OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Assessment of Intrusion Detection Efficiency by SOCs

Methodology and tools

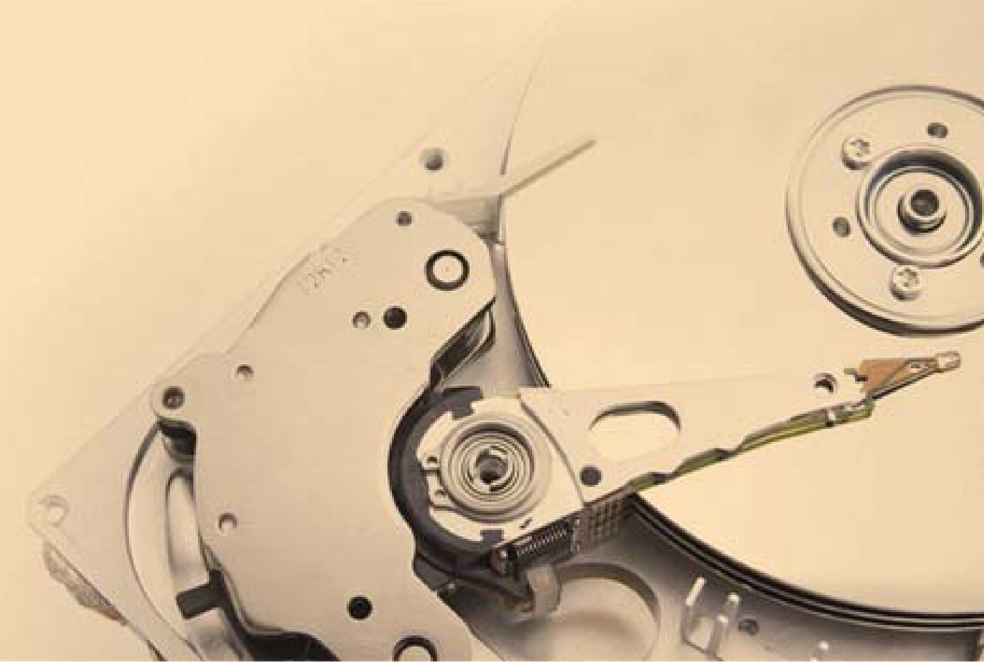
Hervé Hosy
herve.hosy@oppida.fr

28/09/2018

OPPIDA

EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

At first, few words about the company OPPIDA…



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Consulting firm specialized in cybersecurity

- Creation: 1998
- 32 people - 3.6 M €
- Qualified PASSI & PASSI LPM

Our Accreditations

Certification ISO 9001

Accreditation ISO 17025 Test Laboratory

Qualification ANSSI: ITSEF & PASSI LPM

Certification of online gaming operators

Certification MPOS

OPPIDA
Qualifié RGS/PASSI
Attestation LSTI/20022

Certification RGS/PASSI

Our Fields of Intervention

Gouvernance & Conseil

- Management de la sécurité, gestion des risques
- Accompagnement/Certification ISO 27000, HDS
- Assistance RSSI
- Analyse de risque Ebios etc…
- Homologation de sécurité
- Conformité RGPD, RGS, LPM, eIDAS
- Accompagnement système industriel (AMOA, AMOE, Plan d'Assurance Sécurité)

Audit de sécurité

- Audit de sécurité (IT) :
  - physique et organisationnel,
  - architecture,
  - configuration,
  - tests d'intrusion,
  - code, reverse engineering
- Audit Système Industriel
- Audit spécifique : Audit « LPM » (PASSI LPM, PDIS), Audit Système Industriel, Audit PCI-DSS

Laboratoire d'évaluation

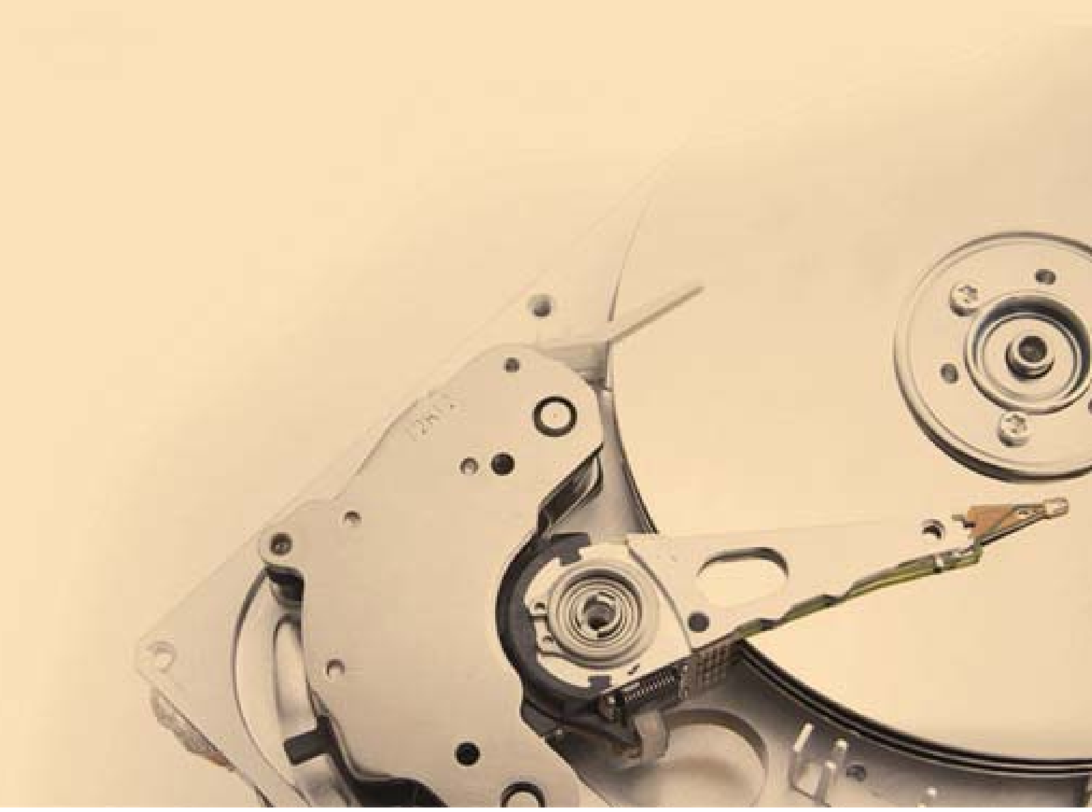
- Laboratoire d'évaluation des produits de sécurité accrédité par le COFRAC et agréé par les services gouvernementaux
  - Evaluations Critères Communs
  - Evaluations CSPN
  - Evaluation CSPN industriel
  - Evaluation eIDAS
  - Expertise Cryptographie & chiffrement

Formation & Recherche

- Organisme de formation agréé
- Formation intrasite spécifique (méthode, technique)
- Sensibilisation aux risques informatiques, phishing
- Projets de Recherche collaboratifs avec des académiques et industriels

www.oppida.fr

What is a SOC?



SOC definition

- Security Operations Center (SOC)
  - An organized team, highly skilled in cybersecurity
- Domains
  - Information system (IT)
  - Industrial Control System (ICS)
- Its mission
  - Monitor and continuously improve the security of an organization's computer system while:
    - Detecting;
    - Analyzing;
    - Alerting; and
    - If possible, responding

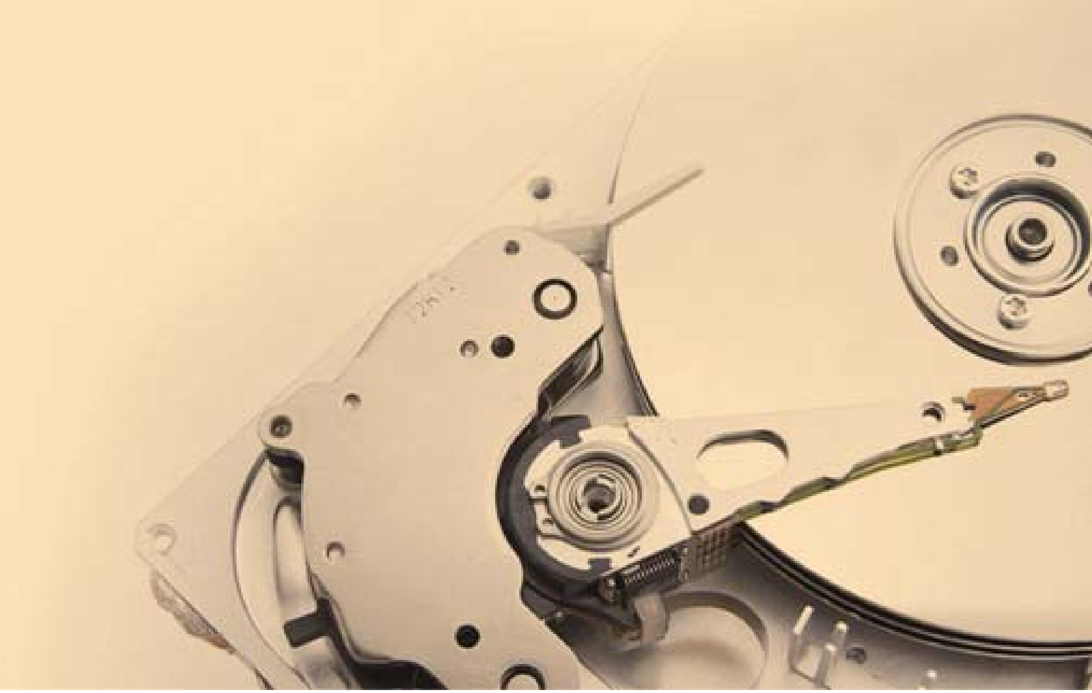
    to cyber security incidents

SOC components

- Staff
  - Skills and training
  - 24 hours a day, 7 days a week
- Environment
  - Secure premises
  - Secure interconnection with the IS to be monitored
- Processes and procedures
  - Event Management
  - Incident management
  - Notification Management
- Tools
  - Event collectors (probes, logs ...)
  - Intrusion Detection / Prevention (IPS / IDS)
  - Security Information and Event Management (SIEM)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Methodology proposed to assess SOC detection efficiency



28/09/2018

OPPIDA methodology to assess SOC detection efficiency

- Evaluation of the means implemented by a SOC
  - Skills and training of staff
  - Security of the premises
  - Security of customer’s systems interconnection
  - SOC processes and procedures for managing events, incidents, and notifications
  - Tools used (probes, IPS / IDS, SIEM ...)

- Assessing intrusion detection efficiency by a SOC
  - Relevance of events sources
  - Relevance of incidents considered
  - Relevance of detection rules

Evaluation of the means implemented by a SOC

- SOC audit against a conformity standard
  - French ANSSI standard « Prestataire de Détection d’Incidents de Sécurité » (PDIS)

Assessing SOC intrusion detection efficiency

- Step 0: Context
  - Presentation of the monitored customer’s computer system
  - Functional description of the business activities
- Step 1: Expression of monitoring needs
  - Identification of the feared events by the business staff (operational risks)
  - Translation of these feared events into threat scenarios on the computer system (security risks)
  - Identification, for each threat scenario, of the events sources to observe
  - Definition, for each threat scenario, of sequences of events leading to the feared event considered (detection algorithm)

Assessing SOC intrusion detection efficiency

- Step 2: Analysis of the configured rules relevance
  - Verification of collection of the events sources necessary to detect of the identified feared events
  - Verification of detection algorithms configured according to sequences of events to be detected
  - Checking the alert type configured for each identified feared event

- Step 3: Analysis of the configured rules efficiency

  With impact on the monitored computer system

  - Integration of vulnerable servers and simulation of attack tests on the monitored computer system to reproduce the identified feared events
  - Perform penetration tests on the monitored computer system to analyze SOC alerts

  Preferred approach

  Without impact

  - Generation of event logs corresponding to the identified feared events
  - Parsing these logs by the SOC (history replay) to analyze rules efficiency

Existing standards in security incidents detection

ANSSI recommendations

- French ANSSI standard « Prestataire de Détection d'Incidents de Sécurité » (PDIS)

  "It is recommended that the sponsor chooses among the indicators proposed by [ETSI_ISG_ISI] the operational and strategic indicators to be defined in the convention of service to measure the level of service of the SOC"

  ⇒ Standard ETSI ISG ISI-001 (90 indicators)

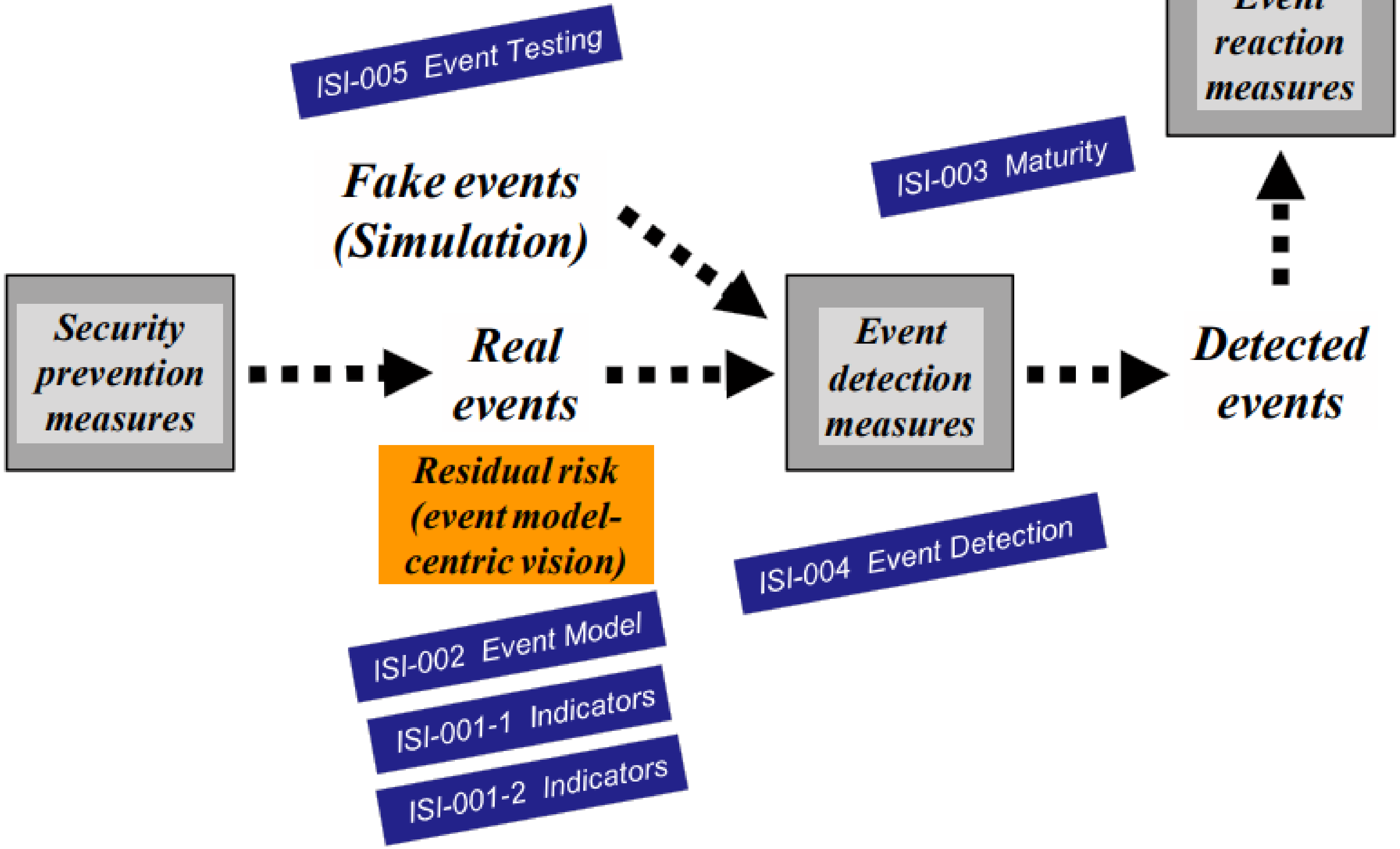
ETSI GS ISG ISI standards

- ETSI = European Telecommunications Standards Institute
  - GS = Group Specifications
    - ISG = Industry Specification Group
      - ISI = Information Security Indicators
- Standards

ETSI GS ISI 001 Parts 1 & 2	Information security indicators
ETSI GS ISI 002	Event classification model
ETSI GS ISI 003	Maturity level in event detection
ETSI GS ISI 004	Event detection
ETSI GS ISI 005	Effectiveness of existing detection means
*ETSI GS ISI 006**	*Language to model threat intelligence information*
*ETSI GS ISI 007**	*Guidelines to build a secure SOC*
*ETSI GS ISI 008**	*SIEM approach not only IT-oriented cyber defence*

** Work in progress*

GS ISG ISI series Summary Definition



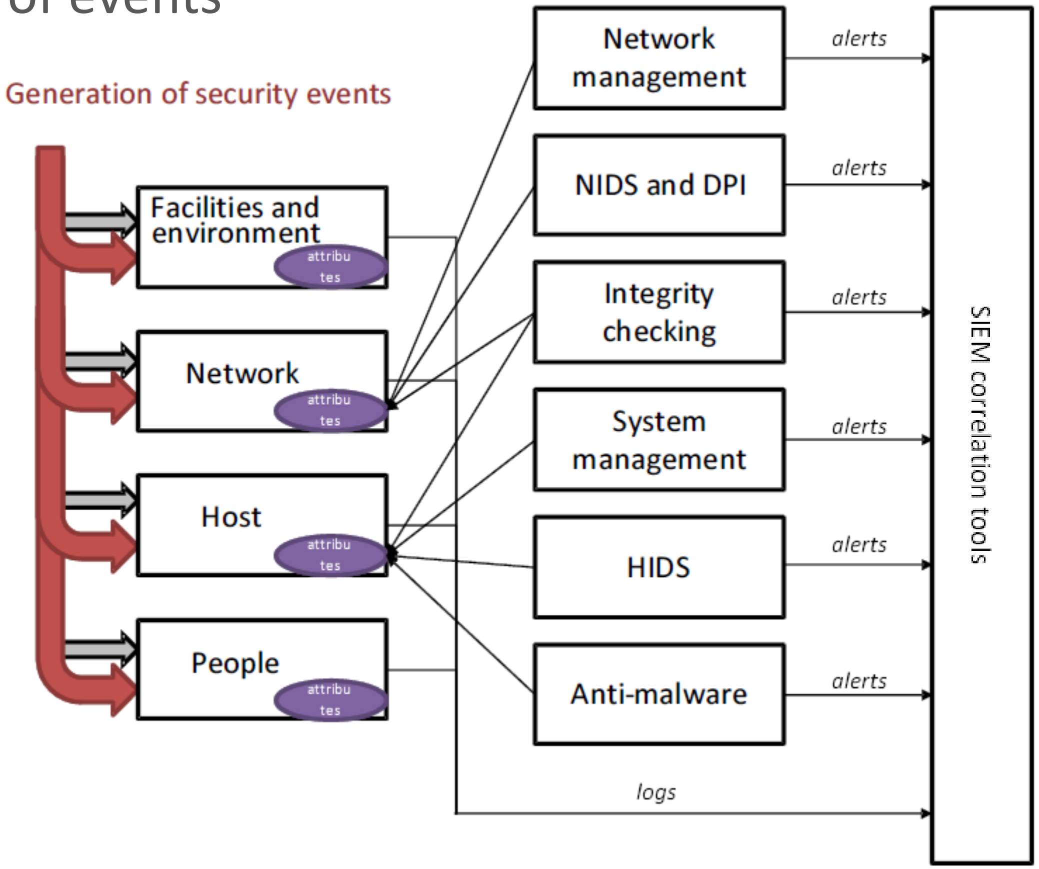
Standard ETSI GS ISI 001 (Indicators)

- Security incidents
  - IEX (Intrusions and external attacks)
  - IMF (Malfunctions)
  - IDB (Internal deviant behaviours)
  - IWH (Whole incident categories)

- Vulnerabilities
  - VBH (Behavioural vulnerabilities)
  - VSW (Software vulnerabilities)
  - VCF (Configuration vulnerabilities)
  - VTC (General security technical vulnerabilities)
  - VOR (General security organizational vulnerabilities)

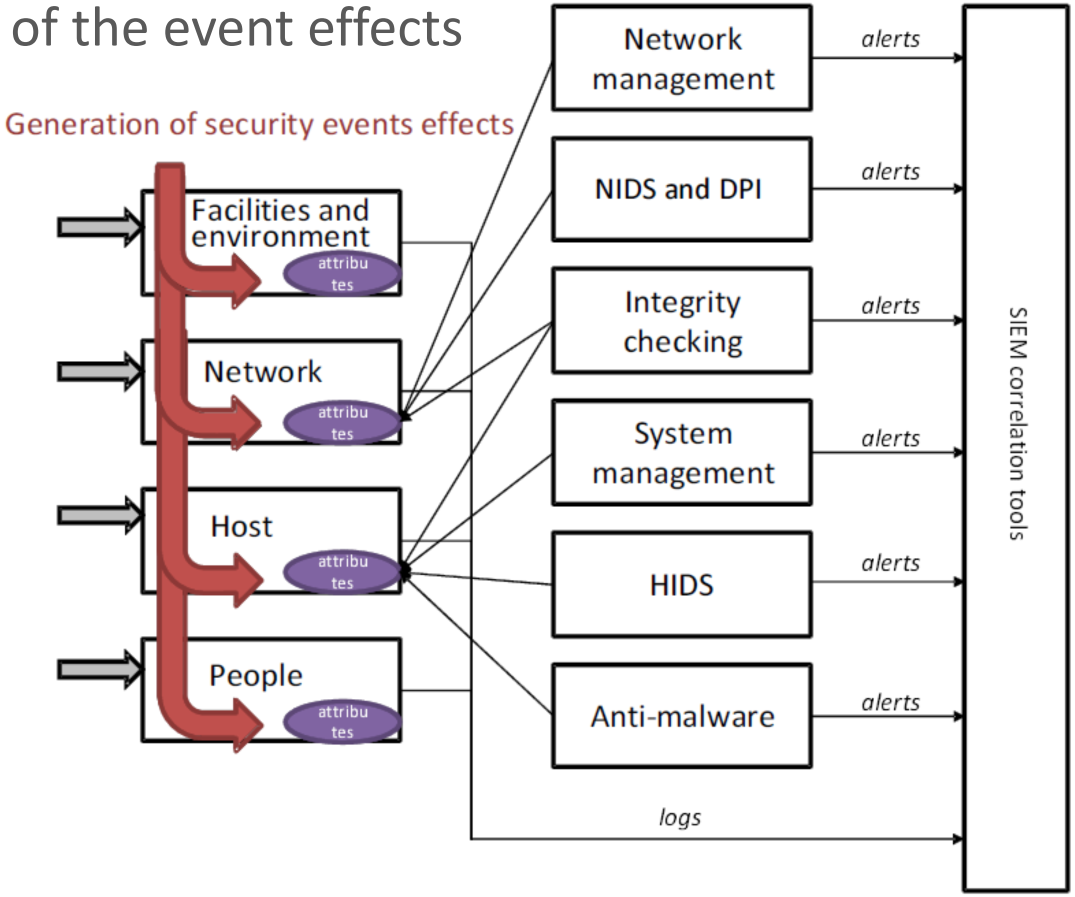
Standard ETSI GS ISI 005 (Event testing)

- Active testing by stimulation
  - Generation of events



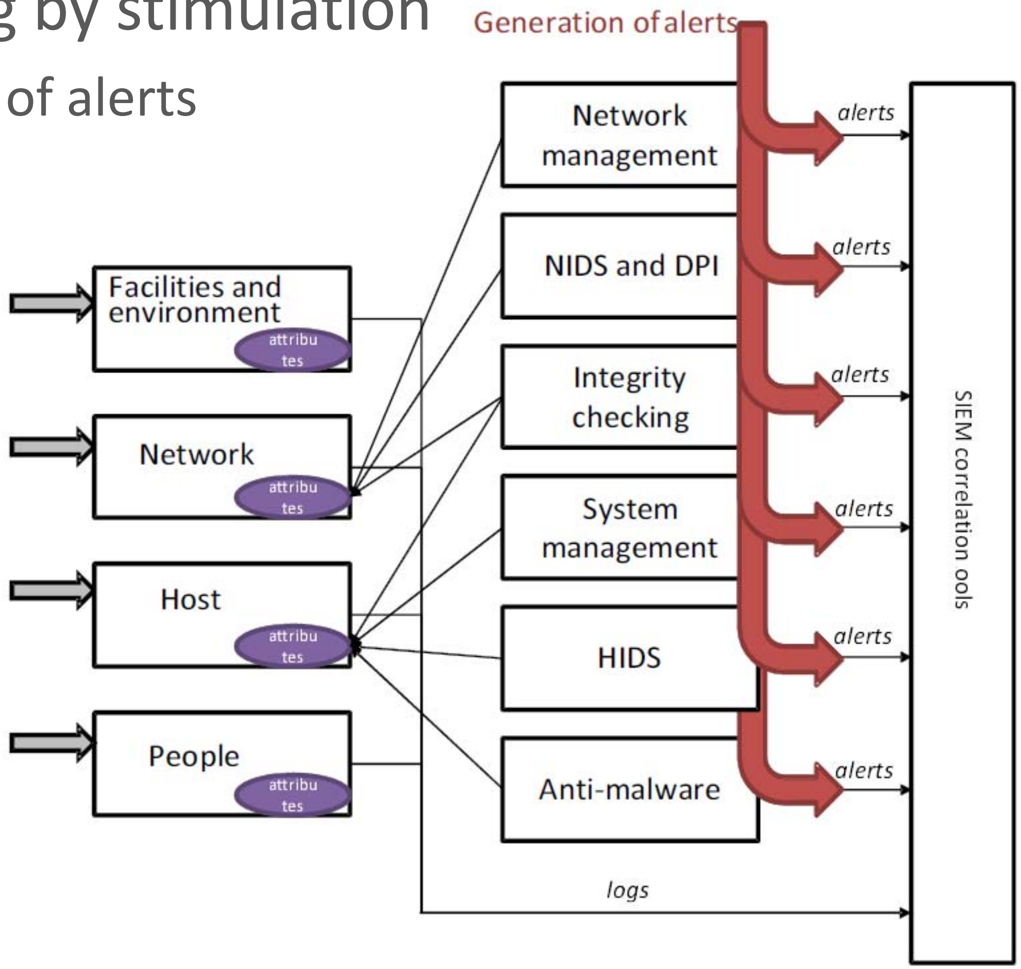
Standard ETSI GS ISI 005 (Event testing)

- Active testing by stimulation
  - Generation of the event effects



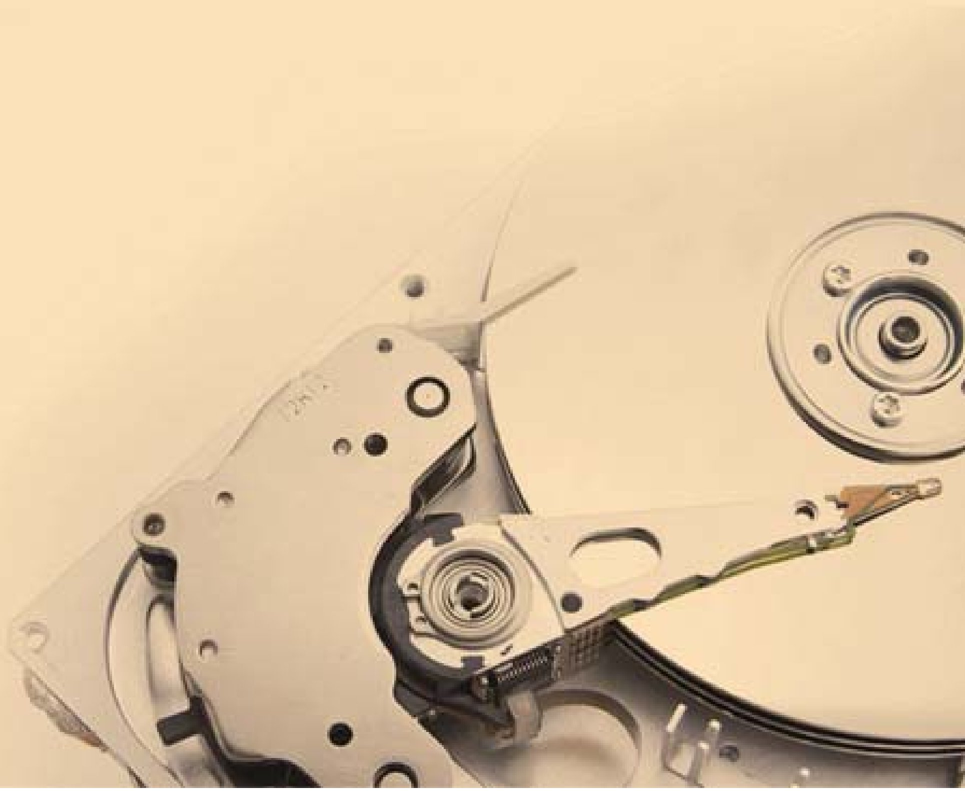
Standard ETSI GS ISI 005 (Event testing)

- Active testing by stimulation
  - Generation of alerts



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

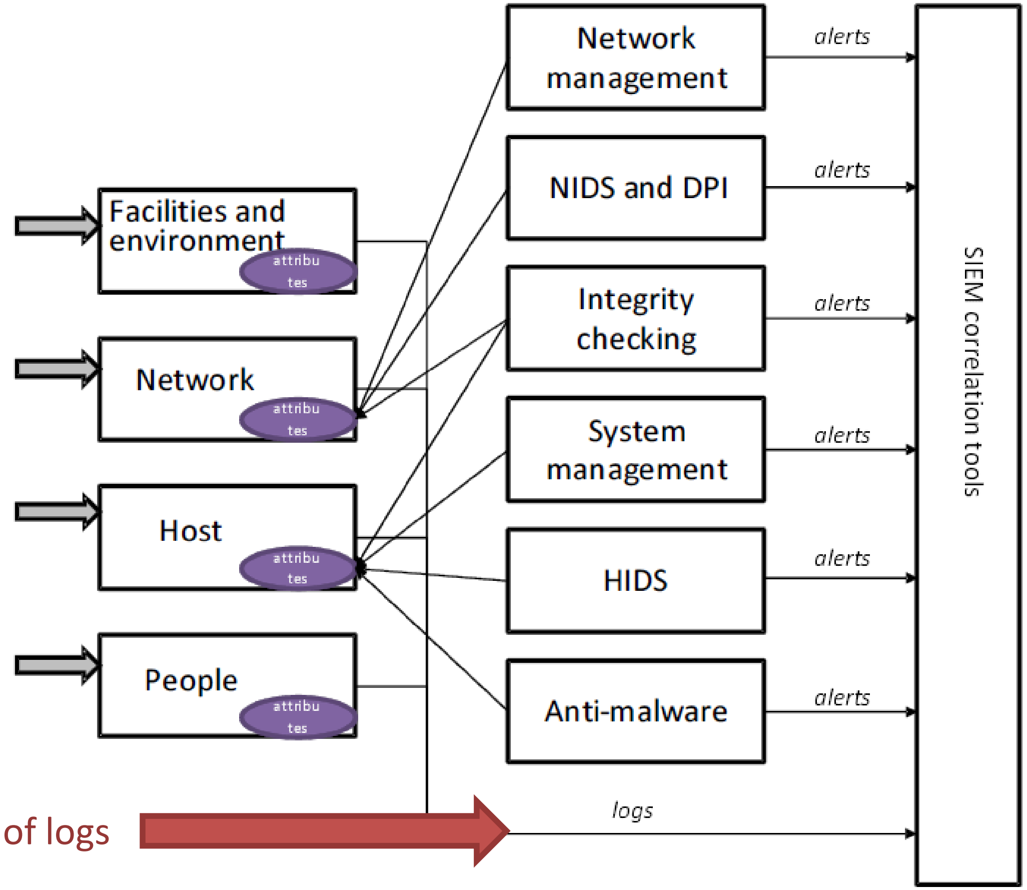
OPPIDA approach to assessing SOC detection efficiency



28/09/2018

OPPIDA approach

- Generation of logs



Generation of logs

OPPIDA approach

- Developing scenarios based on a subset of standard ETSI GS ISI 001 indicators:
  1. Intrusion on externally accessible servers (IEX_INT.2),
  2. Obvious and visible websites defacements (IEX_DFC.1),
  3. Denial of service attacks on websites (IEX_DOS.1),
  4. Malware installed on workstations or servers (IEX_MLW.3 et IEX_MLW.4),
  5. User impersonation (IDB_UID.1),
  6. Privilege escalation by exploitation of software or configuration vulnerability on a externally accessible server (IDB_RGH.1),
  7. Outbound controls bypassed to access Internet (VBH_IAC.1),
  8. Not compliant user rights granted illicitly by an administrator (VBH_RGH.1),
  9. Spear phishing or whaling carried out using social engineering and targeting organization’s specific registered users (IEX_PHI.2)

OPPIDA approach

- For each scenario, definition of levels to rank the results:

  0. No detection
  1. Detection of a scenario that is **very easy** to detect
  2. Detection of a scenario **rather easy** to detect
  3. Detection of a scenario **rather difficult** to detect
  4. Detection of a **very difficult** scenario to detect

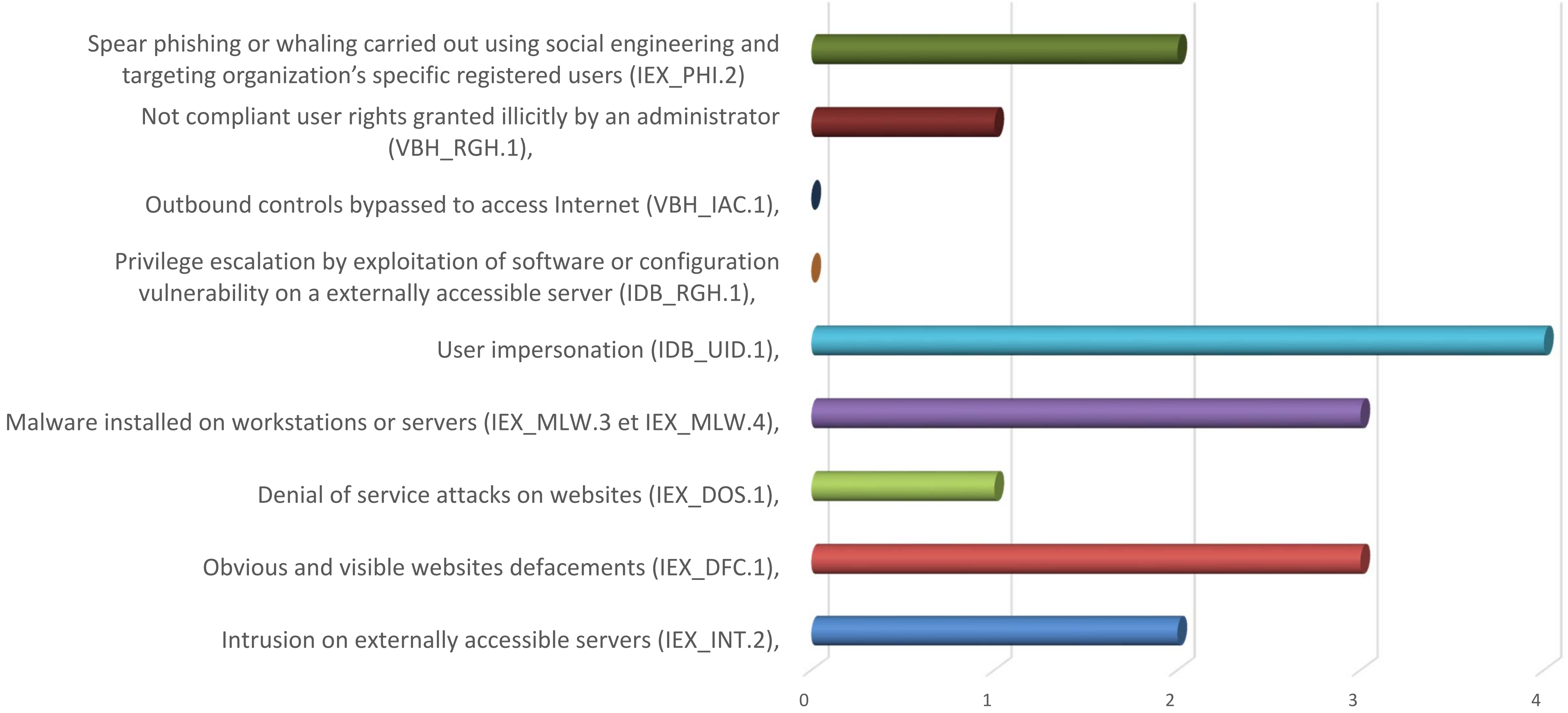
- By varying:
  - The frequency of tests / attempts
  - The typology of tests: use of escape techniques...

OPPIDA approach

- Perform scenarios on a representative testing platform and record relevant logs from security devices
  - In customer or OPPIDA premises
  - Same security devices that SOC monitors (OS, firewall, anti-virus…)
- Manage feared event-specific logs database
  - Recorded event logs corresponding to the identified feared events, with different levels of attack
- Modify recorded event logs to adapt to SOC context
  - Modify IP addresses, timestamps, sequence…
- Parse these logs by the SOC (history replay) to analyze alerts raised by configured rules

OPPIDA approach

Intrusion detection efficiency



OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Benefits of OPPIDA approach to assess SOC efficiency

Benefits of OPPIDA approach

- None impact of the monitored computer system
  - Very important in case of ICS
- Progressive assessment of SOC detection efficiency
  - First focus on business-sensitive scenarios
  - Adding new feared event-specific logs into database
  - Increase complexity of same scenarios, with different levels of attack
  - Progressive improvement and validation of SOC detection algorithms
- Repeatable approach
  - Easy periodic assessment of the SOC with history replay, without operational impact
  - Allow to perform non-regression tests on SOC detection rules