C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

CYBER SECURITY OPERATIONS CENTRE

Security Monitoring for protecting Business and supporting Cyber Defense Strategy

Dr Cyril Onwubiko
Intelligence & Security Assurance
Research Series Limited

CYBER SECURITY OPERATIONS CENTRE

Abstract

Cyber security operations centre is an essential business control aimed at protecting ICT systems and supporting Cyber Defense Strategy. Its overarching purpose is to ensure that Incidents are identified and managed to resolution swiftly, and to maintain safe & secure business operations and services for the organisation. Further, the difficulty and benefits of operating a CSOC are explained.

CYBER SECURITY OPERATIONS CENTRE

What is a Cyber Security Operations Centre?

- It is a centre that comprises **People** (*Analyst, Operators, Administrators* etc.) who monitor ICT systems, infrastructure and applications. They use **Processes**, **Procedures** and **Technology** in order to ***deter*** computer misuse and policy violation, ***prevent*** and ***detect*** cyber attacks, security breaches, and abuse, and ***respond*** to cyber incidents.

What do they do? They

- Ensure ICT, infrastructure and business applications of an organisation are identified.
- Ensure systems, infrastructure and applications are protected.
- Ensure vulnerabilities that may exist in, and within the IT estates are identified and managed.
- Identify threats that could compromise or exploit the vulnerabilities to break in.
- Identify threat actors that could be interested or that may wish to attack the business.
- Monitor the IT estate for real-time or near real-time cyber attacks, policy violations, security breaches or anomalous and symptomatic events, or deviations.
- Profile identities that appear suspicious, interesting and 'risky'.
- Analyse events and alerts in order to determine if they are associated/related to streams of ongoing attack.
- Analyse historical events logs for patterns and trends (trending) symptomatic of an attack / compromise.
- Triage and investigate incidents.
- Coordinate, contain and respond to cyber incidents.
- Provide report and management information.

CYBER SECURITY OPERATIONS CENTRE

Why Cyber Security Operations Centre?

Jan 2015: The US Central Command (Centcom Twitter account was hacked by a group who call themselves the CyberCaliphate

Dec. 2014: SONY suffered an unprecedented Cyber attacks to its Gaming and Film platforms!

2011: IPR theft of the RSA SecurID system and software – believed to be State sponsored.

Aug. 2014: Contact information >76 million households and about 7 million small businesses **were compromised in a cybersecurity attack**

www.C-MRiC.ORG

submission@C-MRiC.ORG

@CMRiCORG

CYBER SECURITY OPERATIONS CENTRE

Why Cyber Security Operations Centre?

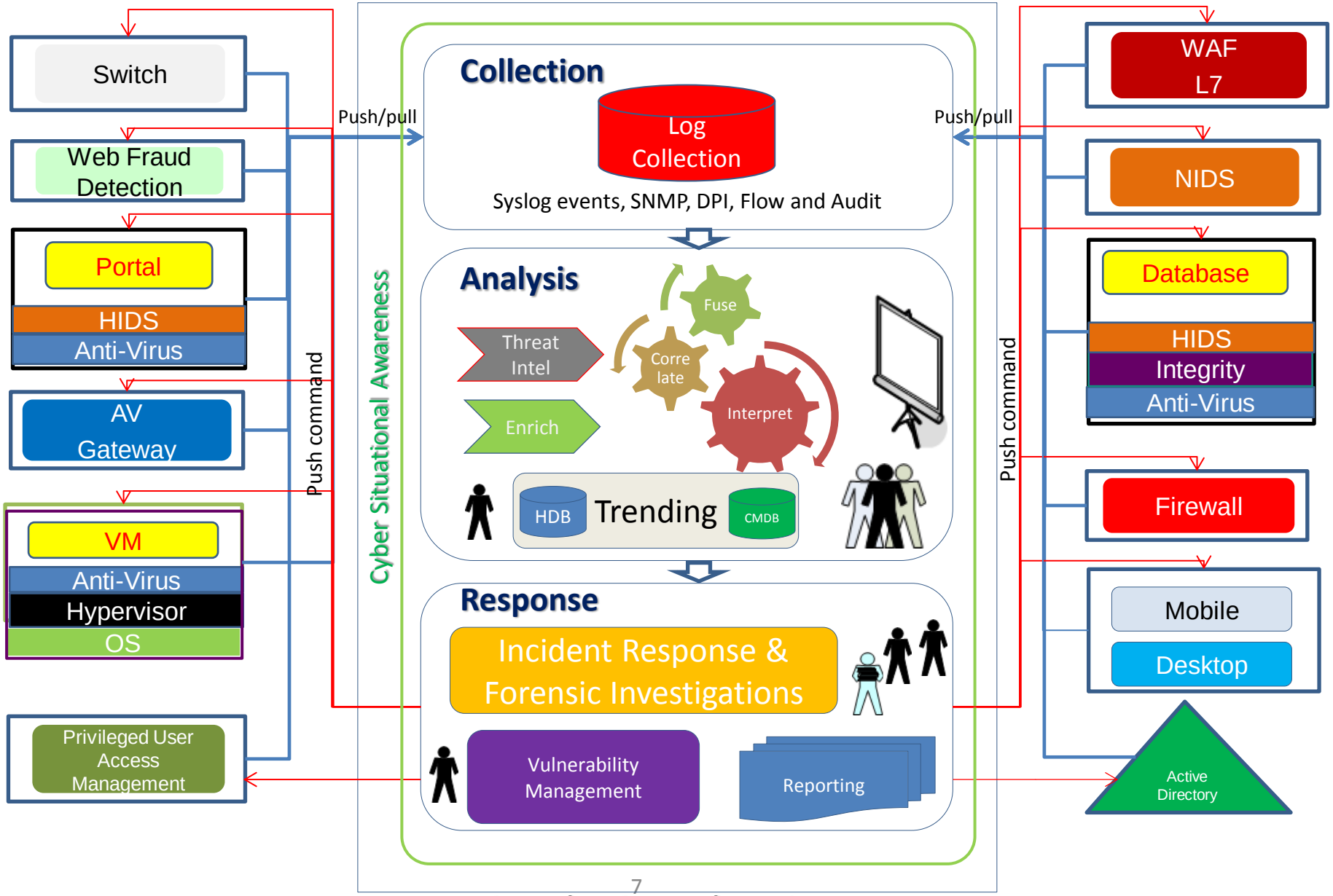
- **Volume:** Some Organisation posses myriad of devices in their IT estate, many of which are no longer managed, unsupported or legacy.
- **Information / Data:** All Organisation have various data that need to be protected such as Customer records, Student records, Citizens data, Bank/financial records, IP (Intellectual Property) etc.
- **Growth:** There's increasing growth in organisation user base, information and data. Networks are extended and expanded to accommodate collaboration, partnerships etc. Hence, isolated and localised point solutions struggle to protect the enterprise.
- **Point Solution Management:** Localised and point solution devices (log sources) need to be monitored, and properly managed, too.
- **Borderless Perimeter:** Collaboration, partnerships etc. and new ways of doing business (internet/eCommerce) means the boundary/perimeter is no longer 'hard' but 'soft'.
- **Privileged User Abuse:** Trusted users with privileged access can turn rogue, such risk must be monitored, mitigated and managed.

CYBER SECURITY OPERATIONS CENTRE

Cyber Security Facts

1. Cyber incidents will always occur.
2. No Organisation is safe.
3. Every system, network, infrastructure or application can be attacked or hacked.
4. Vulnerability exists in every asset/organisation.
5. Risk mitigation is always a proportionality proposition.
6. Cyber landscape is constantly increasing (LAN, MAN, WAN, Internet, Cloud Computing, IoT, IoET etc.).
7. Technology is continuously evolving and complex.
8. Attack surface is growing.
9. Impacts of Cyber attacks can result to significant losses.
10. Attack methods are increasingly complex and well-thought.

CYBER SECURITY OPERATIONS

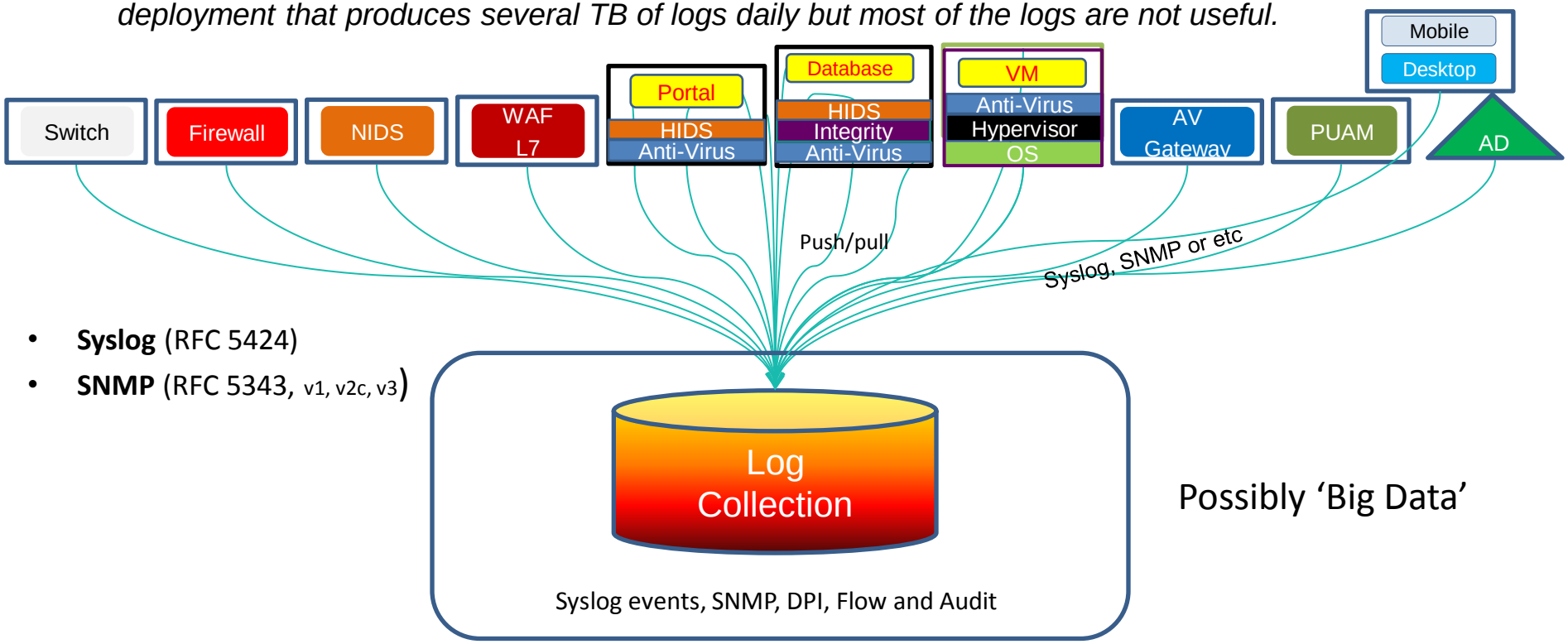


Security Operations Centre

LOG COLLECTION

'Potential to do'

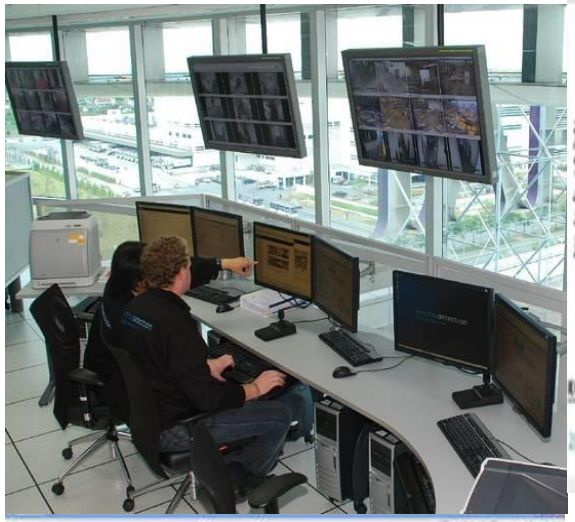
- Every ICT should be configured to produce event logs.
- SIEMs are used to collect events logs of most formats.
- Most SIEMs have the capability to collect logs (push/pull) from a number of Log Sources.
- However, the deployment must enable this to happen!
- System Audit policy must be enabled, and audit logs must be consumed.
- The right events **must** be logged (to providing the right set of accounting data) – *I have seen a deployment that produces several TB of logs daily but most of the logs are not useful.*

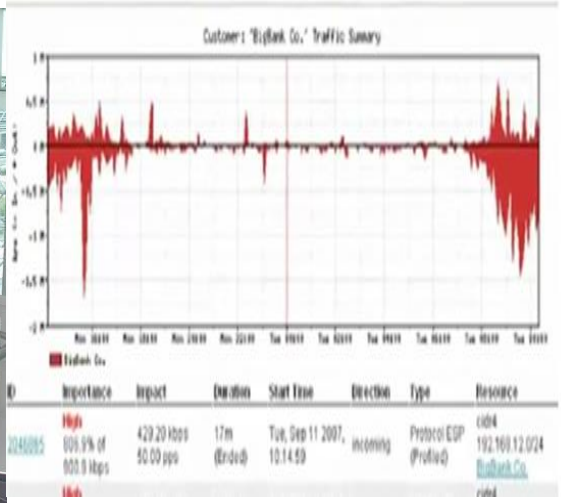


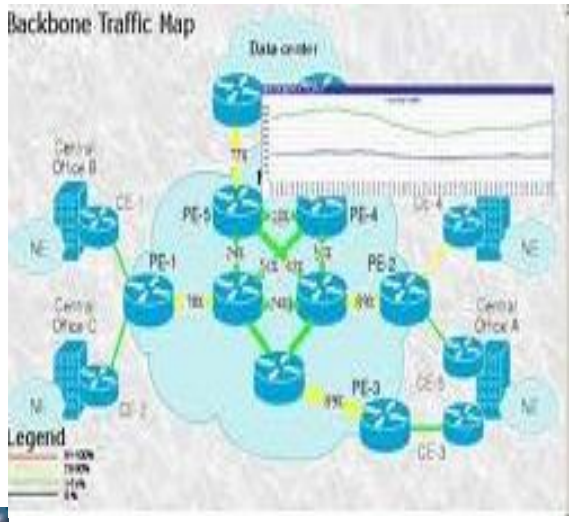
- **Syslog** (RFC 5424)
- **SNMP** (RFC 5343, v1, v2c, v3)

Possibly 'Big Data'

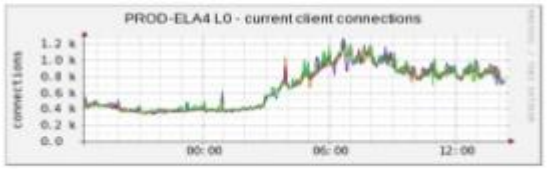
SECURITY MONITORING

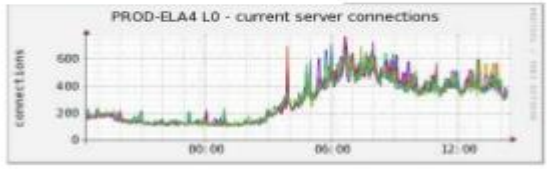






Monitoring:



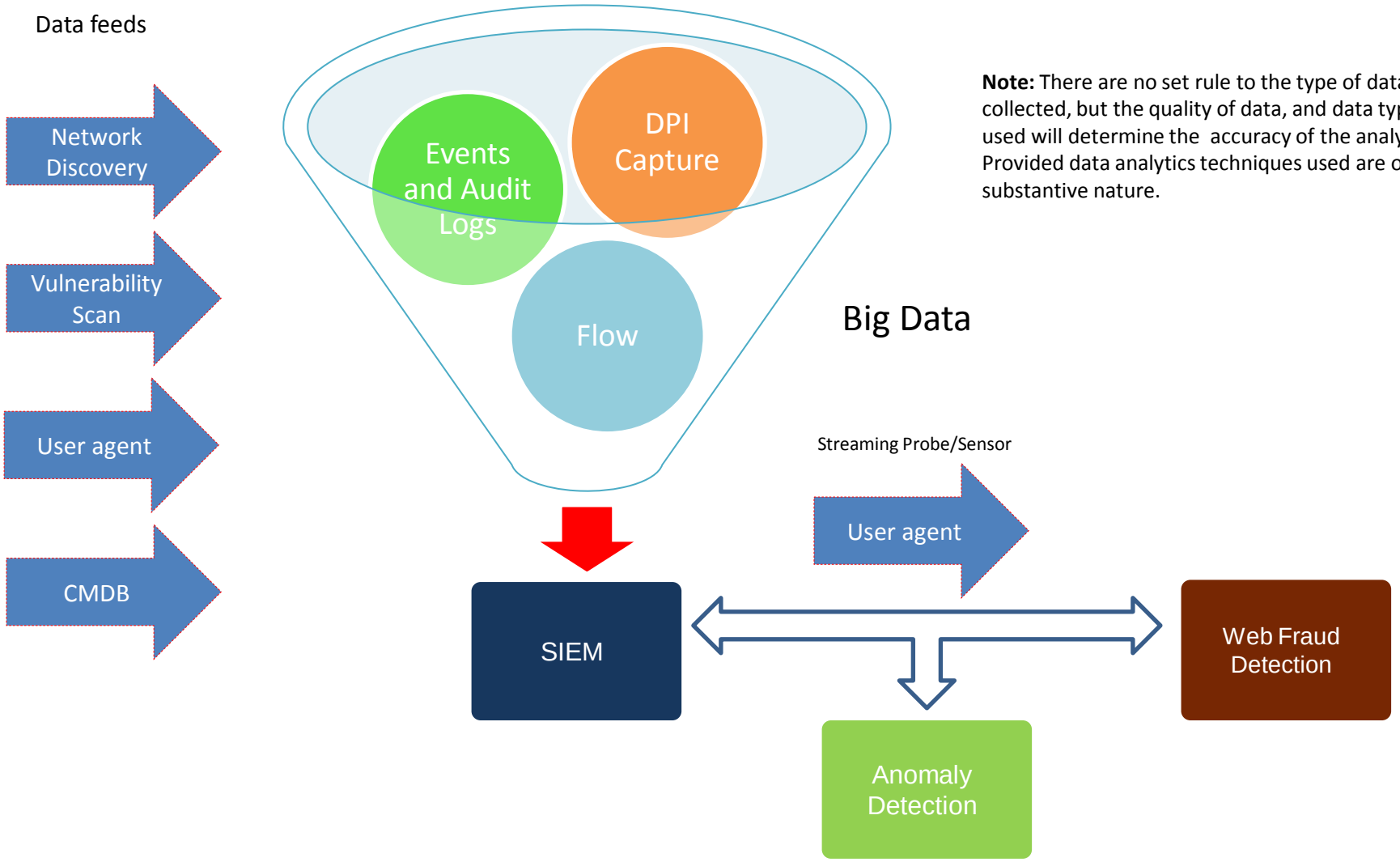


www.C-MRiC.ORG

submission@C-MRiC.ORG

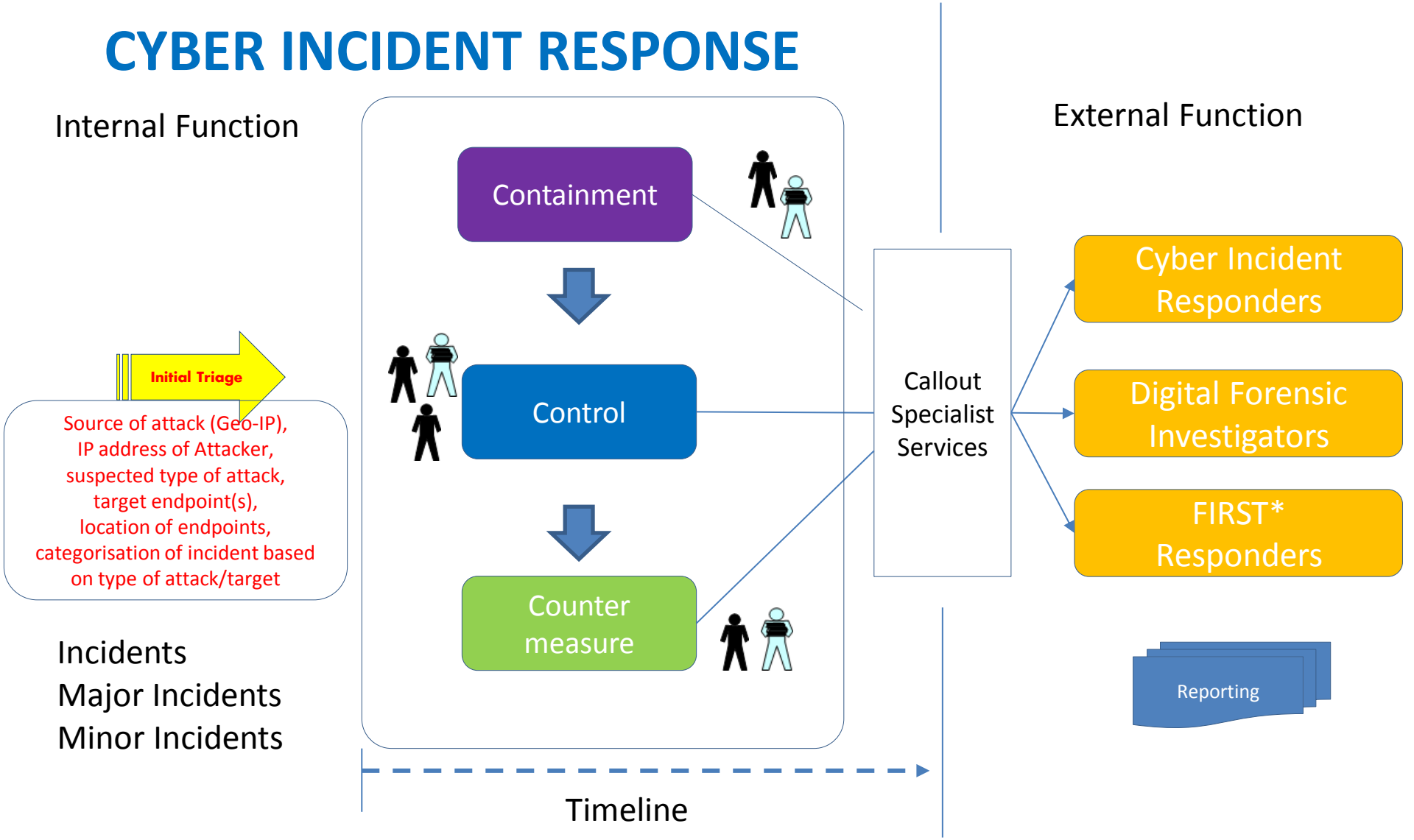
@CMRiCORG

ANALYSIS



Note: There are no set rule to the type of data collected, but the quality of data, and data types used will determine the accuracy of the analysis. Provided data analytics techniques used are of substantive nature.

CYBER INCIDENT RESPONSE



- Time is of essence / critical
- Major incident escalation / reporting and mitigation in minutes (approx.)

** FIRST – Forum of Incident Response and Security Teams*

www.C-MRiC.ORG

submission@C-MRiC.ORG

@CMRiCORG

PEOPLE – ANALYSTS, OPERATORS, ADMINS, ARCHITECTS, ENGINEERS ETC.

1. People are as important as Technology.
2. Analysts & Operators must be well trained and skilled.
3. Processes must exist, and should be followed, and policies must be adhered.
4. Cyber operations require specialist skills, and continuous investments in – training, courses, certifications, memberships
5. The best Cyber operations can only be achieved through people. 'Man in the loop'.
6. People are always the weakness link ☺

REPORTING – MANAGEMENT INFORMATION

Report against the useful indicators important to the business, driving by stakeholders (senior Exec, and Analysts, too)

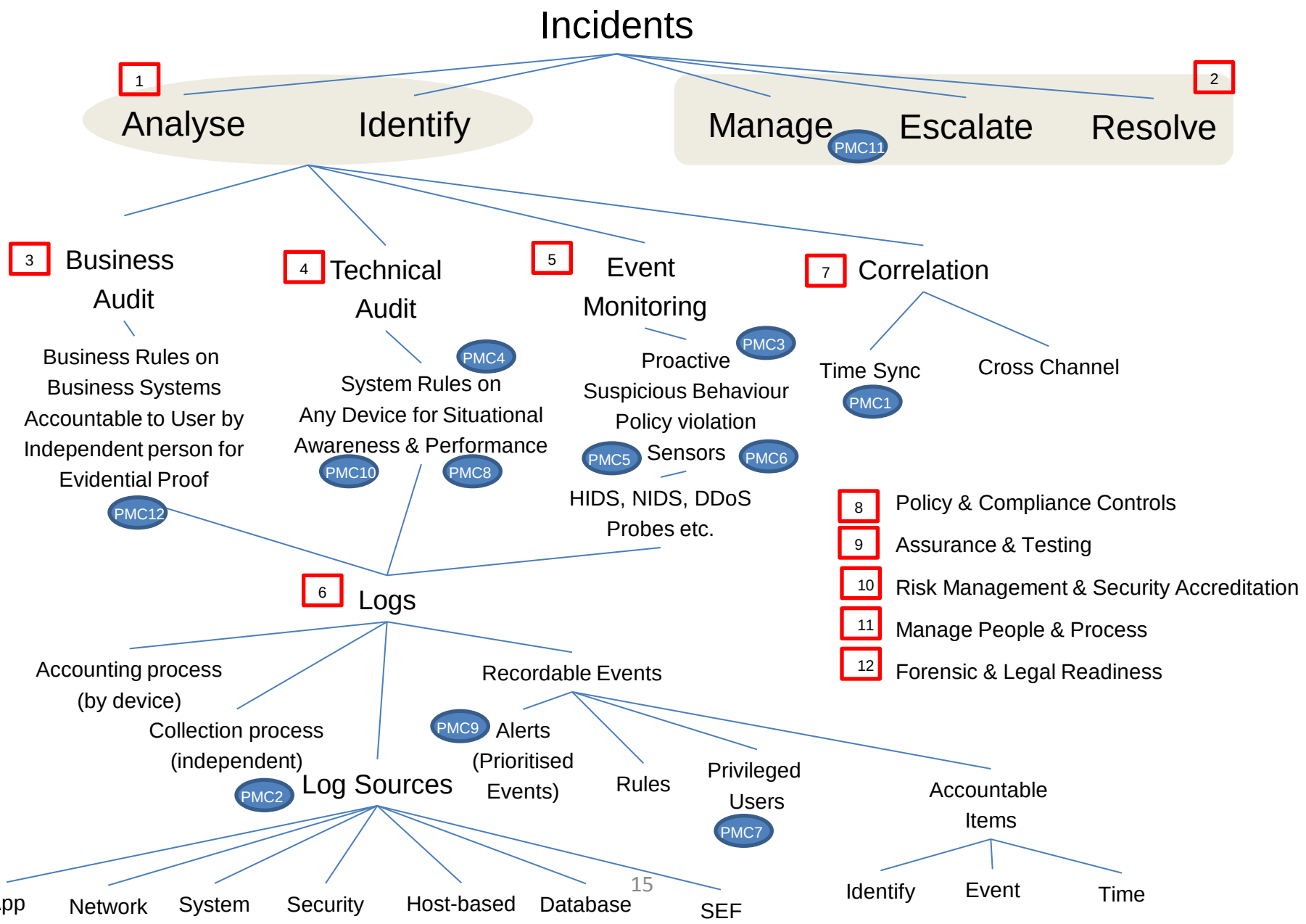
S/N	Sample Important Elements of Cyber Reports
1	Report against SLAs.
2	Performance of the Cyber operations (RoC*, false negative vs false positive vs real negative vs real positive).
3	Rolling "top 5" Cyber Attacks, Geography of origin of the attack.
4	Summary of Internal violations – Privileged User misuse/abuse
5	Summary of current Policy Violations

*ROC – Receiver operating characteristics

SOC – LEGAL CONSIDERATIONS

1. Users must be informed when a SOC is implemented, and what monitoring will occur, what information will be collected, and what the intended uses will be.
2. Policy and standards must be defined, adhered and made relevant
3. Consider wider Directives – EU Directives, DPA, DPP, ICO
4. Consider Laws – Legislations, Compliance mandates etc.
5. Involve Legal and HR Teams

CYBER SECURITY OPERATIONS CENTRE STRATEGY



CYBER SECURITY OPERATIONS CENTRE OBJECTIVES

The 12 Aspects include:

CONCLUSION

1. CSOC is an essential business control to ensure safe and secure business operations and services, esp. online digital service.
2. Business requirements should drive cyber security strategy, and CSOC capabilities & scope.
3. Continuous improvements , including lesson learned should be encouraged.
4. Cyber incident will happen, and every organisation should have proportionate incident response and management strategy, and incident readiness processes in place.
5. Forensic readiness should be considered important and business requirements should focus on this.
6. People and process are the key, while technology is equally important too.
7. Staff training and development should be considered essential.

REFERENCES / SOURCES

1. HMG Government – www.gov.uk
2. CESG Polices & Guidance - http://www.cesg.gov.uk/PolicyGuidance/Pages/index.aspx
3. The UK Cyber Security Strategy - https://www.gov.uk/government/publications/cyber-security-strategy
4. HMG Security Policy Framework - https://www.gov.uk/government/publications/security-policy-framework
5. HMG Good Practice Guide #13 – Protective Monitoring of HMG ICT Systems
6. HMG Good Practice Guide #53 – Transaction Monitoring for HMG Online Service Providers - https://www.gov.uk/government/publications/transaction-monitoring-for-hmg-online-service-providers
7. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271268/GPG_53_Transaction_Monitoring_issue_1-1_April_2013.pdf
8. 10 Steps to Cyber Security - https://www.cesg.gov.uk/News/Pages/10-Steps-to-Cyber-Security.aspx
9. Cyber Essentials Scheme - https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
10. NIST 800-Series – (SP 800-137) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organisations - http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
11. Reducing the Cyber Risk in 10 Critical Areas - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf
12. FIRST – Forum of Incident Response and Security Teams - https://www.first.org/about/organization/teams
13. User Agent (HTTP) - http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html
14. Syslog Standard (IETF 5424) - https://tools.ietf.org/html/rfc5424
15. Renaud Bidou – “Security Operation Center Concepts & Implementation”
16. Cyril Onwubiko & Thomas Owens - “Situational Awareness in Computer Network Defense: Principles, Methods & Applications”

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

CONTACT

Dr Cyril Onwubiko[1, 2]

[1]Chair – Intelligence & Security Assurance

E-Security Group, Research Series

cyril@research-series.com

[2]Steering Committee Chair

Cyber Science 2015

C-MRiC.ORG