Security Operations Centre: Situational Awareness, Threat Intelligence & Cybercrime

Dr Cyril Onwubiko
Chair, Cyber Security Intelligence

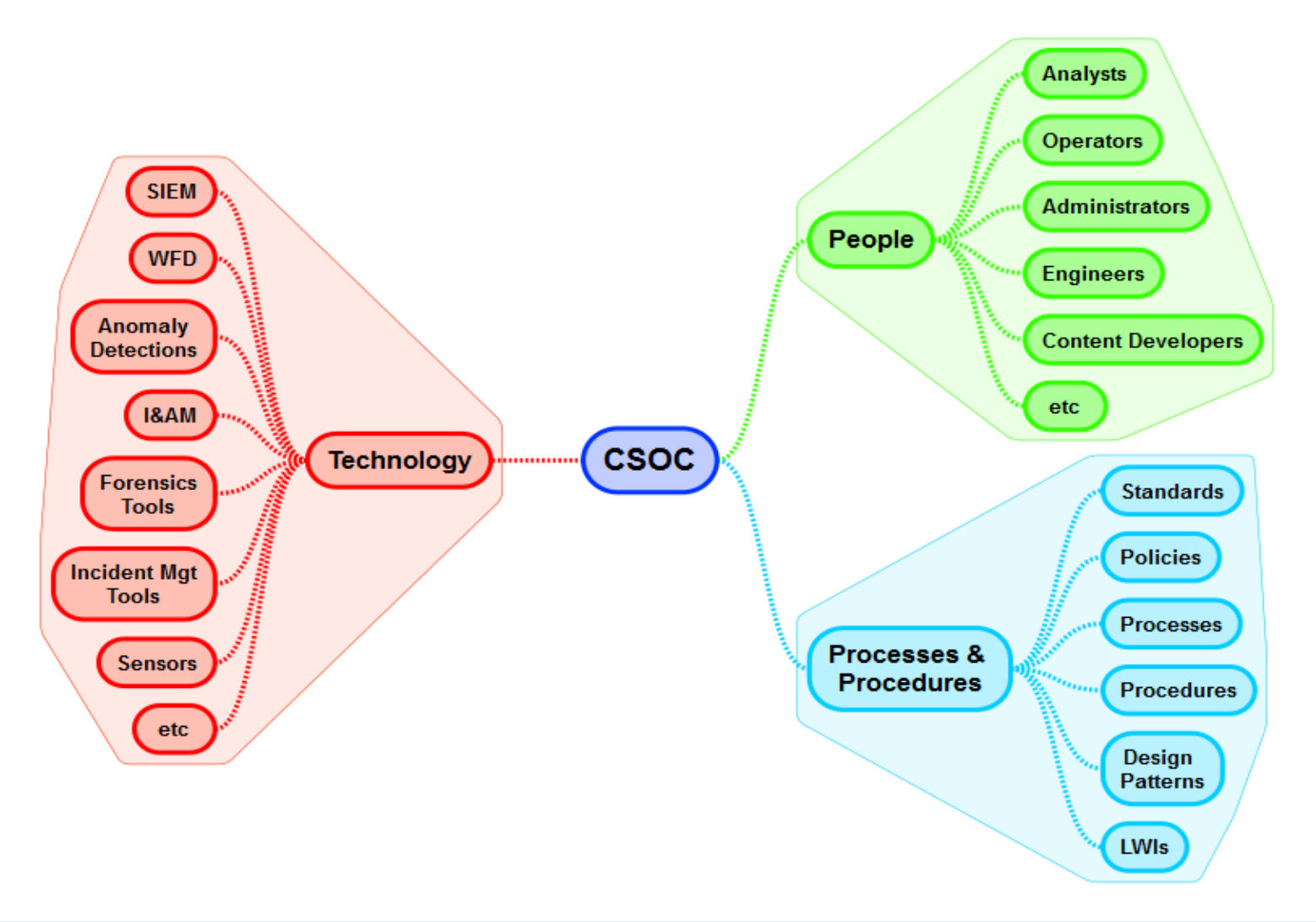
Abstract

- There have been longitudinal advances in both cybersecurity and cyber-threats in recent years.
- The pace of change and advancements has equally been astronomical and astonishing. Technology refresh cycles have been slashed, and are now estimated to between 12 to 18 months, while the number of cyber users or entities has quadrupled in the last five years.
- These continuous changes have left an ever increasing gap between ***cybersecurity*** and ***cyber-threats***
- This gap between cybersecurity and cyber-threats appears to widen even further in areas with far greater financial rewards for the criminals, or nation state political gains.
- Exploits are now common and frequent, and impact far much greater than before.
- This situation is further exacerbated by the lack of adequate and well deployed **security operations centres** to monitor organizational cyber investments.

Aim

Cyber security operations centre deployment models are proposed to provide better and enhanced situational awareness in order to detect common and frequent threats, and also to detect sophisticated and cross-channel exploits.

Cyber Security Operations Centre (CSOC)

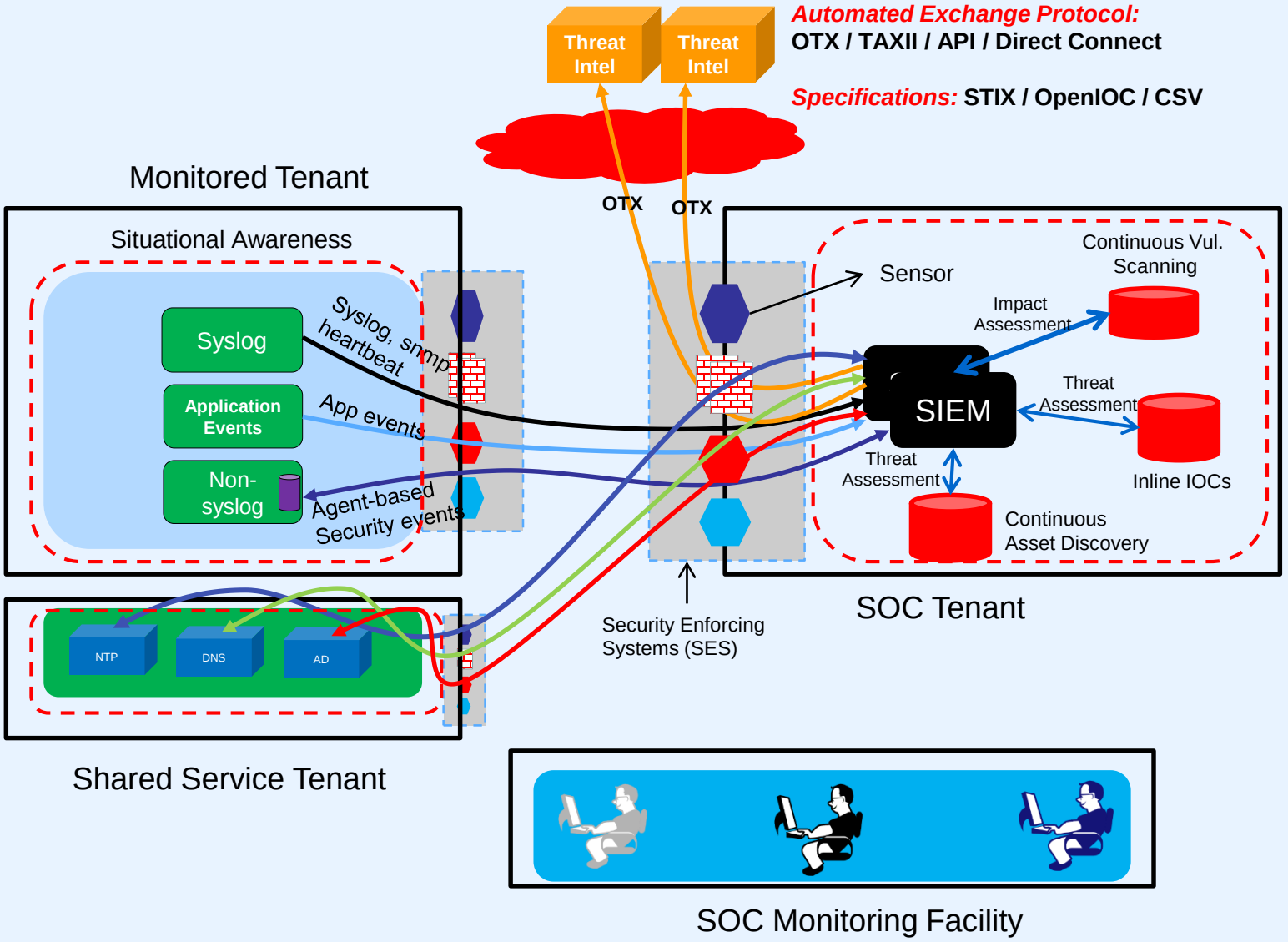


CSOC

Comprises:

People (*Analyst, Operators, Administrators* etc.) who monitor ICT systems, infrastructure and applications. They leverage **Technology** to ***prevent*** and ***detect*** cyber attacks, security breaches, and abuse, and use **Policies** and **Procedures** to ***deter*** computer misuse and policy violation, and to follow up and ***respond*** to cyber incidents.

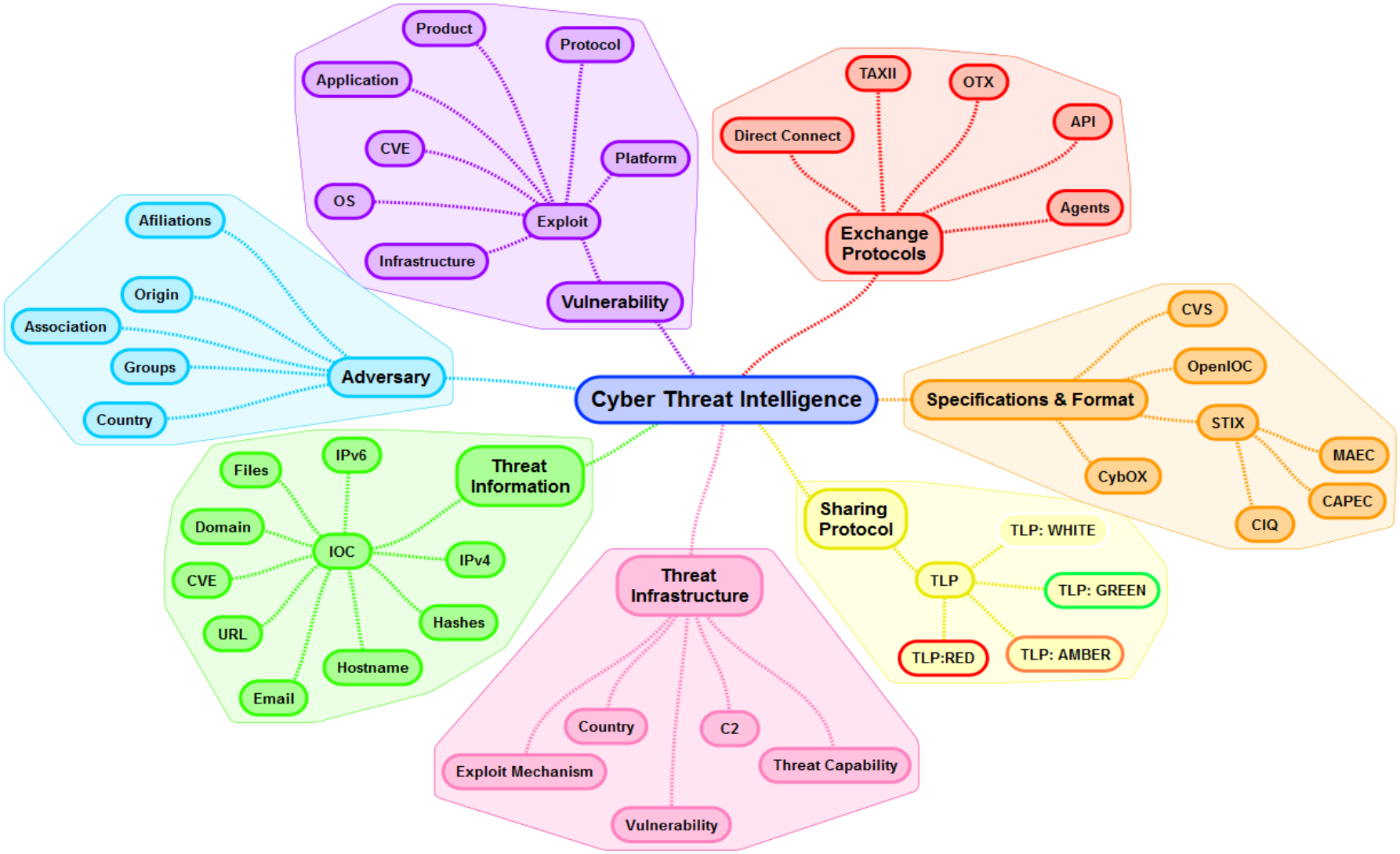
SOC Deployment Model



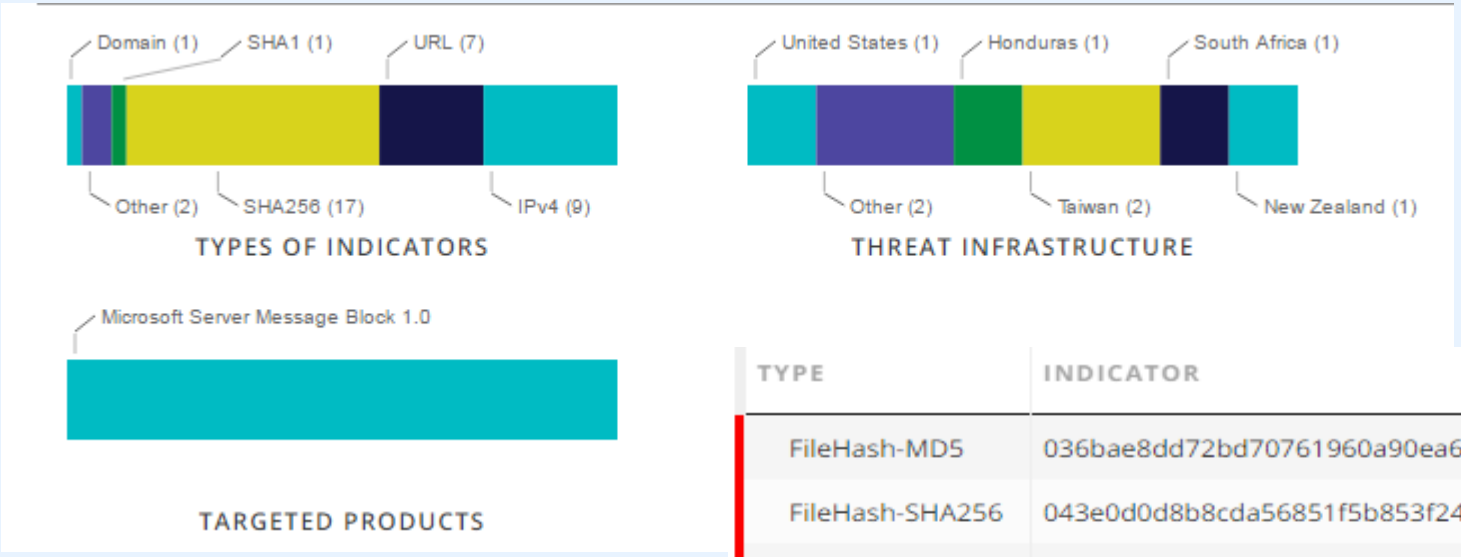
Cyber Threat Intelligence

- Threat intelligence is knowledge and information about threats and threat actors, and their capabilities and actions.
  - Physical, Cyber & Cyber Physical
- Threat information sharing specifications
- Specifications for representing cyber-threats in a standardized format, and most importantly allows automated exchange of cyber-threat information.
  - Structured Threat Information Expression (STIX)
  - Cyber Observable Expression (CybOX)
  - Open Indicators of Compromise (OpenIOC)
  - CSV
- Automated exchange mechanisms
  - Open Threat Exchange (OTX)
  - Trusted Automated Exchange of Indicator Information (TAXII)

Cyber Threat Intelligence Overview



Use case: WannaCry linked Lazarus Indicators



ADVERSARY: Lazarus Group

TLP: White

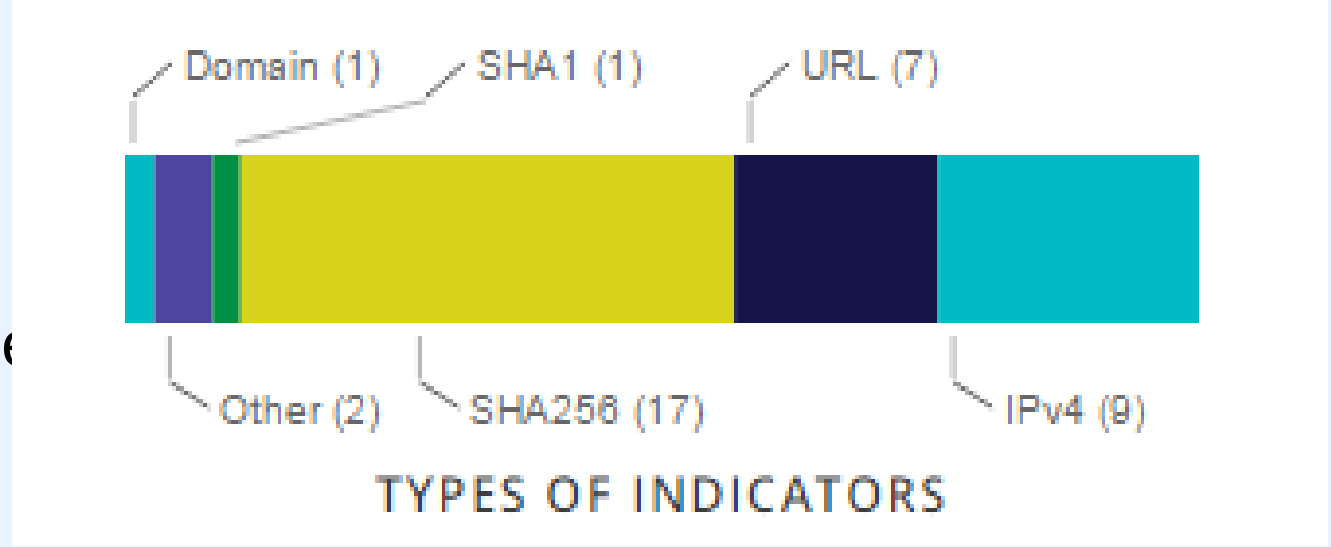
Use case: WannaCry linked Lazarus Indicators

TYPE	INDICATOR
FileHash-MD5	036bae8dd72bd70761960a90ea631ff1
FileHash-SHA256	043e0d0d8b8cda56851f5b853f244f677bd1fd..
FileHash-MD5	0489978ffa3b864ede646d0470500336
FileHash-MD5	0f246a13178841f8b324ca54696f592b
FileHash-SHA256	12d67c587e114d8dde56324741a8f04fb50cc...
IPv4	184.74.243.67
IPv4	190.185.124.125
IPv4	196.45.177.52
FileHash-MD5	1d4ec831292b611f1ff8983ebd1db5d4
IPv4	202.137.244.198

SHOWING 1 TO 10 OF 60 ENTRIES

Indicators of Compromise

- IOCs can be in a number of forms
  - File hashes (FileHash-MD5, or FileHash-SHA256, SHA1)
  - File types and file attachments
  - Domains
  - IPv4 Addresses
  - URL
  - IPv6
  - URI
  - Email
  - Mutex
  - CVE
  - Hostname
  - Others



Traffic Light Protocol (TLP)

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Adversaries

a.k.a. Dukes, Group 100
Cozy Duke, EuroAPT
CozyCar, Cozer, Office Monkeys, Cozy Bear
The Dukes, Minidionis SeaDuke

Anunak
a.k.a.
Carbanak,
Carbon Spider

APT10, menuPass, DustStorm,
Potassium, Gappyongzi

APT28, Pawn Storm, Fancy Bear, Sednit,
TsarTeam, TG-4127, Group-4127,
STRONTIUM, TAG_0700

OilRig

APT17, Deputy Dog, Group 8,
Hinden Lynx, Tailgater Team

Conclusions

- Because we cannot prevent every situation or circumstance, we must get better at detecting what can't be prevented.
- To inform any form of active response, then detection must be realtime, in line and swift.
- Awareness of situations within and around the monitored environment or assets must be gained.
- To do this, threat intelligence must be automated, and assets and the environment must be continuously threat assessed based on the particular situations.
- We need a Cyber Security Operations Centre that can help detect situations that could be prevented on stopped, and further, that is able to support realtime situational awareness.

References

1. 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 (Cyber SA 2015), joint and co-located with Cyber Science 2015 conferences, London, UK, June 8-9, 2015.
2. STIX v1.1.1, next ver 1.2 - https://stix.mitre.org/language/version1.1.1/samples.html
3. OpenIOC - http://www.openioc.org/
4. TLP - https://www.us-cert.gov/tlp
5. Threat Information Sharing Specification - https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity
6. STIX Specification and associated working groups - https://stixproject.github.io/about/
7. Threat Information Sharing Partnerships – CiSP

Thank-You ☺

Questions?

