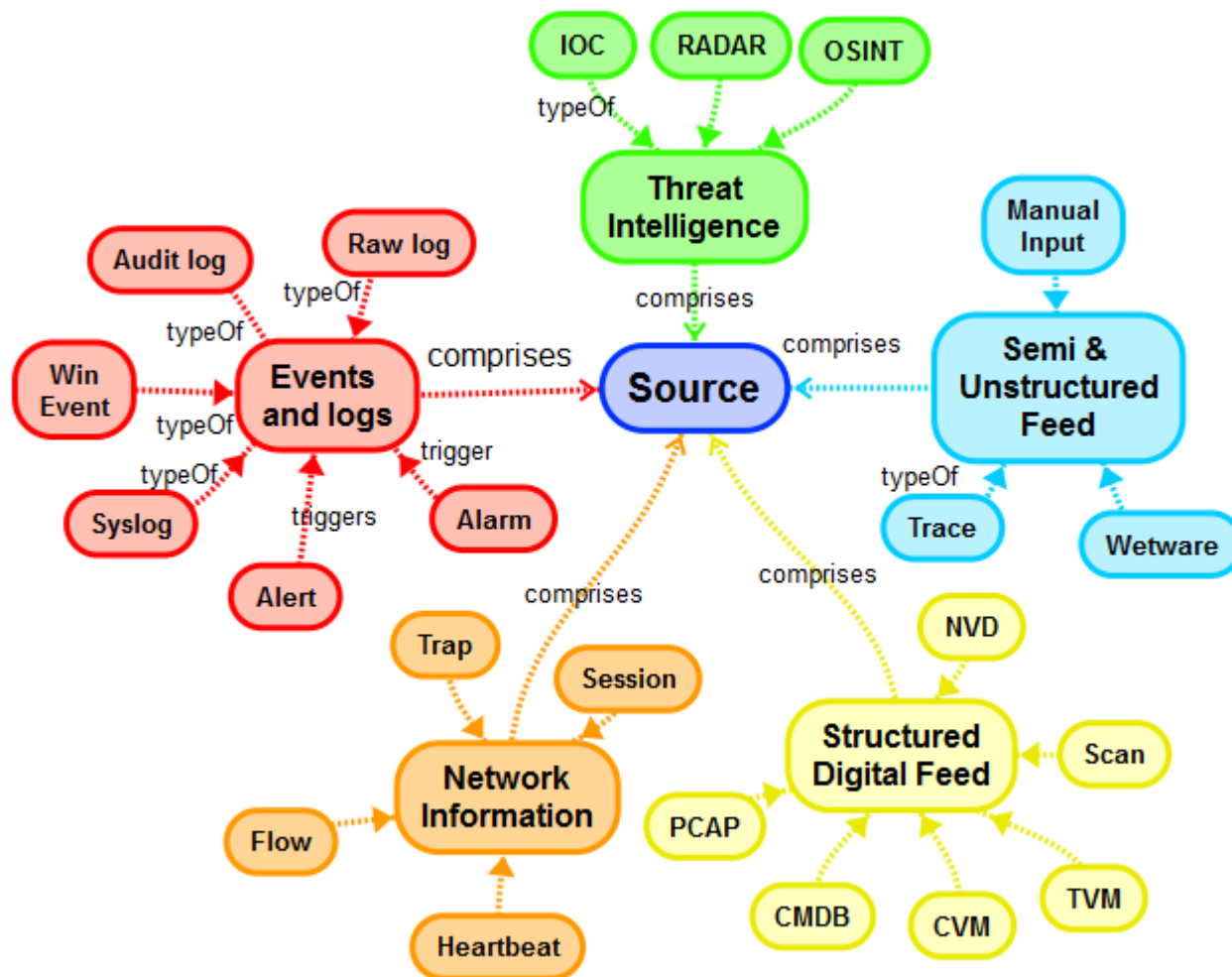


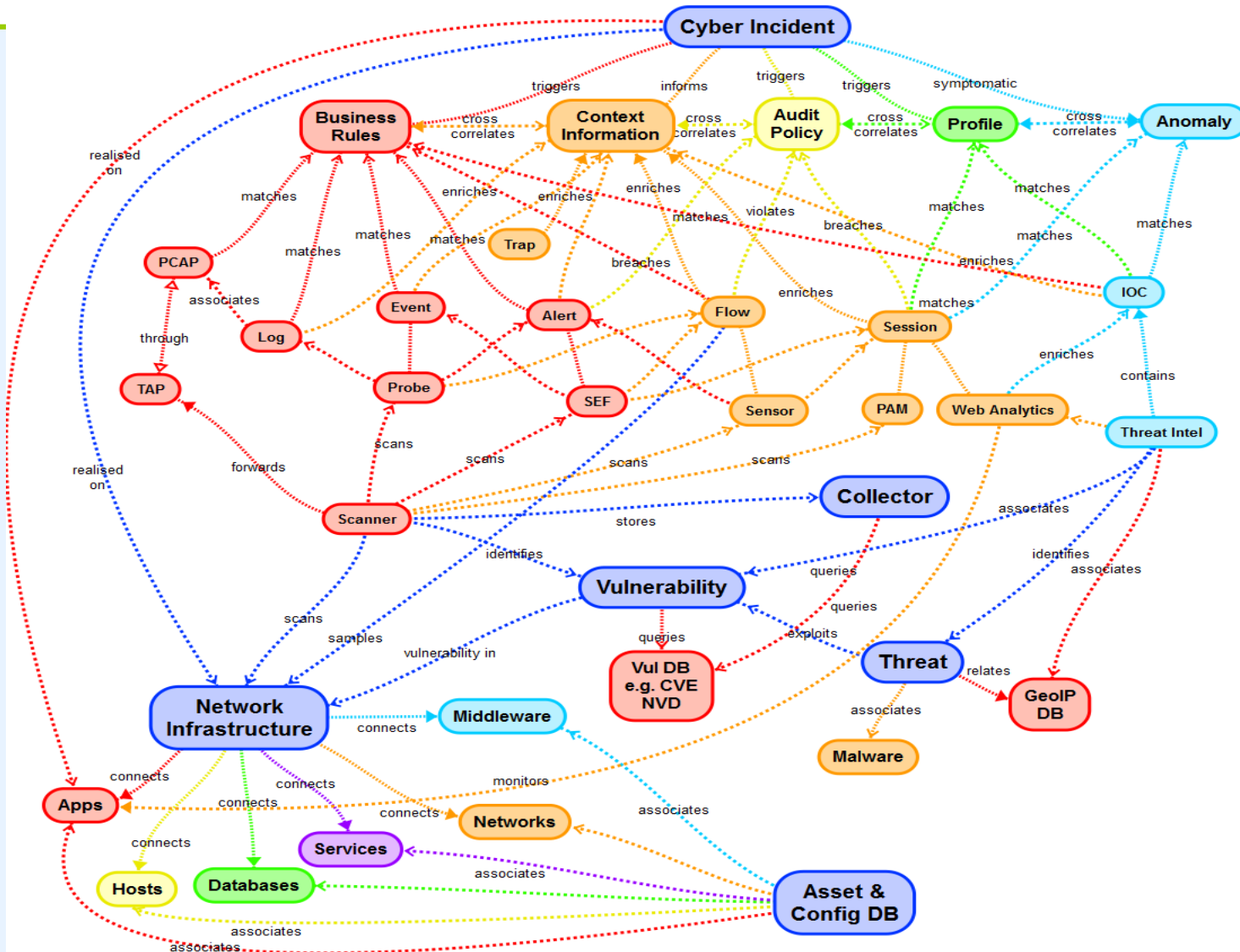
CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process

Dr. Cyril Onwubiko
Chair, Cyber Security Intelligence

Context

CoCoa – is an ontology-based knowledge graph of cyber incident for enhanced situational awareness of the monitored environment.





Conclusion

- *Ontology-based knowledge graph* offers semantics for knowledge encoding that enables understanding.
- CSOC Analysis is a vital process for all SOC's.
- Log Collection and Collation on itself is insufficient, and analysis of in-flight messages, events, and traffic sessions is needed to detect threats and gain better understanding and awareness.
- Threat intelligence offers augmented 'threat picture'

References

1. C. Onwubiko (2015), Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy, IEEE Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015), DOI 10.1109/CyberSA.2015.7166125
2. C. Onwubiko (2018), CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process, IEEE Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2018), Glasgow, Scotland, UK
3. Cyber Science 2015 – <http://www.c-mric.org/index.php/cs2015>
4. International Journal on Cyber Situational Awareness (IJCSA) - <http://www.c-mric.org/journals-ijcsa>