University of BRISTOL

CyBOK

Security Operations & Incident Management KA

Hervé DEBAR

University of BRISTOL

CyBOK

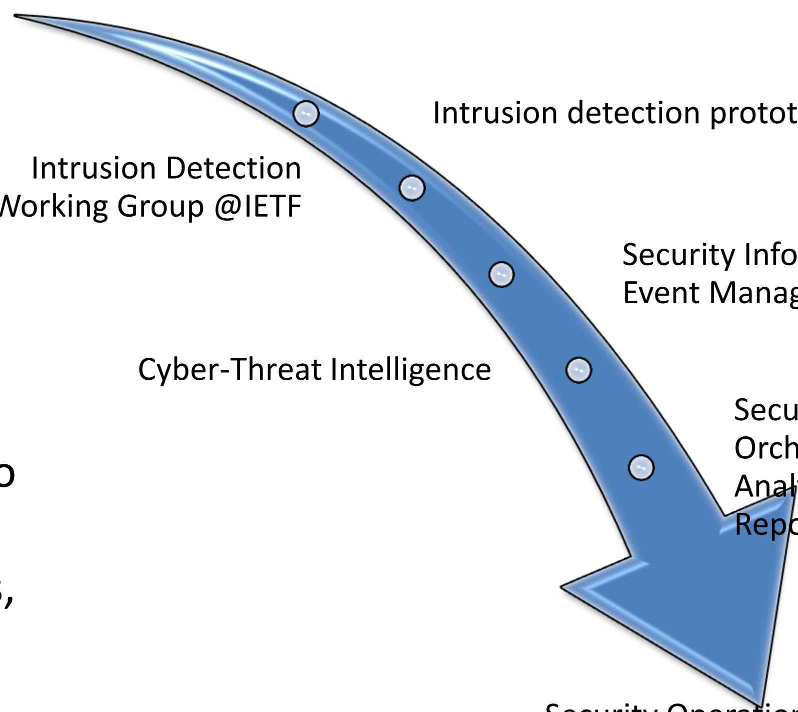
The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

bristol.ac.uk

What is it about ?

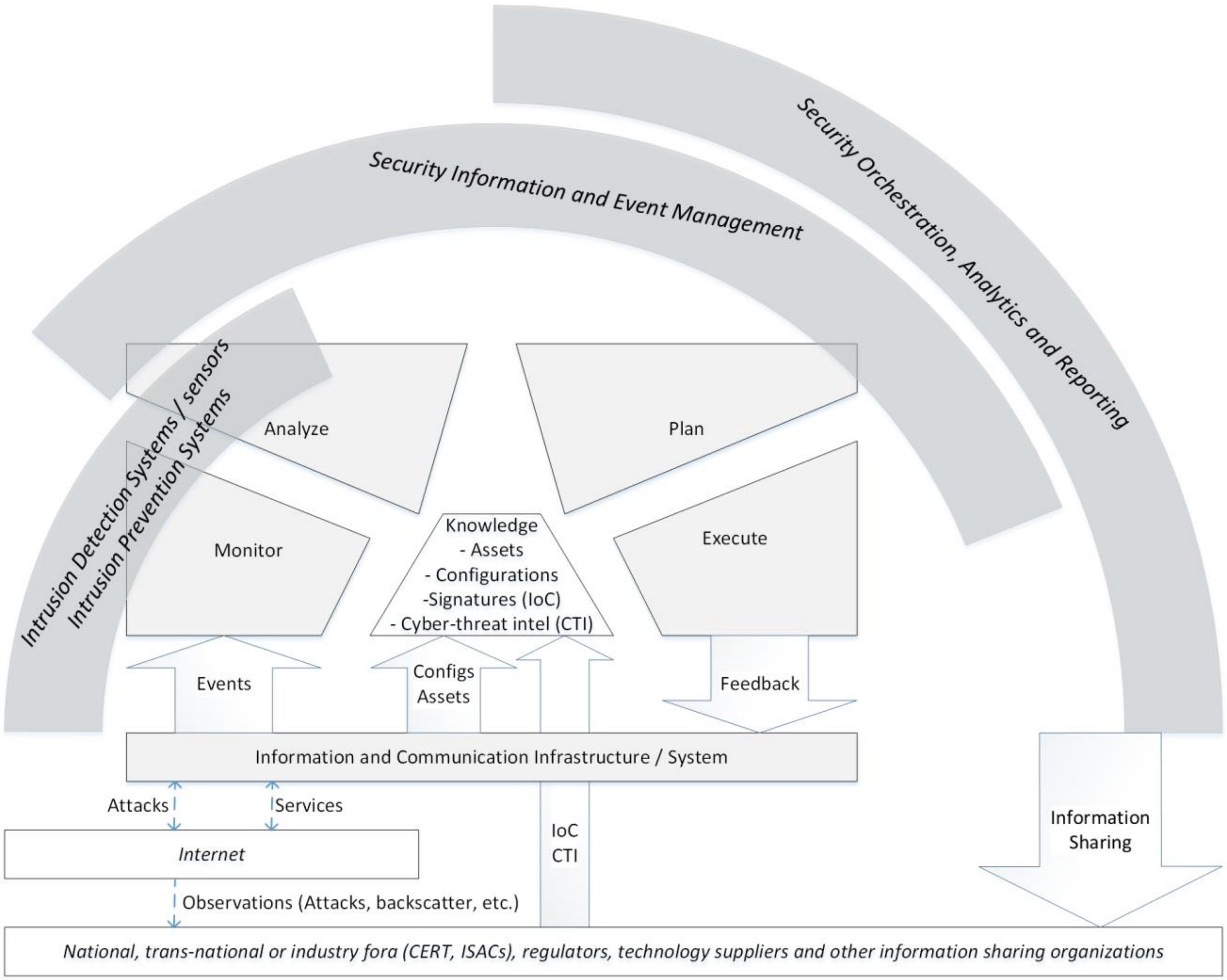
- Information systems are targets of attacks
  - Resources
  - Information
- Full protection is impossible
  - Limits use
  - Cost
- Detecting attacks as early as possible is the next best option

Timeline and scope



Needs have evolved to meet the increasing complexity of systems, services and attacks.

Overall MAPE-K loop



Components of MAPE-K
Monitor-Analyse-Plan-Execute

- Intrusion detection systems (IDS)
  - Monitor systems and networks to create or collect execution traces
  - Analyse them (in real time) to detect issues and provide alerts
- Security Information and Event Management (SIEM) platforms
  - Analyse events and alerts to triage them according to their impact; identify incidents
  - Plan: select potential responses to incidents
  - Execute: push recommendations to system and network analysts
- Security Orchestration, Analytics and Reporting (SOAR) platforms
  - Analyse further the collected information (events, alerts, incidents)
  - Plan: assess response plans according to business impact
  - Execute: partially automate deployment of response plans

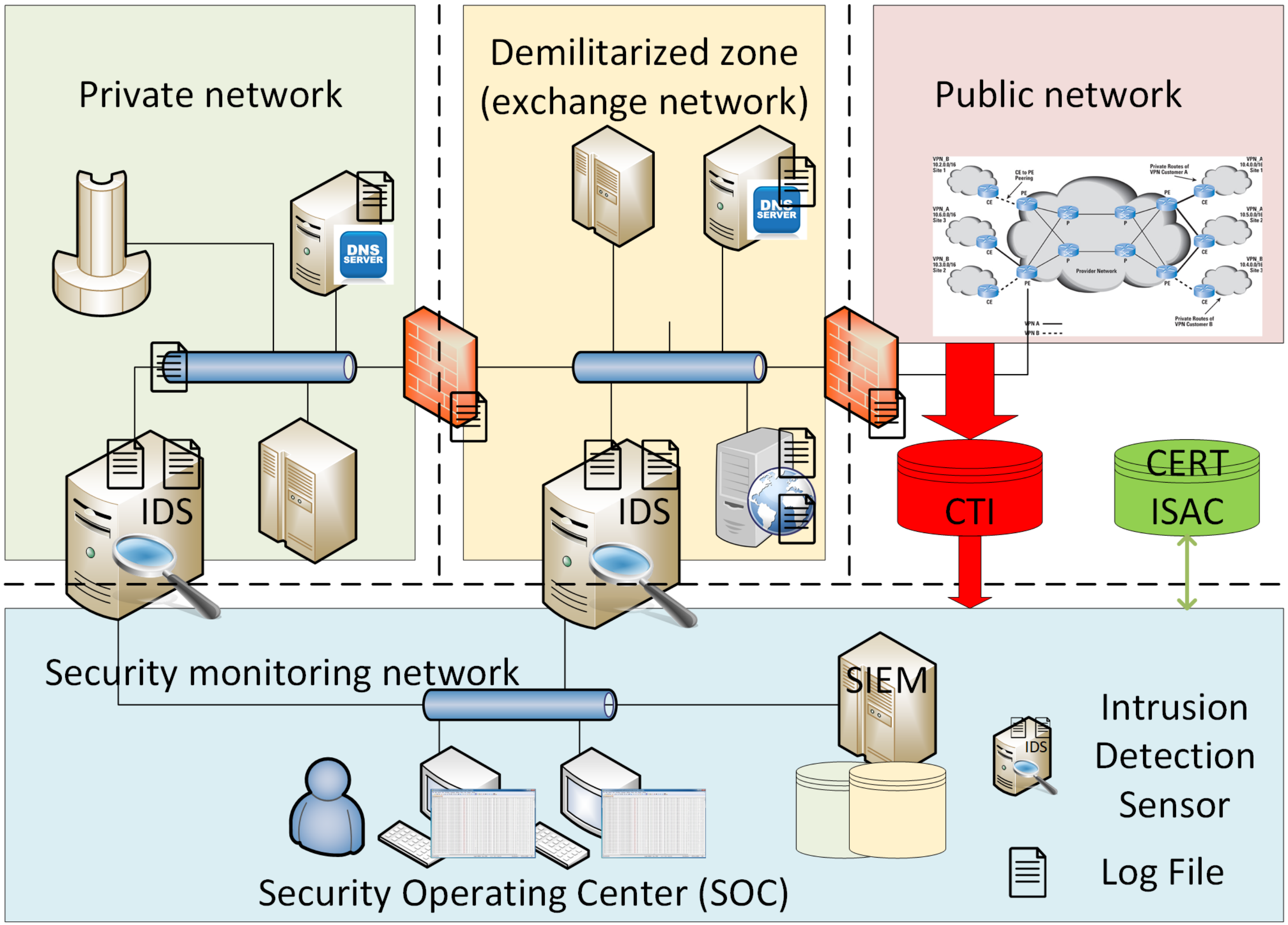
Deployment of SOIM technologies

CyBOK

- Segmentation of the network in zones
  - Sensitivity
  - Quantity of exchanges
- Sensors and log feeds deployed to collect traces and detect malicious behaviour
- Private network to gather event and alert feeds
- SIEM platform to manage events, alerts and incidents
  - Technical support of Security Operating Centre (SOC)

Typical architecture

CyBOK



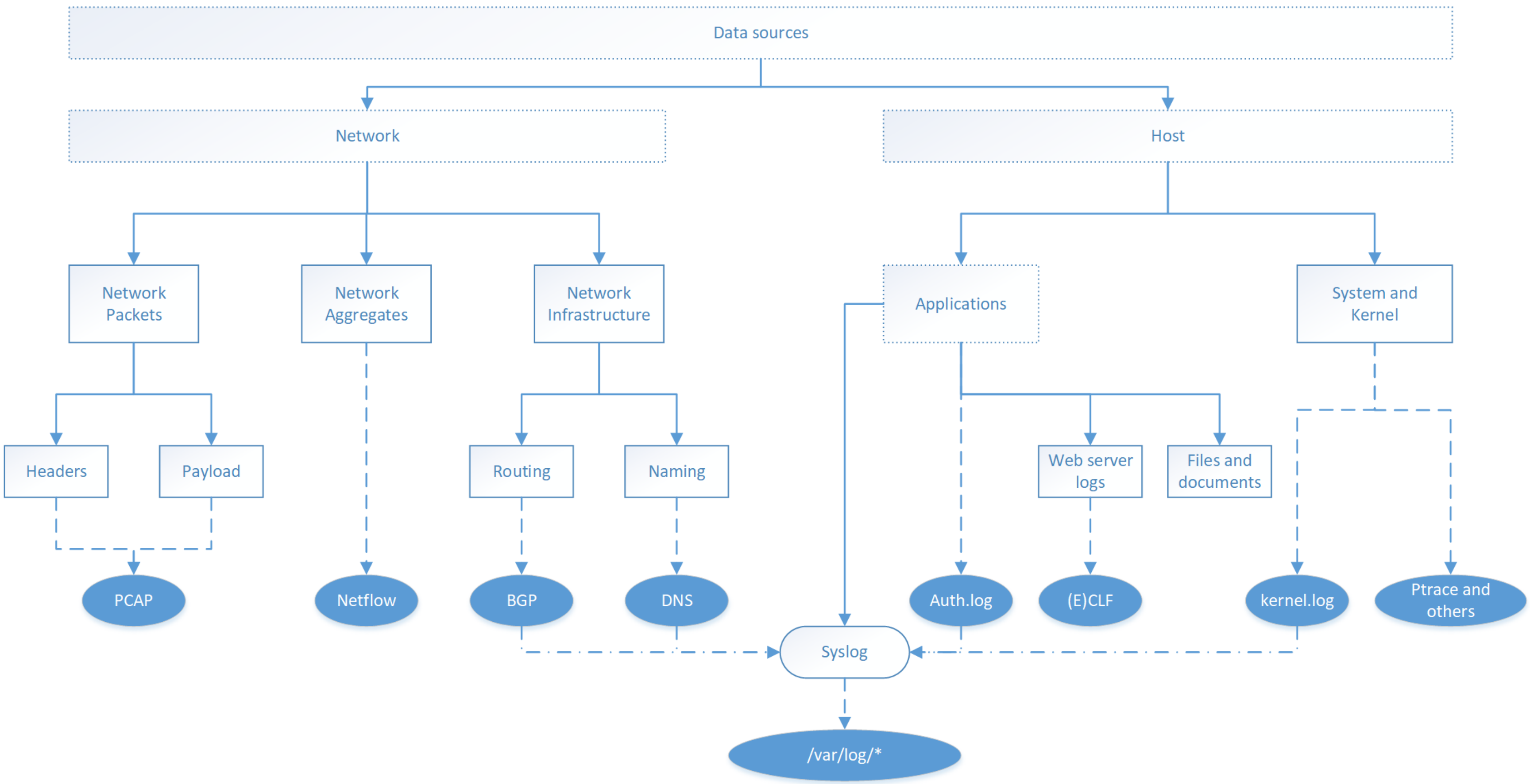
Intrusion Detection and Prevention Systems

From events and traces to alerts

Intrusion Detection

- Process traces of execution
  - Representative of the activity of a « system »
  - Enable differentiation between normal and malicious activity
- Separate appropriate from malicious activity
  - Rationale for suspicion (what)
  - « Evidence » if possible (why)
  - Levels of suspicion frequently used
- Raise alert: symptom of misbehaviour

Data sources



Network data sources: Possible detections

- Network packets
  - Carriers of attacks (e.g. malware in payload)
  - Symptoms of compromise (e.g. connection to Command&Control infrastructure)
- Network aggregates
  - Deviations in traffic patterns (ports, conversations, volume)
- Network infrastructure
  - Use of the Domain Name System (DNS) for command and control
  - Manipulation of the routing infrastructure to reroute traffic or hide malicious activity

Application data sources

- Traces provided by applications related to their runtime behaviour
  - Web servers in particular
  - Representing specific activity
- Usually collected through system mechanisms
  - Unix: /var/log
  - Syslog
- Also includes documents
  - Complicated parsing

System data sources

- Kernel logs
  - Intercepted very low in the execution path (assembly)
  - Focusing on malware detection

- Interest in the Android ecosystem
  - Understand interactions between apps and supporting libraries
  - Call-back mechanism obscures malicious activities

Syslog

- Generic logging infrastructure
- Entry composed of
  - Timestamp
  - Hostname
  - Process
  - Priority
  - PID
  - Message
- Extremely useful both for event and alert management

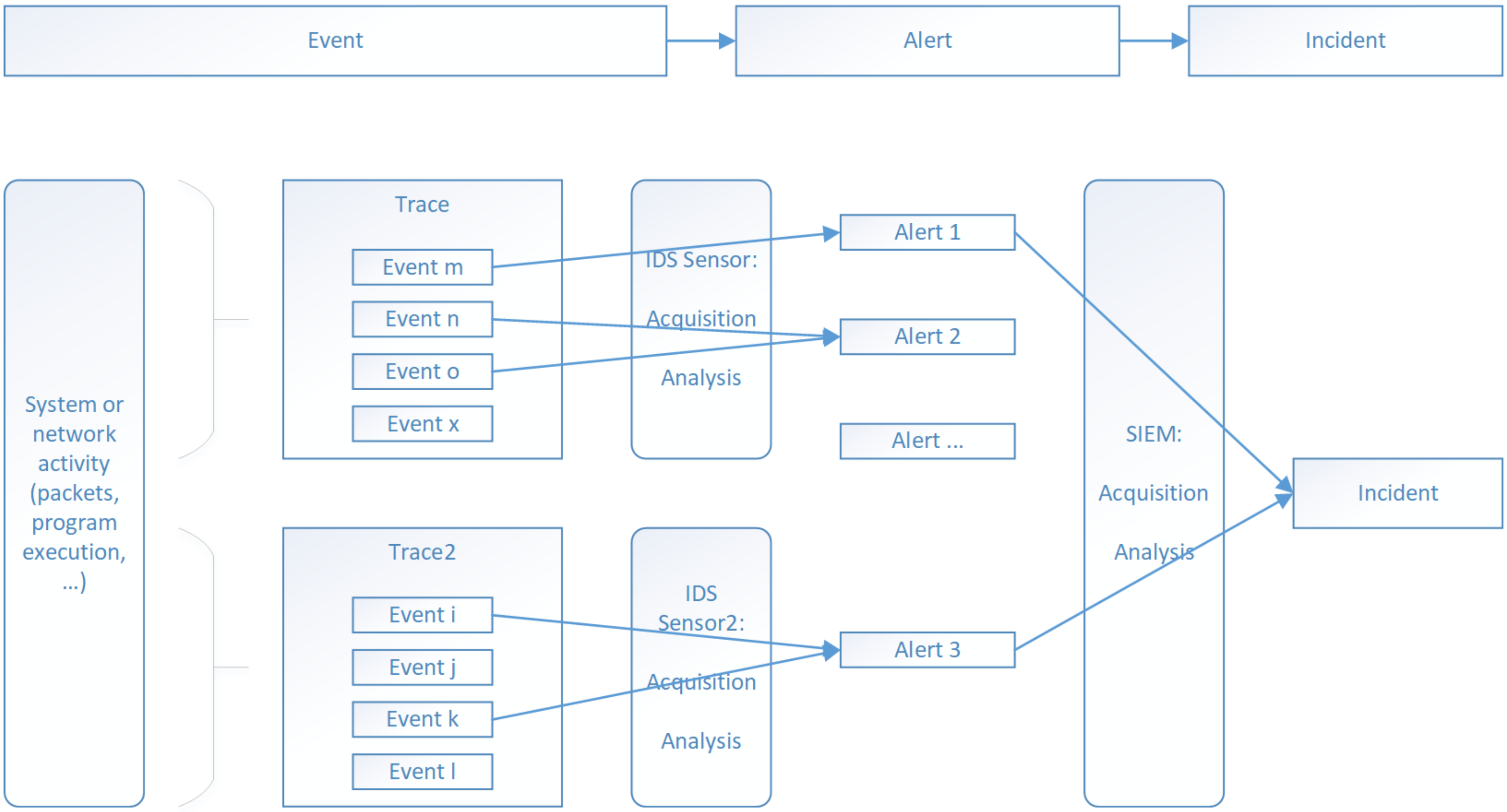
Frequent data sources issues

- Normalization, canonization and labelling
  - Syntax of the data
  - Semantic of the data
- Transformation to meet needs of detection algorithms
  - E.g. transform text data in numerical form
- Encrypted data flows
  - Access limited to the outer envelope of the data
- Voluminous data flows
  - Limits transportation and storage
- Personally Identifiable Information (PII)
  - Conflict between technical data and PII: network addresses

Analysis of traces

- Objective : generate incidents from alerts and events
- Intrusion detection sensors
  - Deployed in the field
  - Collect event information
  - Produce alerts
- Analysis techniques
  - Misuse detection
  - Anomaly detection

From Event to Incident



Misuse detection

- Gather knowledge about attack processes
- Model occurrence of attack in traces
  – Signatures
- Detect presence of such occurrence in current trace
- Advantage
  – Alerts are qualified by a root cause
- Drawback
  – Management of attack process knowledge
    - Expertise and time

Anomaly detection

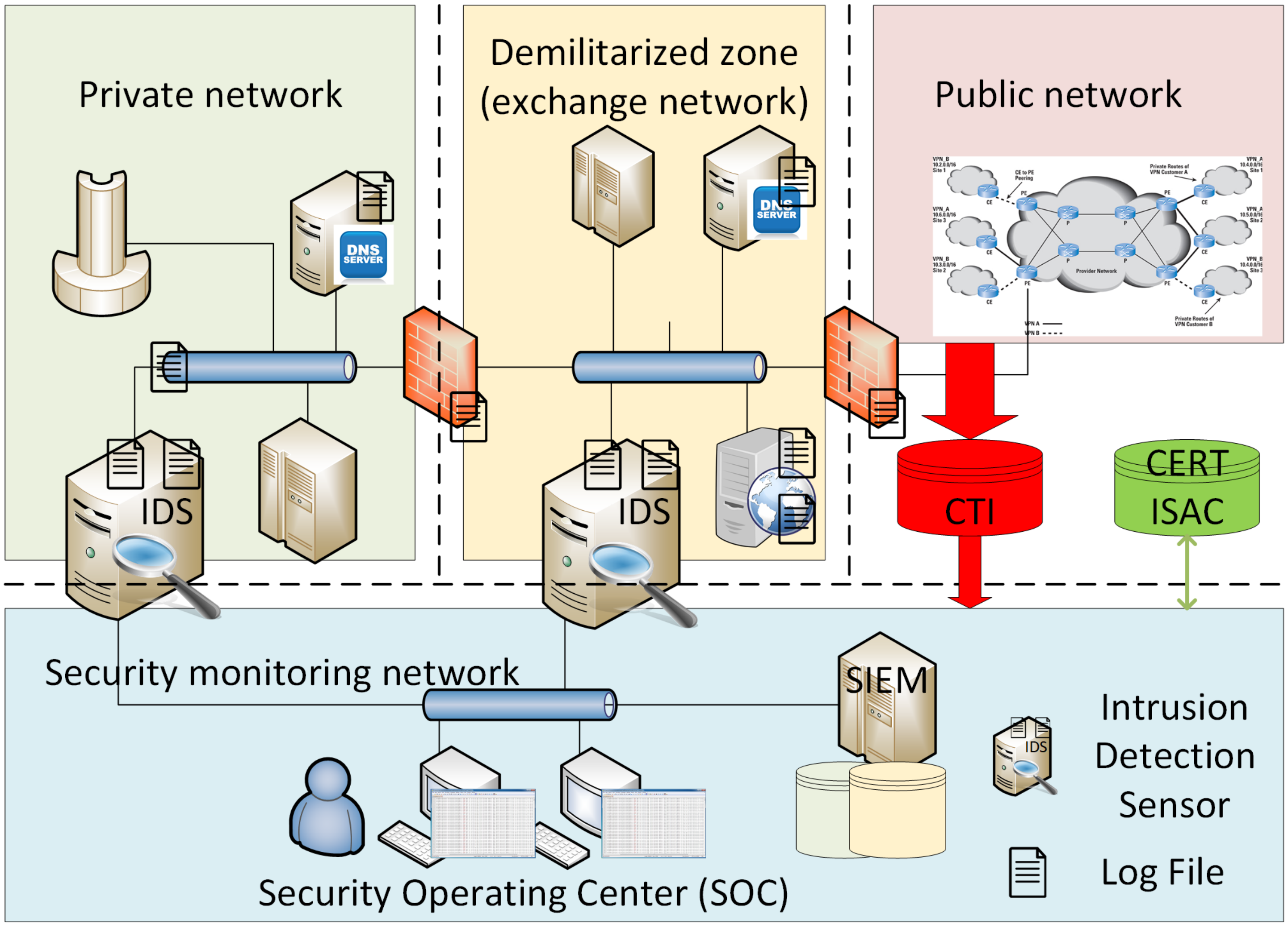
- Gather knowledge about process behaviour
  - Expected behaviour (e.g. standards and policies)
  - Behaviour learned through observation
    - Machine learning
- Detect presence of such occurrence in current trace
  - Define deviation from the norm
- Advantage
  - Unknown attack processes are detected by their side effects
- Drawback
  - Diagnosis of alert impact
  - Selection of behavioural model (many possibilities)
  - Attack-free training (ground truth)

General intrusion detection issues

- False positives
- False negatives
- Base-rate fallacy
  - Magnitude of difference between the volume of attacks and the volume of normal activity in traces
- Metrics for testing and evaluation

Security Information and Event Management

Typical architecture



Data collection in SIEMs

- Definition of
  - Schema: structure and semantic of messages
  - Encoding: transformation of message in bit string
  - Transport protocol

Format	Owner	Transport	Encoding	Structure	Number of attributes
CEF	HP/Arcsight	Syslog	Key/value	Flat	117
LEEF	IBM/QRadar	Syslog	Key/value	Flat	50
CIM	DMTF	Any	(XML)	UML	58
CADF	The Open Group (NetIQ)	Any	(JSON)	Classes	48
CEE	MITRE	(Syslog)	JSON, XML	Structured	56
IDMEF	IETF	IDXP	XML	UML	166

Alert correlation

- Objectives
  - Reduce the number of alerts to process
  - Automatically identify false positives
  - Group alerts into incidents
  - Propose remediations
- Correlations techniques
  - Alerts sharing the same characteristics (addresses, ports, etc.)
  - Alerts associated with contextual information
    - Environment
    - Cyber-Threat Intelligence
    - Information exchange

Mitigations and countermeasures

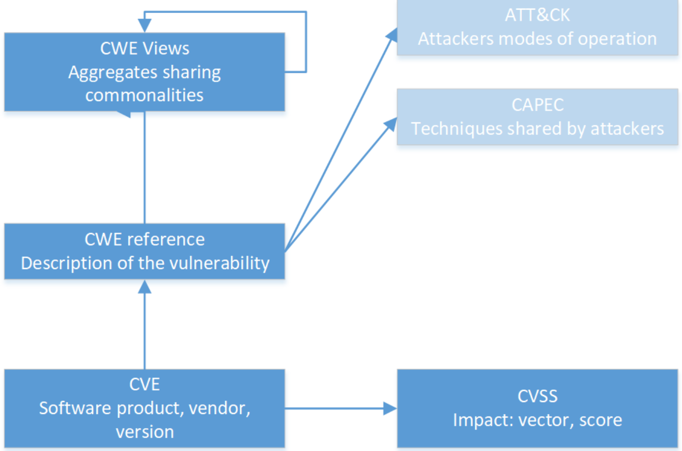
Objective: block attacks

Tools and techniques

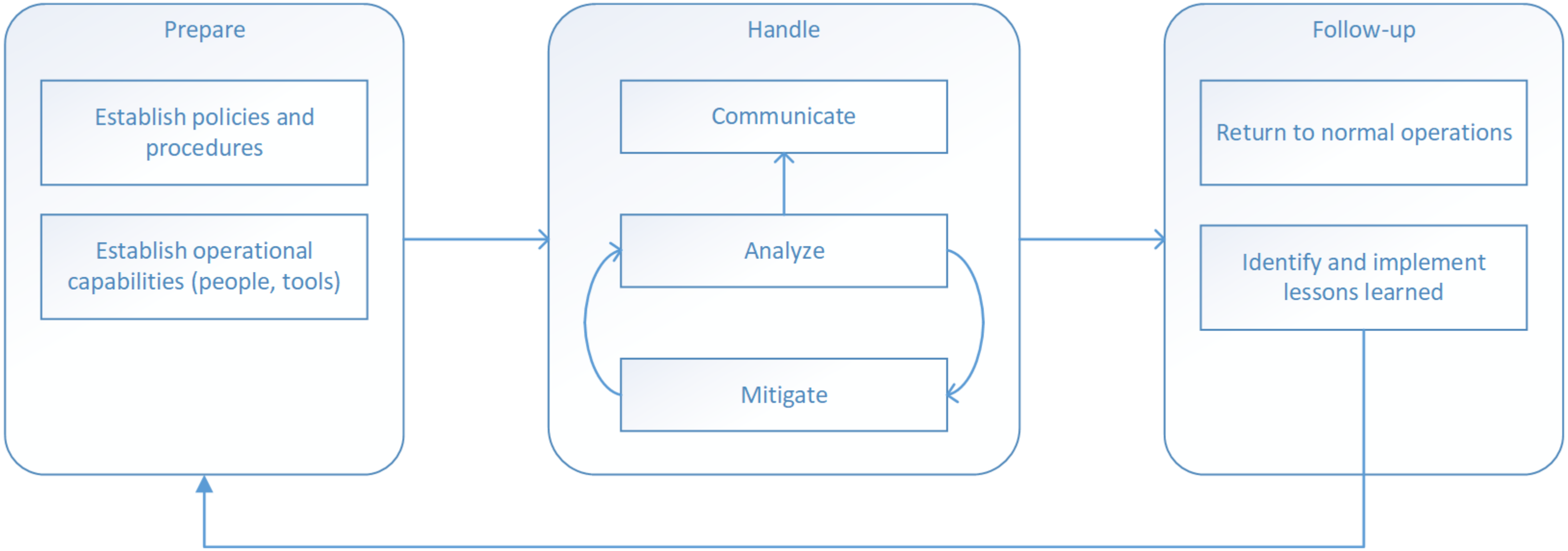
- Intrusion Prevention Systems
  - Immediately apply remediation to the data stream upon detection
  - Block or terminate connections at the network level
  - Change content (a.k.a. virtual patching)
- Traffic management for denial of service attacks
  - Dedicated tunnels
  - Anycast
- Impact and risk assessment
  - Understand the business risk associated with the incident

Intelligence and Analytics

- Relevant normalized knowledge sources
  - Common vulnerabilities and exposures
  - Common vulnerability scoring system
  - Common Weakness Enumeration
  - Common Attack Pattern Enumeration and Classification
  - Adversarial Tactics, Techniques & Common Knowledge
- Honeypots and honeynets
- Cyber-Threat Intelligence
  - Understand malicious activity in the Internet
  - Identify relevant threats and deploy detection/protection means
  - Share compromise information
    - Information Sharing and Analysis Centres



Incident Management Lifecycle



Conclusion

- Security Operations and Incident Management increasingly relevant
  - Wide range of connected devices
  - Complex dynamic systems
    - DevOps
- Require skilled personnel
  - Automation
  - Decision support