Distinguished Lecture

Rethinking Cyber Security Onboarding

Dr Cyril Onwubiko

Director, Enterprise Security Architecture, Pearson

October 29, 2020

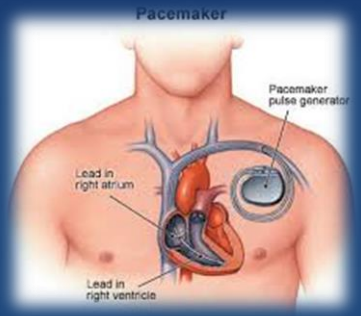
C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Agenda

- Cyber Security Benefits & Challenges
- Cyber Security Operations Centre
- Challenges to Cyber Security Onboarding
- Rethinking Cyber Security Onboarding
- Recommendations
- Conclusions
- Q&A

Cyber Security, then What?



C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Cyber Security Challenges

C-MRiC.ORG®

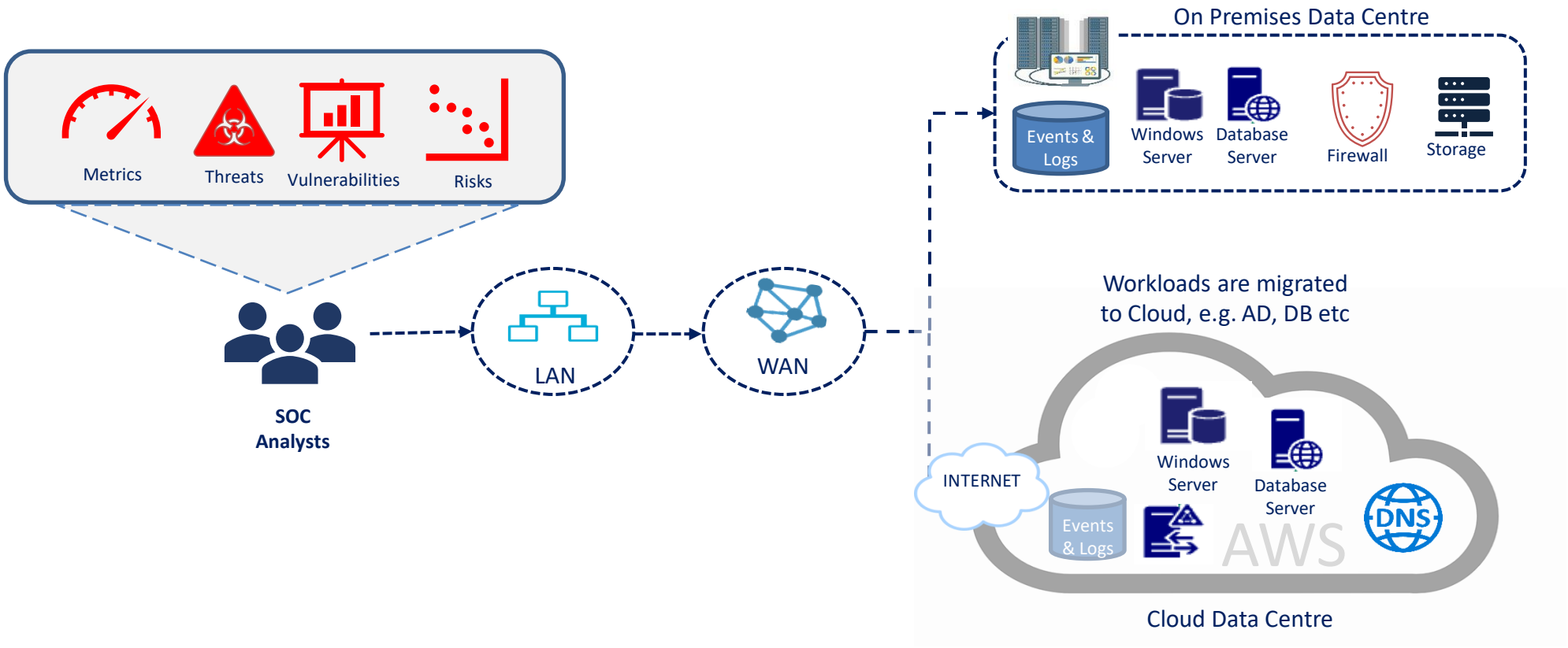
Centre for Multidisciplinary Research, Innovation and Collaboration

Cyber Security Operations Centre

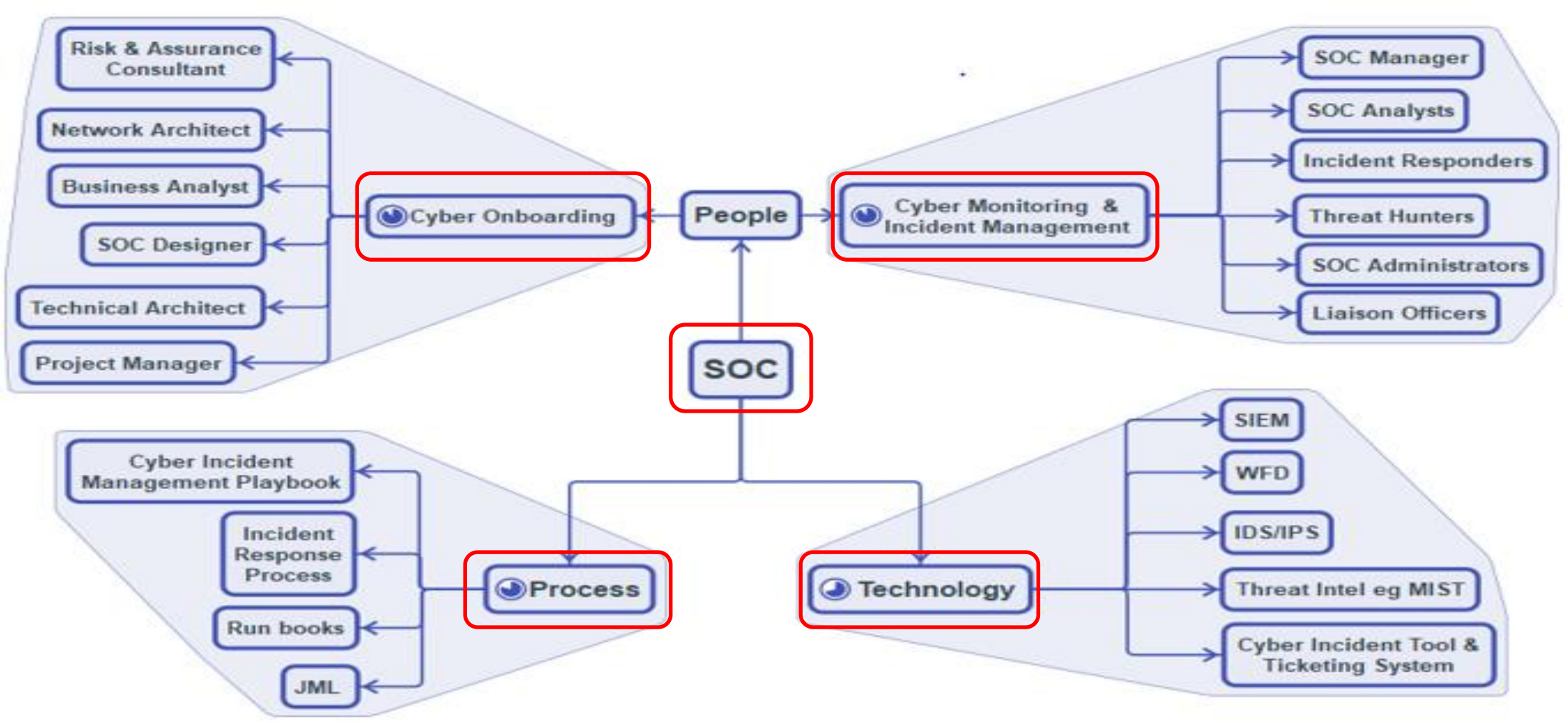
Building a CSOC comprises two key aspects:

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

Cyber Security Monitoring



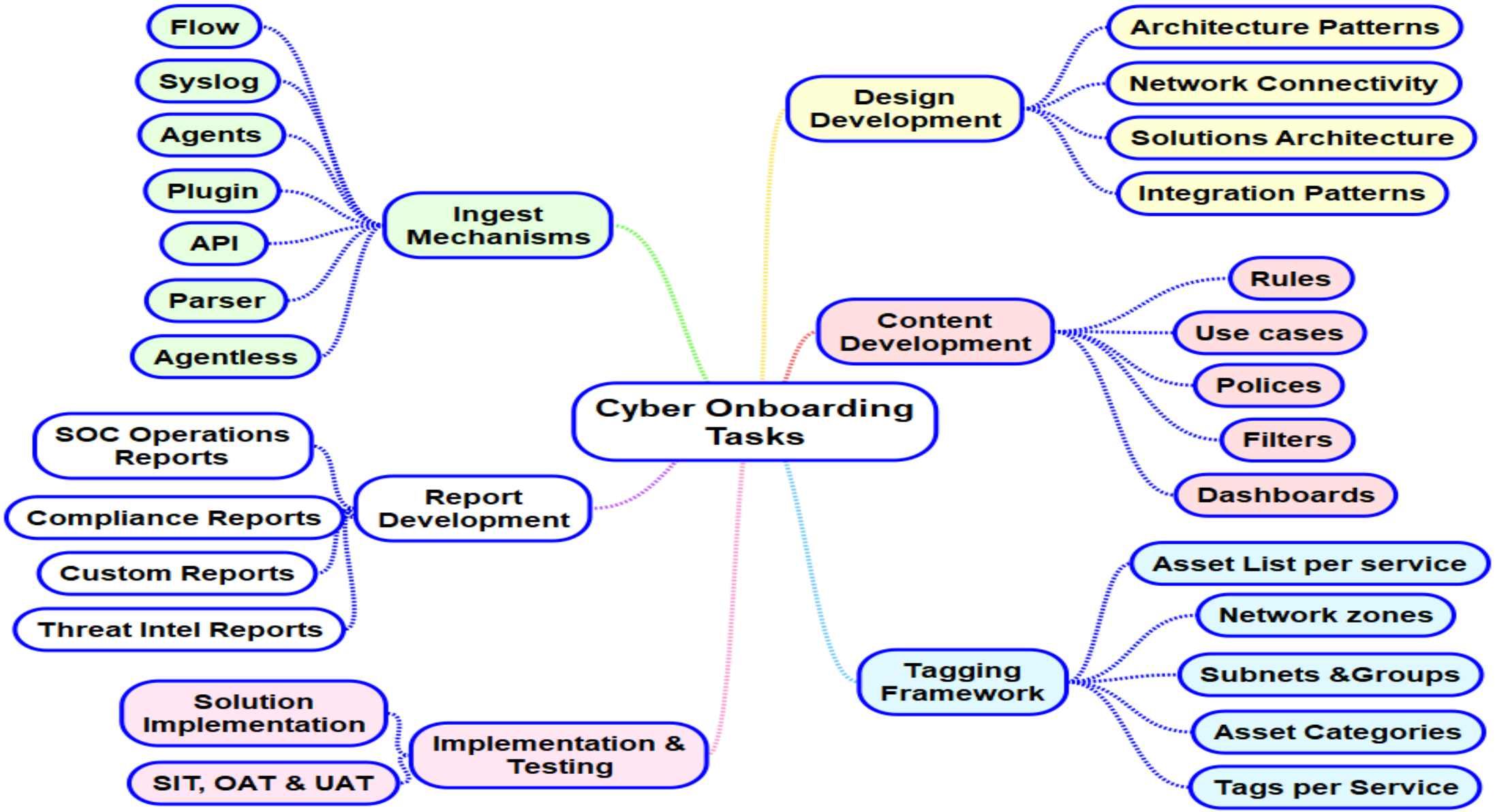
Functional Representation of SOC



C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Cyber Security Onboarding



Cyber Security Onboarding Reframing Matrix

CSOC Perspective	Client Perspective
• Not enough feeds to monitor • Poor quality of onboarding e.g. missing parsers & plugins • Incomplete documentation • Too many dashboards	• Lack of funds • Wrong funding model • Lack of return on security investment (ROSI) • Time consuming

Cyber Onboarding is 'Broken'

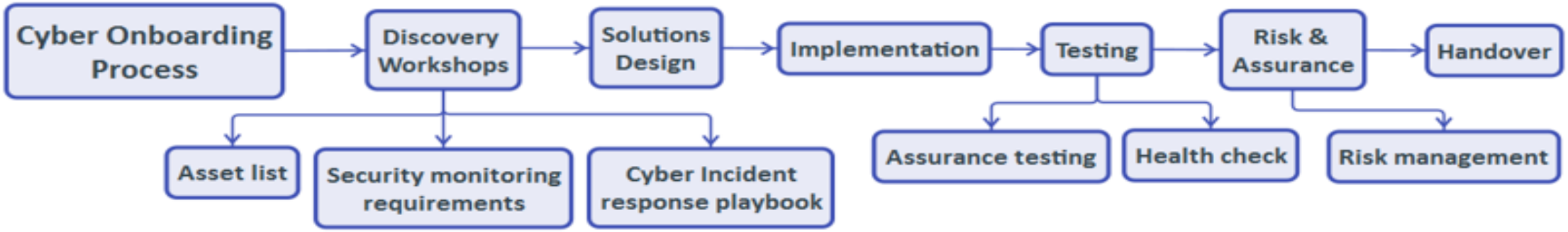
Onboarding Perspective	SMT Perspective
• Lack of SMT support • SOC maturity • Onboarding is complex • Dependency issues e.g. lack of business resource	• Too expensive and inconvenient (painful) • Lack of clarity • Governance • Structure

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Rethinking Cyber Security Onboarding

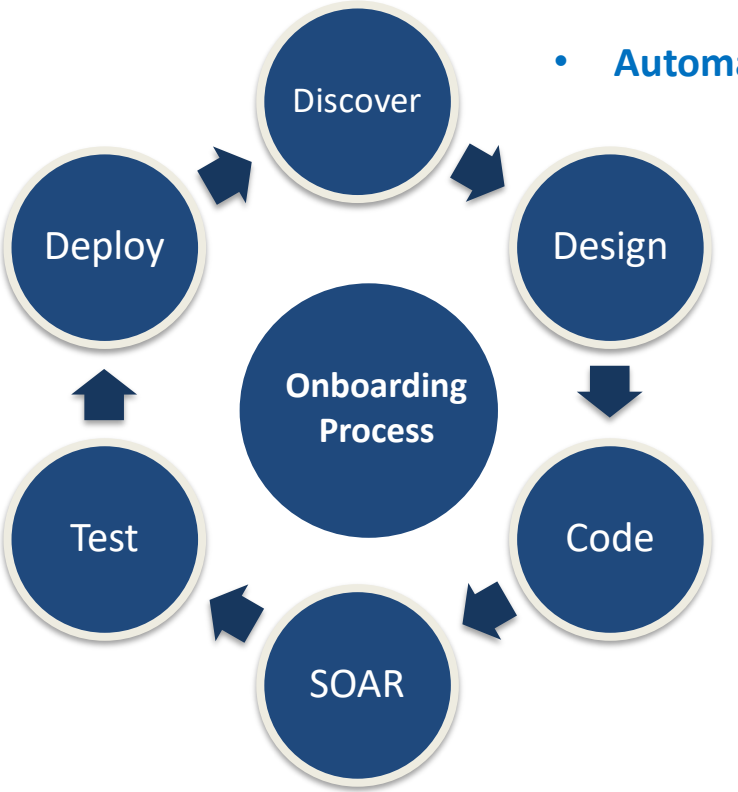
Current State



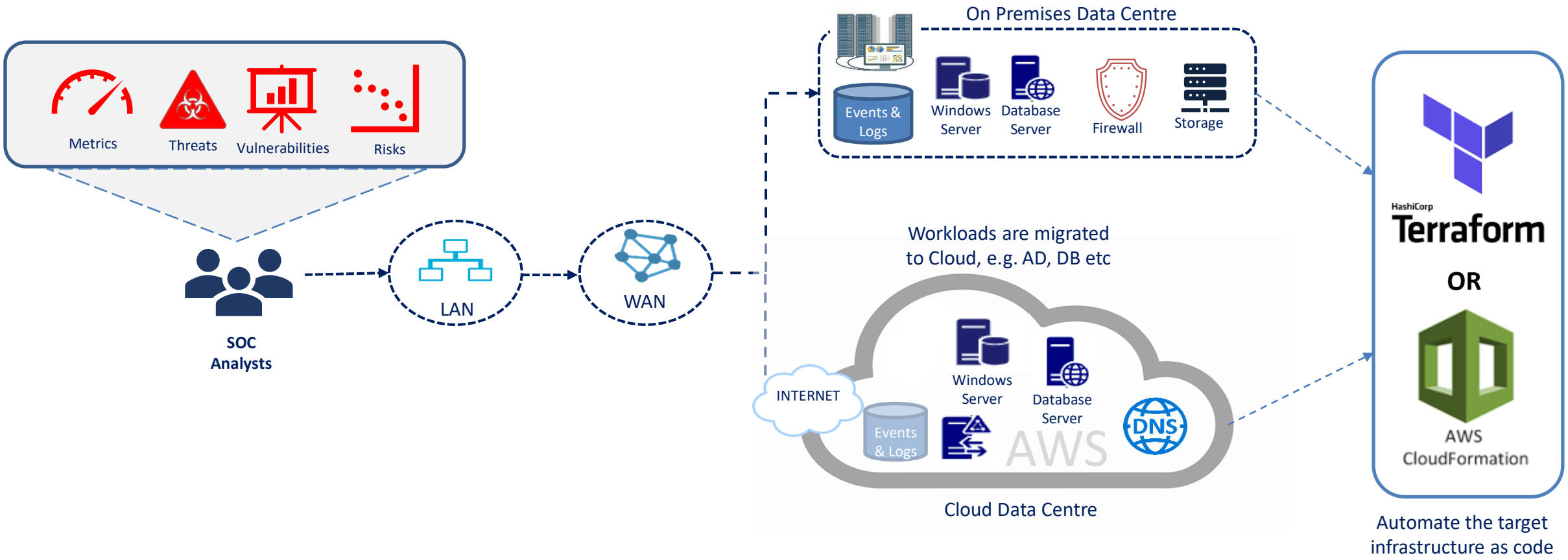
- Linear
- Takes between 6-36 months depending on size
- Process intensive
- Waterfall and onerous

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

Future State



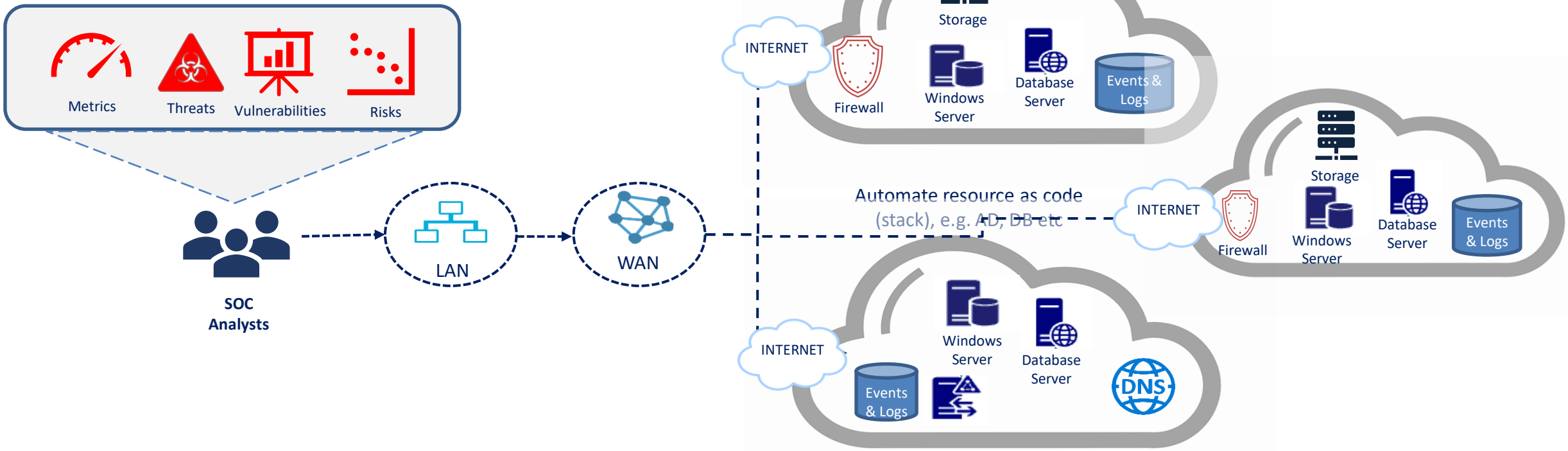
Cyber Security Monitoring – Automating Infrastructure as Code



C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Automating & Orchestrating Cyber Security Onboarding



C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

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

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

A cyber strategy must enable and support overarching business mission

Governance structure must exist to ensure business strategy is successful

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

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

7 Automate Threat Intelligence with SIEM

8 Automate SOC Processes & Techniques

9 Conduct Continuous Vulnerability Assessment

12 Build Cyber Resilience & Recovery Capability

11 Automate Incident Response

10 Use Artificial Intel & Machine Learning Tools

References

1. C Onwubiko, K Ouazzane (2019): "**Cyber Onboarding is 'Broken'**" Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, June 3-4, 2019. [Download]
2. Onwubiko, C. and Ouazzane, K. (2019): "**Challenges towards Building an effective Cyber Security Operations Centre"**. *International Journal on Cyber Situational Awareness, Vol. 4, No. 1*, pp11-39. [Download]
3. C. Onwubiko (2018): **"CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process"**, Proceedings of the 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), DOI: 10.1109/CyberSA.2018.8551486 [Download] [Presentation]
4. C. Onwubiko (2015): "**Cyber Security Operations Centre: Security Monitoring for protecting Business and supporting Cyber Defense Strategy**", Proceedings of the IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015), joint and co-located with Cyber Science 2015 conferences, London, UK, June 8-9, 2015 [Download]

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Thank you to the sponsors

IEEE Kenya Section

IEEE young professionals Kenya Section

IEEE computer society

IEEE youngprofessionals region 8

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

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 https://www.c-mric.com/conferences

June 14-16, 2021 | Dublin, Ireland

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration