SMT Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of SMT support</td>
<td>Too expensive and inconvenient (painful)</td>
</tr>
<tr>
<td>SOC maturity</td>
<td>Lack of clarity</td>
</tr>
<tr>
<td>Onboarding is complex</td>
<td>Governance</td>
</tr>
<tr>
<td>Dependency issues e.g. lack of business resource</td>
<td>Structure</td>
</tr>
</tbody>
</table>

---

[CMRIC.ORG](http://CMRIC.ORG) - Centre for Multidisciplinary Research, Innovation and Collaboration
Rethinking Cyber Security Onboarding

Current State

- Linear
- Takes between 6-36 months depending on size
- Process intensive
- Waterfall and onerous

- Cyclic
- Takes Days and Weeks
- Automated
- Agile and straightforward

Future State

Discover

Deploy

Design

Test

Code

SOAR

Onboarding Process
Cyber Security Monitoring – Automating Infrastructure as Code

Workloads are migrated to Cloud, e.g. AD, DB etc

Automate the target infrastructure as code

C-MRiC.ORG
Centre for Multidisciplinary Research, Innovation and Collaboration
Automating & Orchestrating Cyber Security

Onboarding

LAN

WAN

SOC Analysts

INTERNET

Firewall

Windows Server

Database Server

Events & Logs

Storage

INTERNET

Firewall

Windows Server

Database Server

Events & Logs

Storage

INTERNET

Events & Logs

Database Server

DNS

C-MRiC.ORG

Centre for Multidisciplinary Research, Innovation and Collaboration

Automate resource as code stack, e.g. AD, DB, etc.
Recommendations (MoSCoW)

- Return on investment (RoI) and return on cyber security investments (RoSI)

- Prioritise the onboarding effort based on risk

- Business functions must be appropriately aligned

- Strategy: A cyber strategy upon which SOC strategy and other programme-level strategies align to

- Value: A cyber strategy must enable and support overarching business mission

- Structure: Governance structure must exist to ensure business strategy is successful

- Prioritisation: Prioritise the onboarding effort based on risk

- Investment: Return on investment (RoI) and return on cyber security investments (RoSI)
Conclusions

1. SOC is a significant Organisational Investment

2. 3- Key Drivers: Business Requirement, Security & Compliance

3. Building efficient SOC takes Time & Effort (Complex)

4. Create Standard Operating Procedures, Playbooks & Run books

5. Leadership Support

6. Train and Develop your SOC Staff
Conclusions

- Automate Threat Intelligence with SIEM
- Automate SOC Processes & Techniques
- Conduct Continuous Vulnerability Assessment
- Build Cyber Resilience & Recovery Capability
- Automate Incident Response
- Use Artificial Intel & Machine Learning Tools
Thank you to the sponsors
Thank-You 😊

Q&A

My Contact
Dr. Cyril Onwubiko
Twitter: https://twitter.com/DrCyrilOnwubiko
Web: https://www.c-mric.com/cyril

C-MRiC.ORG
Centre for Multidisciplinary Research, Innovation and Collaboration
IEEE Cyber Science 2021 [link](https://www.c-mric.com/conferences)
June 14-16, 2021 | Dublin, Ireland

**CyberSA 2021**  
Trustworthy and Transparent AI  
14-16 June 2021 | [link](https://www.c-mric.com/csa2021)

**Social Media 2021**  
AI-enabled Social Media Innovative Information Operation  
Virtual / Online  
14-16 June 2021 | [link](https://www.c-mric.com/sm2021)

**Cyber Security 2021**  
Advancing Cyber Security Education in a post-COVID World  
Virtual / Online  
14-16 June 2021 | [link](https://www.c-mric.com/cs2021)

**Cyber Incident 2021**  
Cyber Resilience as Code  
Virtual / Online  
14-16 June 2021 | [link](https://www.c-mric.com/ci2021)