SUPERVISION DE SÉCURITÉ - SECURITY INFORMATION AND INCIDENT MANAGEMENT

HERVÉ DEBAR
TÉLÉCOM SUDPARIS

Information systems are targets of attacks

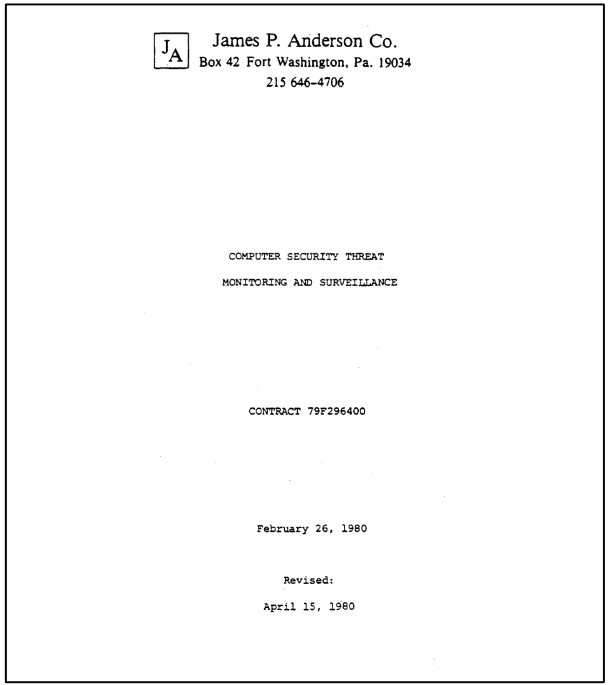
Resources
Information

Full protection is impossible or impractical

Limits use and scalability
Cost
Management

Detecting attacks as early as possible is the next best option

And deploying appropriate remediation



James P. Anderson Co.
Box 42 Fort Washington, Pa. 19034
215 646-4706

COMPUTER SECURITY THREAT

MONITORING AND SURVEILLANCE

CONTRACT 79F296400

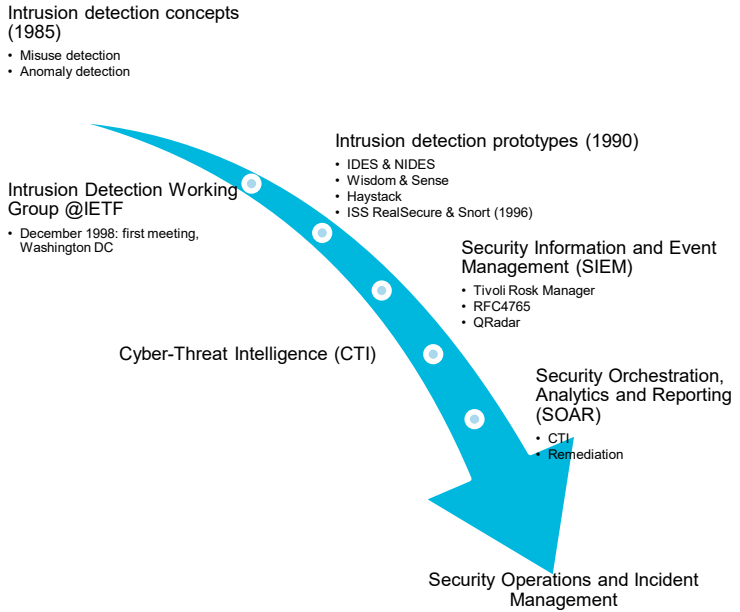
February 26, 1980

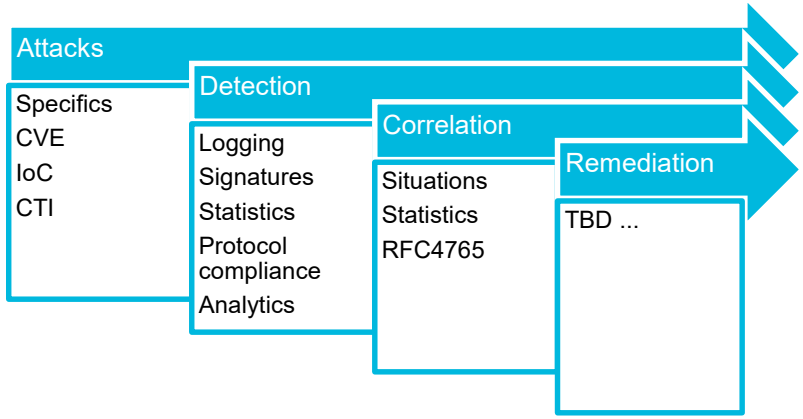
Revised:

April 15, 1980

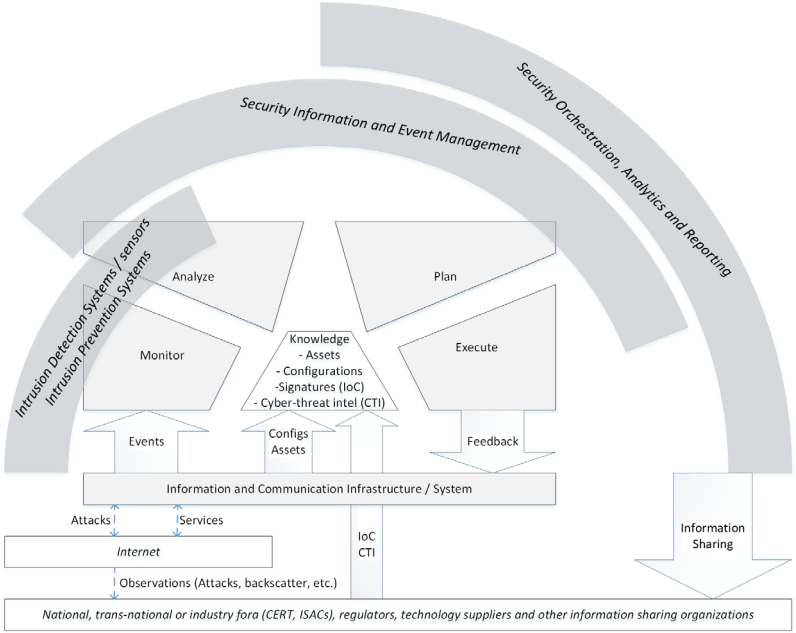
TABLE OF CONTENTS

TIMELINE AND SCOPE





https://csrc.nist.rip/publications/history/



Supervision is about information management

Logs and others
Processing
Decision
Feedback & control

Many actors with conflicting interests

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

Segmentation of the network in zones

Sensitivity
Quantity of exchanges

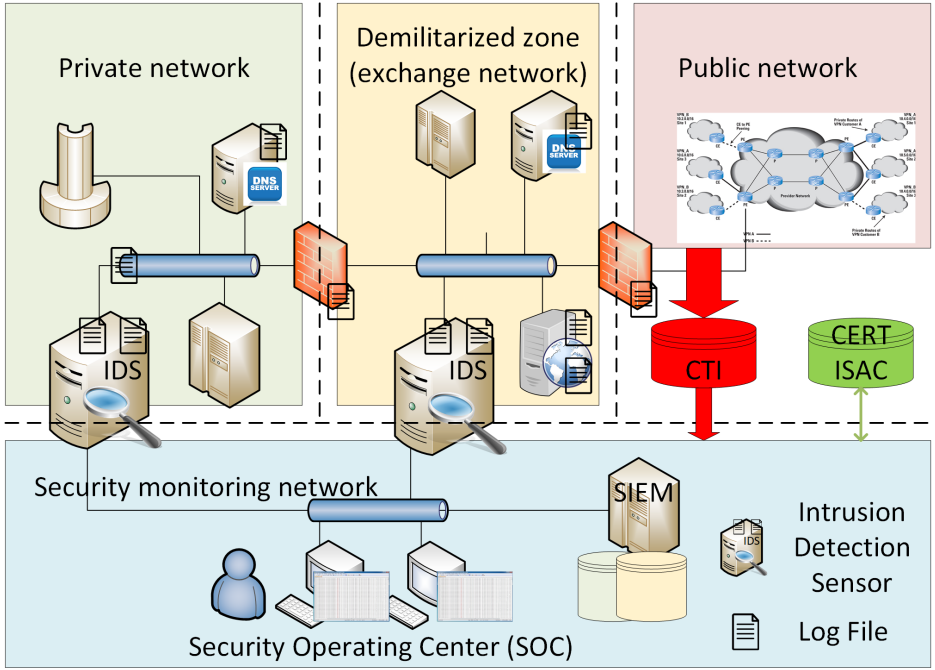
Sensors and log feeds deployed to collect traces and detect malicious behaviour

Private network to gather event and alert feeds

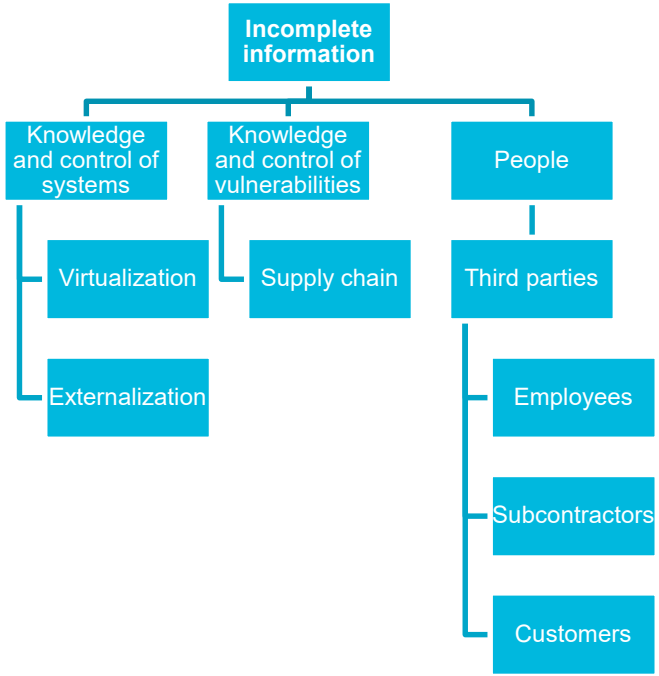
SIEM platform to manage events, alerts and incidents

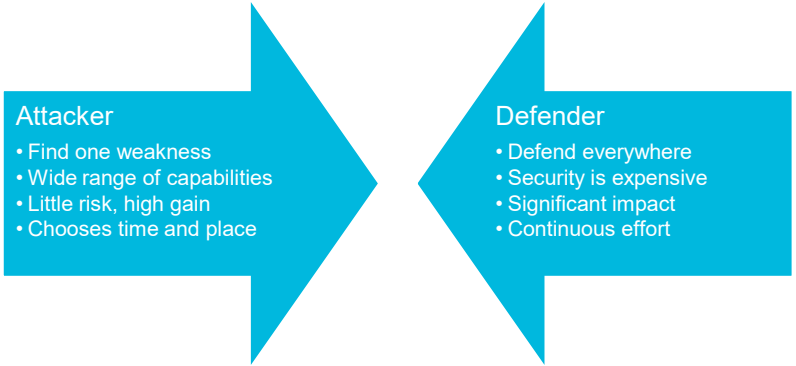
Technical support of Security Operating Centre (SOC)

TYPICAL ARCHITECTURE



TWO PROBLEMATIC CHARACTERISTICS





Any contribution must include a relevant threat model and demonstrate progress w.r.t the threat model.

INTRUSION DETECTION AND PREVENTION SYSTEMS
FROM EVENTS AND TRACES TO ALERTS

Process traces of execution

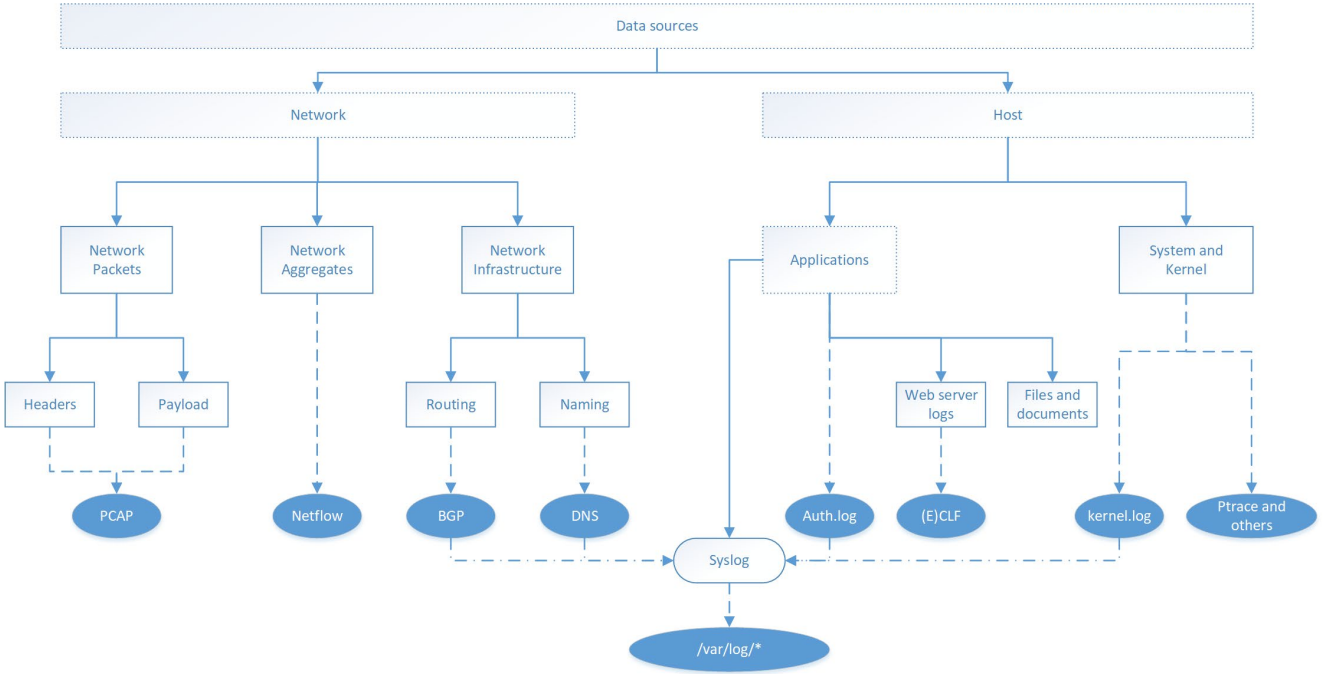
Representative of the activity of a « system »
Enable differentiation between normal and malicious activity

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 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

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

Underestimated research issue

Trustworthiness
Performance

Kernel logs

Intercepted very low in the execution path (assembly language)
Focusing on malware detection

Interest in the Android ecosystem

Understand interactions between apps and supporting libraries
Call-back mechanism obscures malicious activities

Hardware-based capture ?

Generic logging infrastructure

Entry composed of

Timestamp
Hostname
Process
Priority
PID
Message

Extremely useful both for event and alert management

But need stronger semantic for « Message »

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

Objective : generate incidents from alerts and events

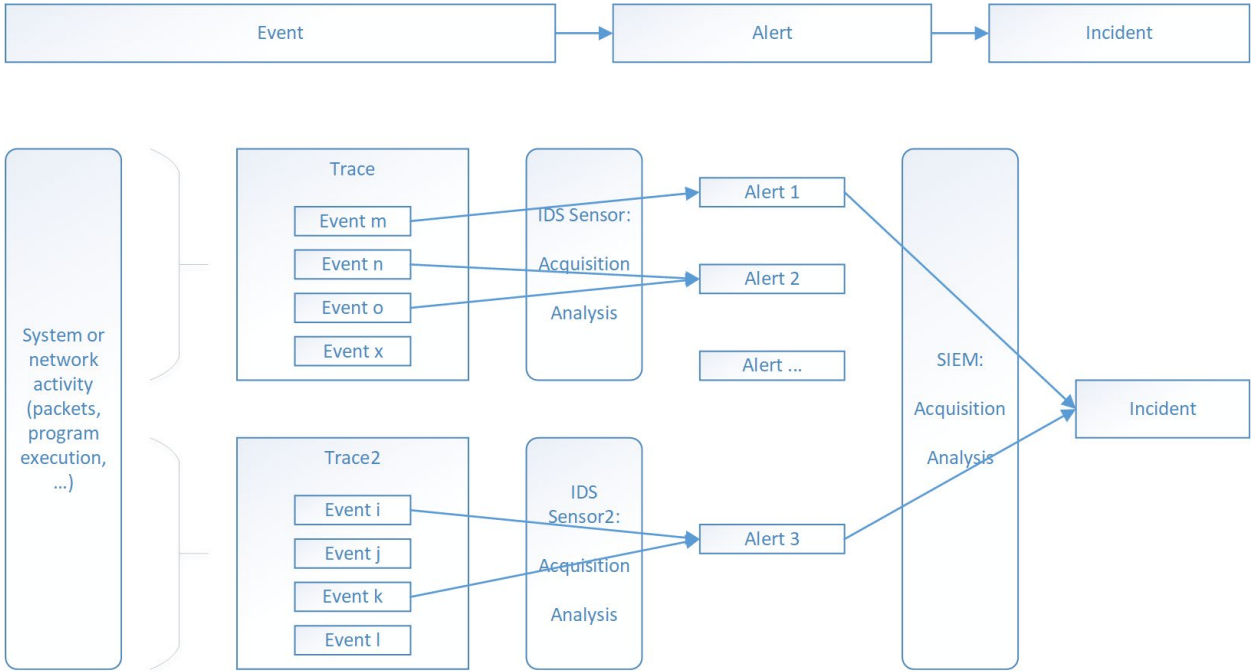
Intrusion detection sensors

Deployed in the field
Collect event information
Produce alerts

Analysis techniques

Misuse detection
Anomaly detection

FROM EVENT TO INCIDENT



Gather knowledge about attack processes

Model occurrence of attack in traces

Signatures (indicators of compromise

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

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

Advantages

Unknown attack processes are detected by their side effects

Drawbacks

Assumption of detectable side effect
Diagnosis of alert impact
Selection of behavioural model (many possibilities)
Attack-free training (ground truth)

Understand and specify the detection target
Which attacks (or attack categories), how reliable

Classic evaluation metrics
Significance of false positives and false negatives improvements
Ability to compare one's work to the state of the art

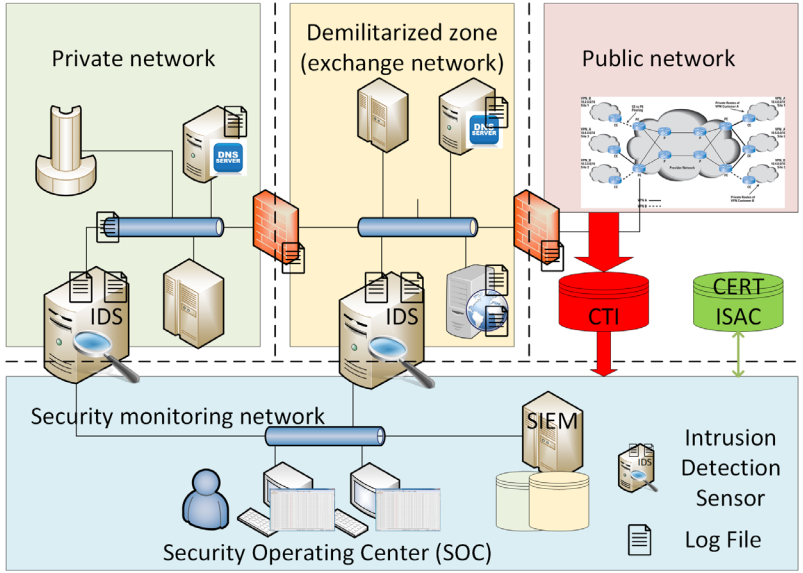
Base-rate fallacy
Magnitude of difference between the volume of attacks and the volume of normal activity in traces

Trustworthy and efficient logging

Test, evaluation and validation
Methodologies and metrics
► Including relevance "in the field"
Libraries, tools, … for practical undertaking of evaluation and validation

SECURITY INFORMATION AND EVENT MANAGEMENT

« THE BACK-END »



Blue part

Personnel component essential

Managed service model

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

Examples

Hiet, G., Debar, H., Ménouar, S., & Houdebine, V. (2015, November). Etude comparative des formats d'alertes. In C&ESAR (Computer & Electronics Security Applications Rendez-vous) 2015 (pp. 125-148).

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

Obtain situational awareness

Appropriately assess risk of events

Impact on IT infrastructure
Impact on organization
Applicability to new architectures and attack patterns (loosely controlled systems, IoT, …)

Long-term diagnosis

Evaluate past decisions regarding incidents in the light of new information
Posture analysis (continuous risk assessment)
Efficiency analysis (detection coverage, decision capability)

Decision support system

Reporting and attribution (and their consequences on detection and correlation)

Test, evaluation and validation

MITIGATIONS AND COUNTERMEASURES

OBJECTIVE: BLOCK ATTACKS BEFORE SIGNIFICANT DAMAGE

Institut Mines-Télécom

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) in network packets or instruction sequences

Traffic management for denial of service attacks

Dedicated tunnels
Anycast
Sort of « out of tune » in recent years

Impact and risk assessment

Understand the business risk associated with the incident
Understand potential collateral damage of reacting / doing nothing

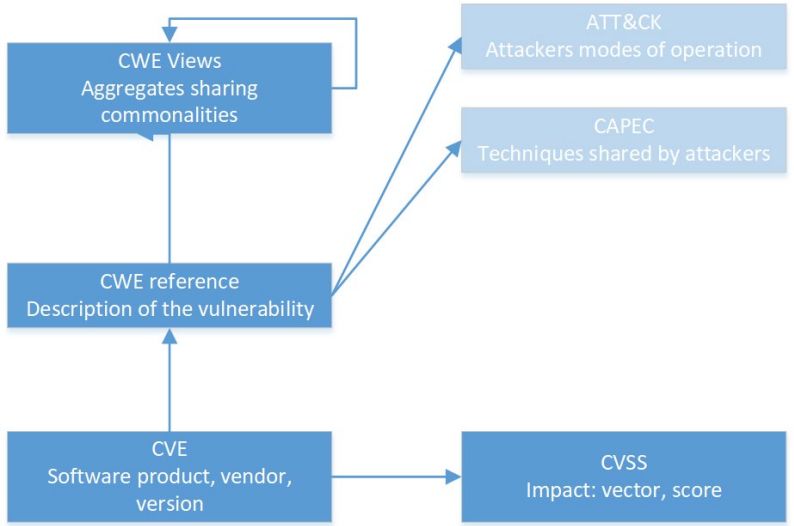
Relevant normalized knowledge sources

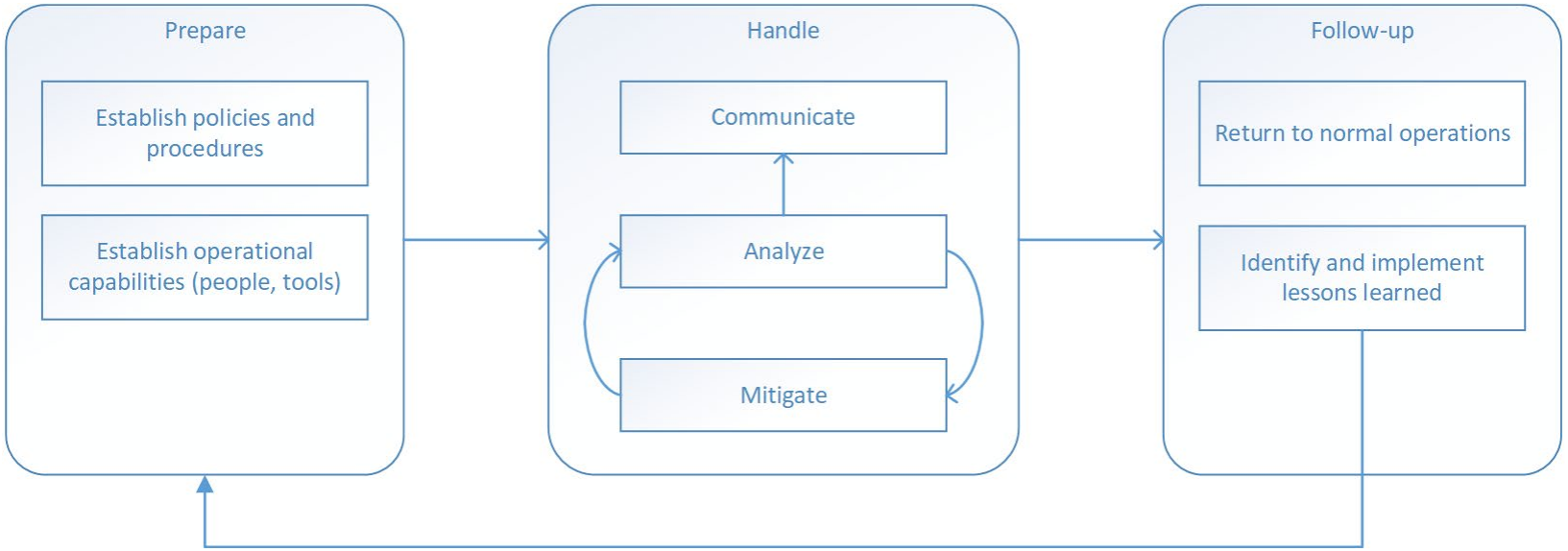
Common vulnerabilities and exposures (CVE)
Common vulnerability scoring system (CVSS)
Common Weakness Enumeration (CWE)
Common Attack Pattern Enumeration and Classification (CAPEC)
Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)
…

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




Prepare
Establish policies and procedures
Establish operational capabilities (people, tools)
Handle
Communicate
Analyze
Mitigate
Follow-up
Return to normal operations
Identify and implement lessons learned

Provide relevant and actionable decisions for mitigating and removing threats

Effectiveness of threat removal
Cost/gain analysis

Deploy appropriate counter-measures in complex distributed systems

Including legal challenges (e.g. device identification and ownership)
Feasibility of responding in cyber-physical systems

Test, evaluation and validation

Security Operations and Incident Management increasingly relevant

Wide range of connected devices
Complex dynamic systems
►DevOps

Require skilled personnel

Automation
Decision support

Biggest challenge: test, validation and evaluation