2021-2022学年春季学期

# 网络空间安全态势感知

# *Cyber security situation awareness*

授课团队：刘宝旭 卢志刚 刘玉岭

助　　教：李　宁

# 网络空间安全态势感知

*Cyber security situation awareness*

# [第11次课] 传统态势识别技术

授课教师：刘玉岭

授课时间：2022.3.28

# 内容概要

- 一、入侵检测与防御技术
- 二、安全信息和事件管理SIEM
- 三、安全管理中心SOC
- 四、相关系统和工具

- 不同技术阶段的网络安全态势感知

| 方法 | 分析重点 | 主要数据源 | 输出结果 |
| --- | --- | --- | --- |
| 基于安全关键“点”的方法 | 安全脆弱性态势的发掘分析 | 源代码、二进制代码等 | 脆弱性的有无和多少 |
| 基于安全攻防“线”的方法 | 攻防利用途径和可能性的纵向分析 | 脆弱性和资产信息 | 可能的攻防途径及其可能性 |
| “平面化”的方法 | 安全风险态势的迭代性分析 | 脆弱性、资产、威胁、拓扑关系等信息 | 风险有无及其严重程度 |
| “立体化”的方法 | 安全状况和趋势的量化分析 | 全方位的网络安全信息 | 整体安全状况及可能的演变趋势 |

## ●不同呈现形态的网络安全态势感知

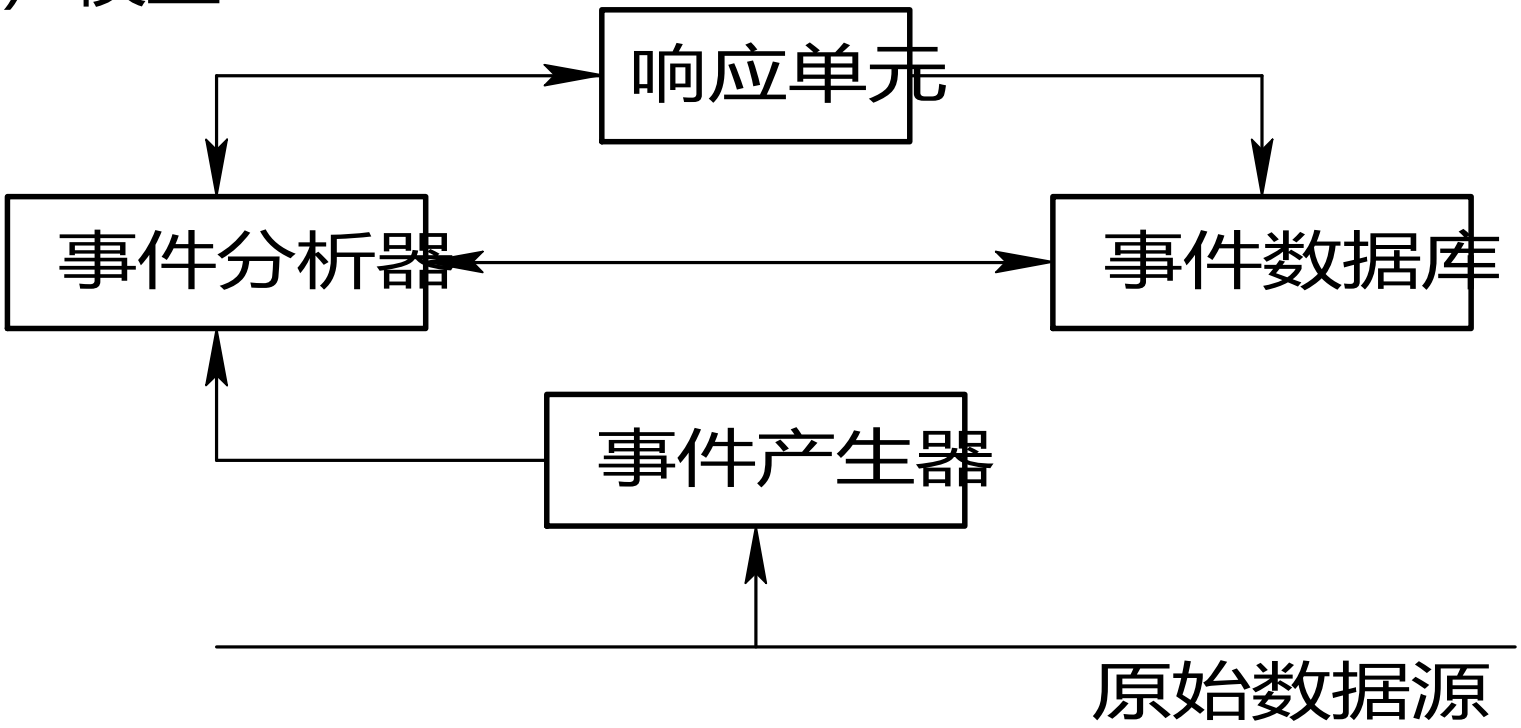
| 方法 | 数据来源 | 数据分析深度 | 分析结果用途 |
| --- | --- | --- | --- |
| 类SOC方法 | 安全设备的数据 | 以资产为核心进行安全事件全流程的分析 | 安全事件管理、应急响应等 |
| 面向Web的方法 | 安全设备的数据、主动获取的网络安全状态数据 | 以安全威胁为核心进行全面的风险分析 | 安全预警、安全整改等 |
| 大数据驱动的方法 | 安全设备的数据、主动获取的网络安全状态数据、威胁情报数据 | 以安全事件为驱动因素进行全面分析 | 通报预警、应急响应、追踪溯源、调查取证等 |

# 一、入侵检测与入侵预防技术

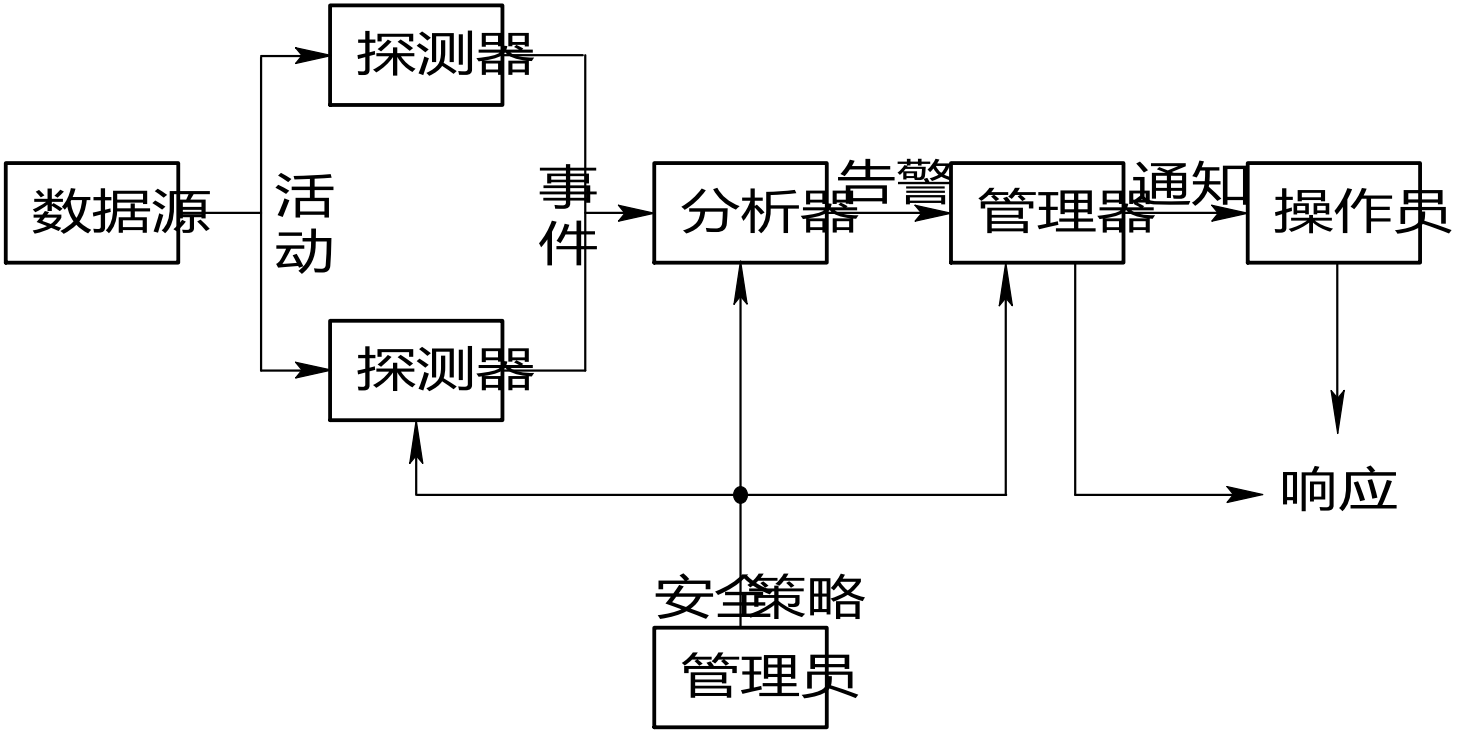
- 入侵检测系统IDS
  - 一种网络安全设备或应用软件，可以监控网络传输或者系统，检查是否有可疑活动或者违反企业的政策，侦测到时发出警报或者采取主动反应措施
  - IDS最早出现在1980年4月，James P. Anderson为美国空军做了一份题为《Computer Security Threat Monitoring and Surveillance》的技术报告，提出了IDS的概念
- 入侵预防系统IPS
  - 一种能够监视网络或网络设备的网络数据传输行为的计算机网络安全设备，能够即时的中断、调整或隔离一些不正常或是具有伤害性的网络数据传输行为

面向网络安全异常，发出告警并采取措施

- 入侵检测系统的CIDF（通用入侵检测架构组织）模型



- IETF（互联网工程任务组）的入侵检测系统模型



# 一、入侵检测与入侵预防技术

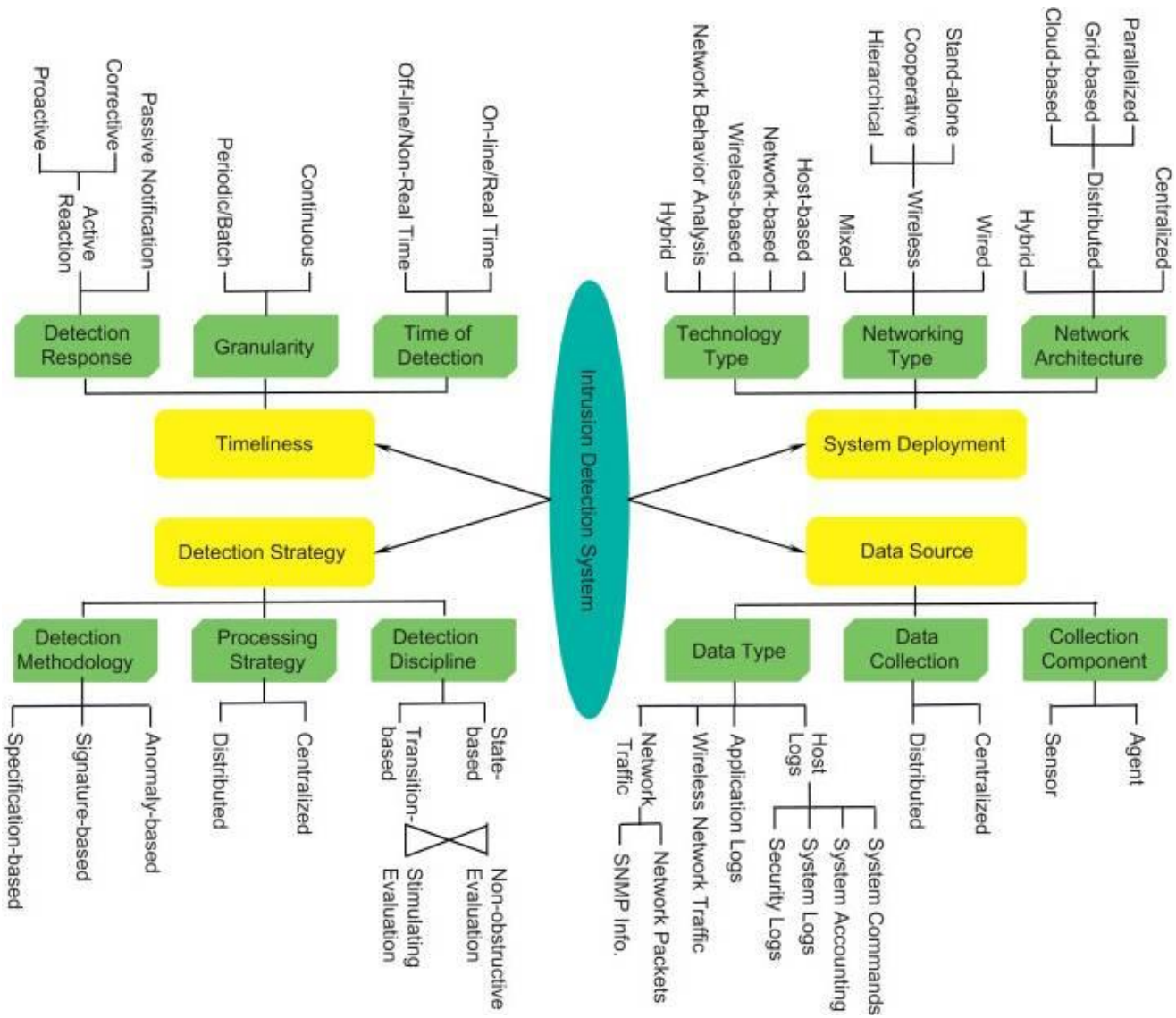
- IDS/IPS
  - 作为防火墙技术的补充，开展网络行为的安全管理
  - 模式发现技术：基于知识
    - 前提：所有入侵行为和手段都能够表示为一种模式或特征
    - 关键：如何表示入侵的模式，恰当的分开正常行为和入侵
  - 异常发现技术：基于行为
    - 前提：所有入侵行为与正常行为都是不同的
    - 关键：异常阈值与特征的选择
  - 状态协议分析技术：基于场景
    - 前提：入侵行为并不能靠单一的数据包分析得出，需结合协议建模，加入状态特性
    - 关键：协议状态模型的表达能力：完备性、正确性

- IDS/IPS
  - 模式发现技术：基于知识
    - 优点：简单有效，详细的上下文分析
    - 缺点：不能有效检测未知攻击、已知攻击的变种攻击和逃避攻击；特征和模式难以及时更新；知识维护比较费时
  - 异常发现技术：基于行为
    - 优点：对于新型攻击的检测比较有效；不依赖于OS；易于发现特权滥用行为

| Signature-based (knowledge-based) | Anomaly-based (behavior-based) | Stateful protocol analysis (specification-based) |
|---|---|---|
| Pros<br>• Simplest and effective method to detect known attacks.<br>• Detail contextual analysis. | • Effective to detect new and unforeseen vulnerabilities.<br>• Less dependent on OS.<br>• Facilitate detections of privilege abuse. | • Know and trace the protocol states.<br>• Distinguish unexpected sequences of commands. |
| Cons<br>• Ineffective to detect unknown attacks, evasion attacks, and variants of known attacks.<br>• Little understanding to states and protocols.<br>• Hard to keep signatures/patterns up to date.<br>• Time consuming to maintain the knowledge | • Weak profiles accuracy due to observed events being constantly changed.<br>• Unavailable during rebuilding of behavior profiles.<br>• Difficult to trigger alerts in right time. | • Resource consuming to protocol state tracing and examination.<br>• Unable to inspect attacks looking like benign protocol behaviors.<br>• Might incompatible to dedicated OSs or APs. |

# 一、入侵检测与入侵预防技术

- IDS/IPS划分（4个维度）
  - 系统部署
  - 数据源
  - 检测策略
  - 时间性




Intrusion detection system: A comprehensive review，2012

## ●大数据时代IDS/IPS面临的挑战

| | |
|---|---|
| 1. "Comprehensive Enterprise Coverage" | The entire production IT stack (e.g., "networks, hosts, applications, databases, identities") for the enterprise must be monitored by the ESM regardless of environment (i.e., onsite or in the cloud). |
| 2. "Information Interaction and Correlation" | All meaningful events, logs, and similar from input sources in #1 must be capable of being collected for correlation. |
| 3. "Technology Interaction and Correlation" | The SIEM will serve as the foundation of the correlation engine, however it should also integrate with other important security technologies such as: Firewalls, IDSs/IPSs, DLPs, Vulnerability Management, and Anti-Malware. |
| 4. "Business Interaction and Correlation" | The ESM must be aware and tuned to the specifics of the organization's business context to better assess an attacker's motivation and yield better correlation and intelligence. |
| 5. "Cross-Boundary Intelligence for Better Decision Making" | The ESM solution must span organizational boundaries across the entire enterprise in a cohesive and collaborative manner, and not permit fragmentation with regards to its overall cyber defense. |
| 6. "Visualized Output for Dynamic and Real-time Defense" | The output of the system must be easily visualized and understandable by end user analysts in an effective manner. |

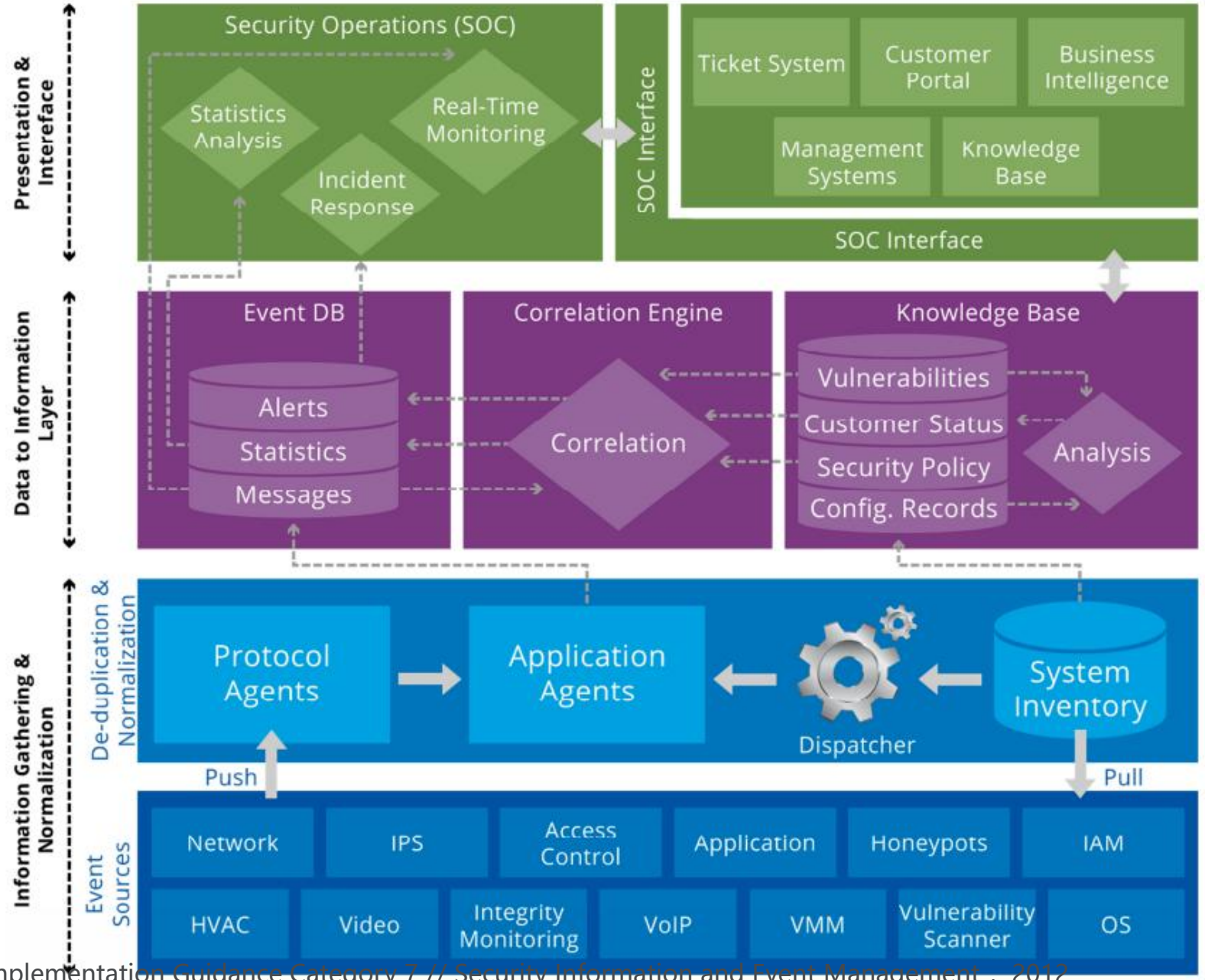
Intrusion detection and Big Heterogeneous Data: a Survey，2015

## 内容概要

- 一、入侵检测与防御技术
- 二、安全信息和事件管理SIEM
- 三、安全管理中心SOC
- 四、相关系统和工具

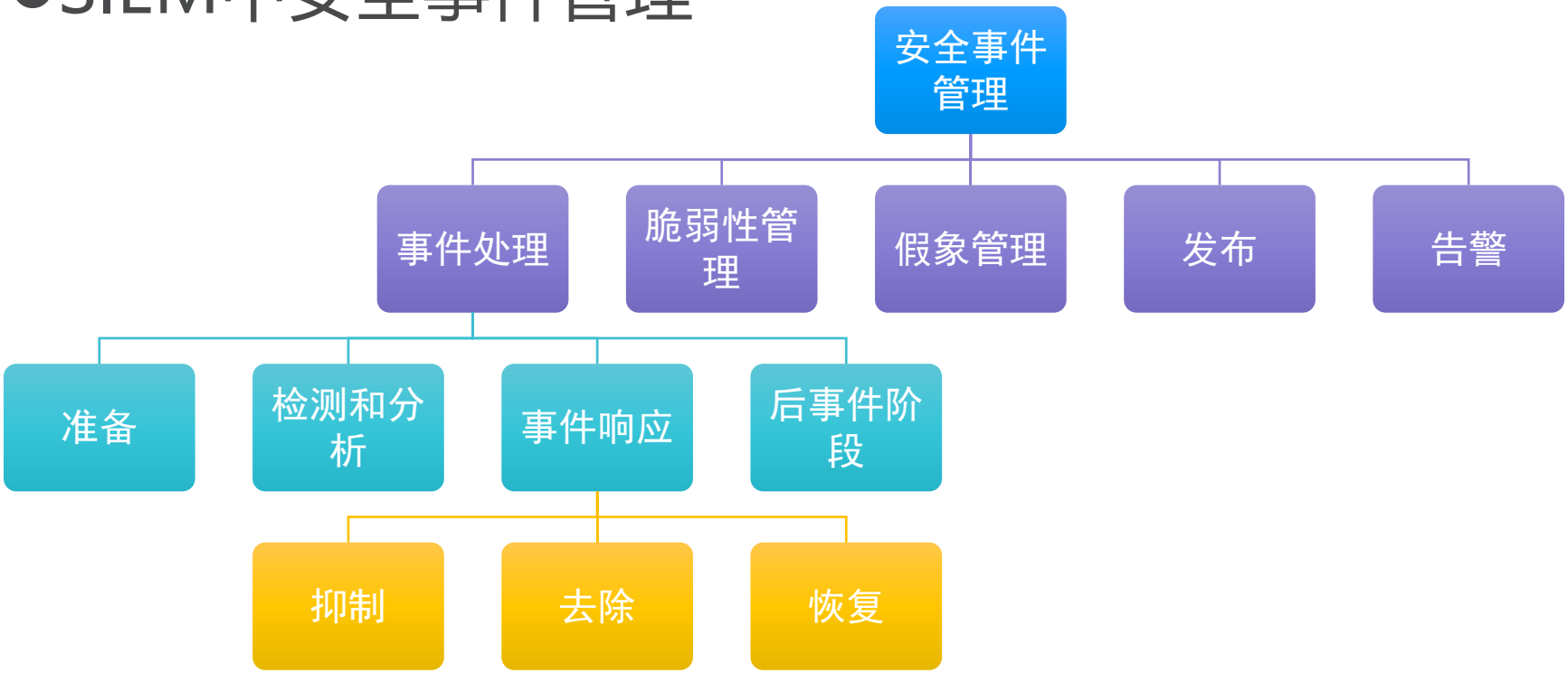
## ●SIEM工作原理


Log Collection
Log Analysis
Event Correlation
Log Forensics
IT Compliance
Application Log Monitoring
Object Access Auditing
SIEM
Real-time Alerting
User Activity Monitoring
Dashboards
Reporting
File Integrity Monitoring
System & Device Log Monitoring
Log Retention




SecaaS Implementation Guidance Category 7 // Security Information and Event Management，2012

## ●SIEM中安全事件管理



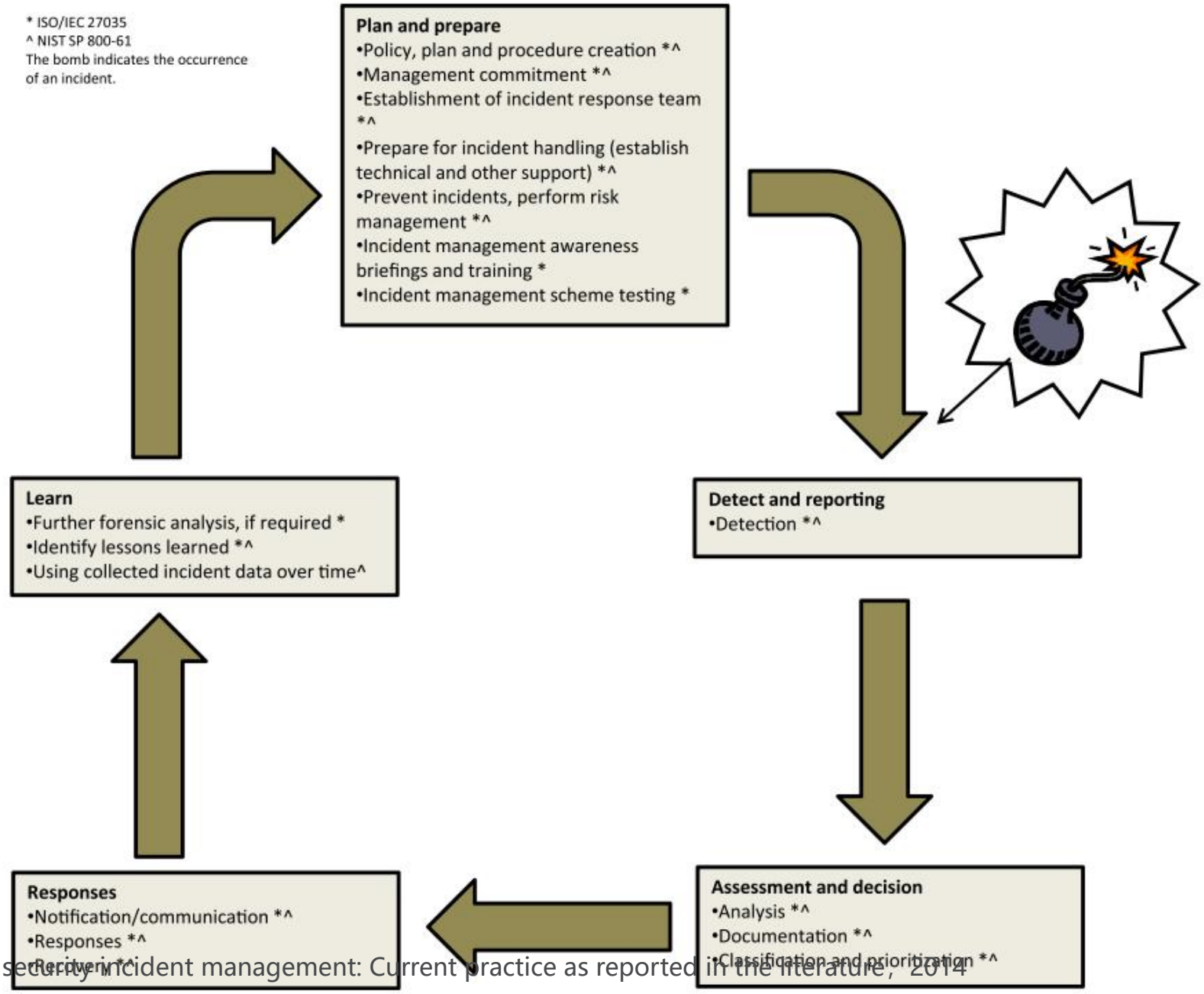

A survey of information security incident handling in the cloud，2015

## 三

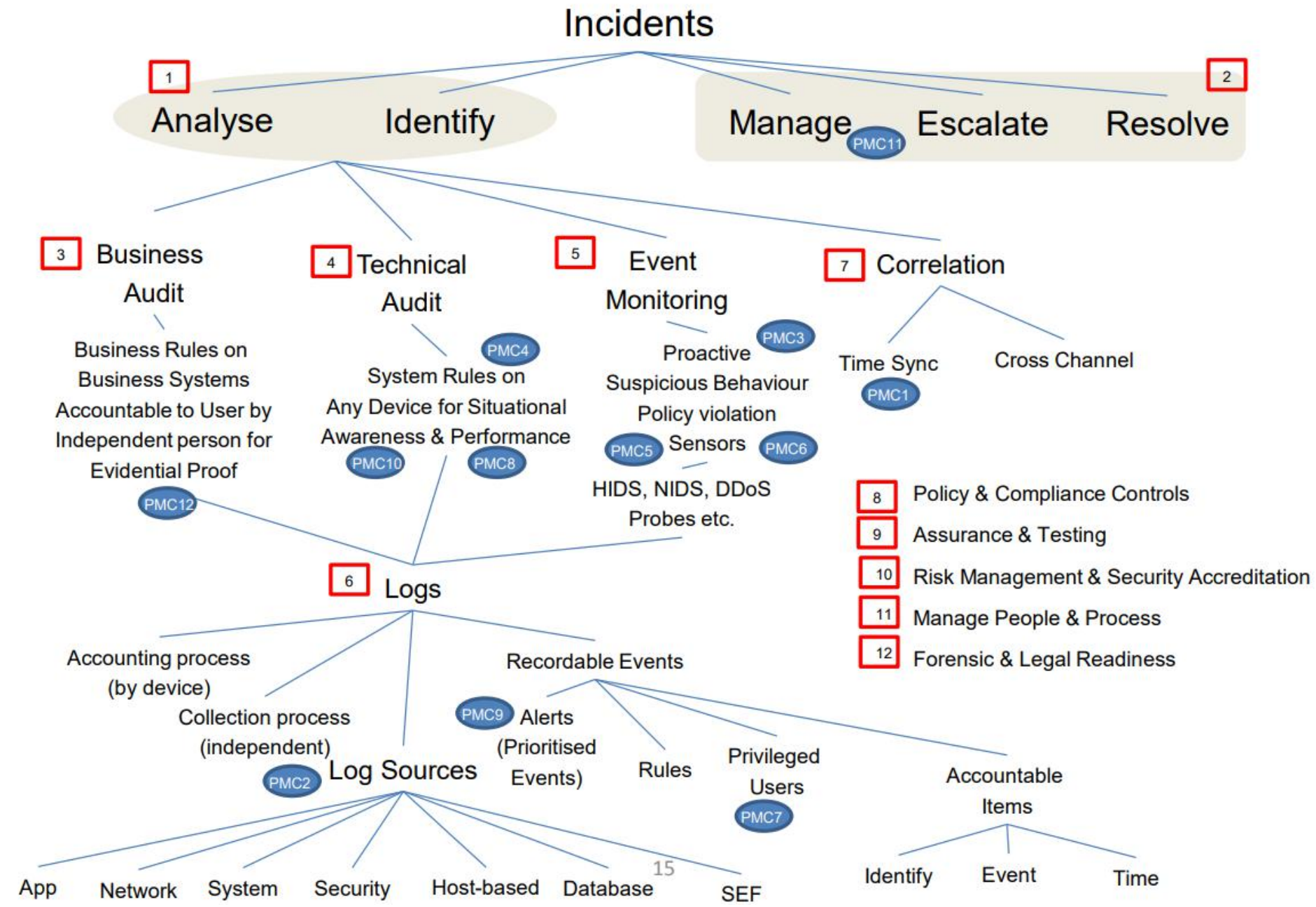
●SIE

| Phase | Research area | Theme/application domain |
|---|---|---|
| Preparation | CSIRT | Automation workflow |
| | | Establishing and coordinating CSIRT model |
| | | Collaborative information sharing model |
| | Incident management/handling strategies | Model |
| | | Collaborative structure |
| | | Cloud computing |
| Detection and analysis | Incident reporting | Model |
| | | Cloud computing |
| | | Information exchange format |
| | Risk management | Model |
| | | Cloud computing |
| | | Critical infrastructure |
| | | Smartphone |
| | Incident prioritisation | Model |
| Response (containment, eradication and recovery) | Response selection technique | Static mapping |
| | | Dynamic mapping |
| | | Cost-sensitive mapping |
| | Backup and recovery | Performance |
| | | Technologies |
| | | Techniques and implementation |
| Post incident | Adaptive incident learning | Model, information content and template |
| | | Organisational learning theory |
| | | Web-based technology |

A survey of infc



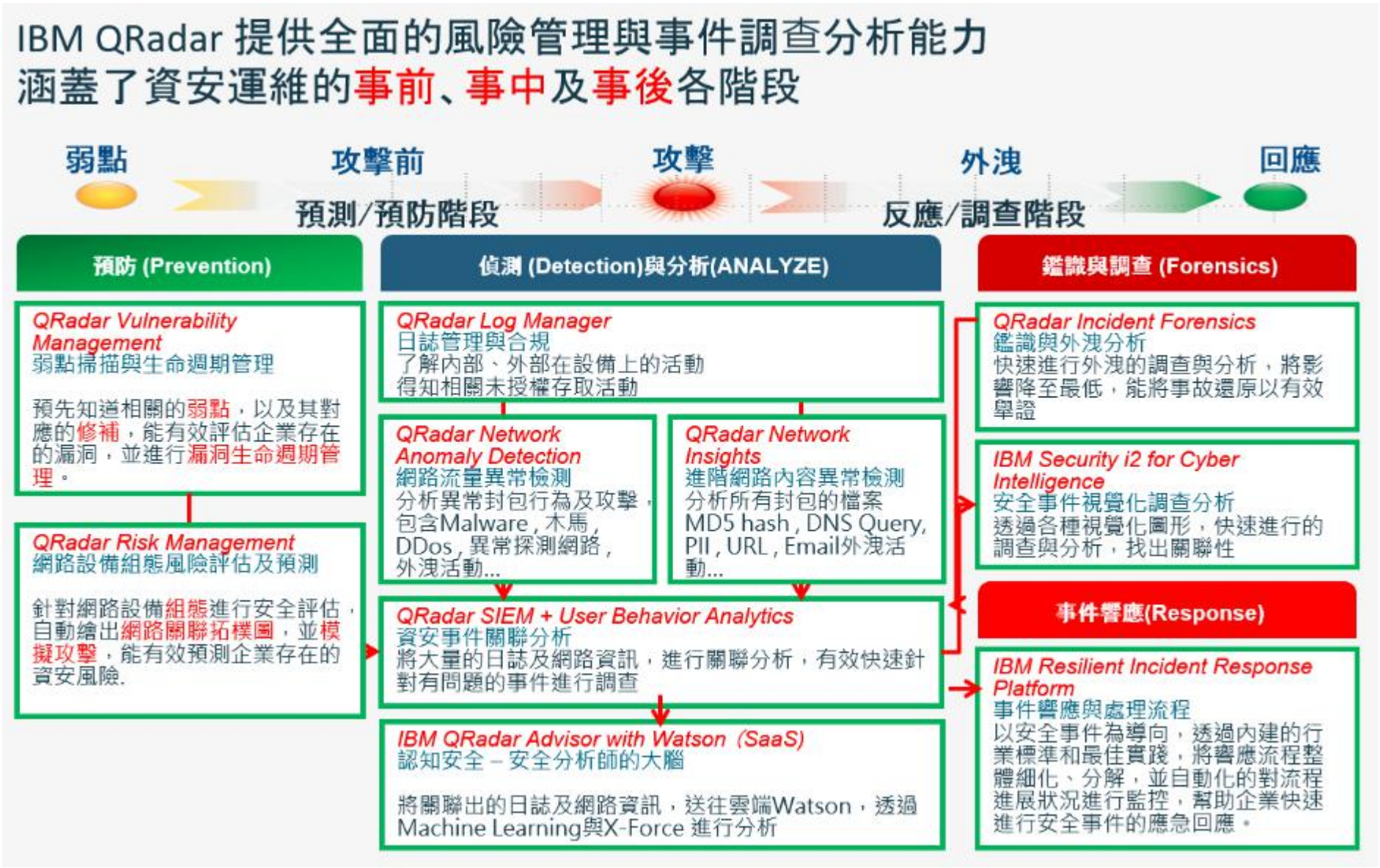

Information security incident management: Current practice as reported in the literature, 2014


Incidents
1
Analyse
Identify
2
Manage
PMC11
Escalate
Resolve
3
Business Audit
Business Rules on Business Systems Accountable to User by Independent person for Evidential Proof
PMC12
4
Technical Audit
PMC4
System Rules on Any Device for Situational Awareness & Performance
PMC10
PMC8
5
Event Monitoring
PMC3
Proactive Suspicious Behaviour Policy violation
PMC5
Sensors
PMC6
HIDS, NIDS, DDoS Probes etc.
7
Correlation
Time Sync
PMC1
Cross Channel
8
Policy & Compliance Controls
9
Assurance & Testing
10
Risk Management & Security Accreditation
11
Manage People & Process
12
Forensic & Legal Readiness
6
Logs
Accounting process (by device)
Collection process (independent)
PMC2
Log Sources
Recordable Events
PMC9
Alerts (Prioritised Events)
Rules
Privileged Users
PMC7
Accountable Items
Identify
Event
Time
App
Network
System
Security
Host-based
Database
SEF
15

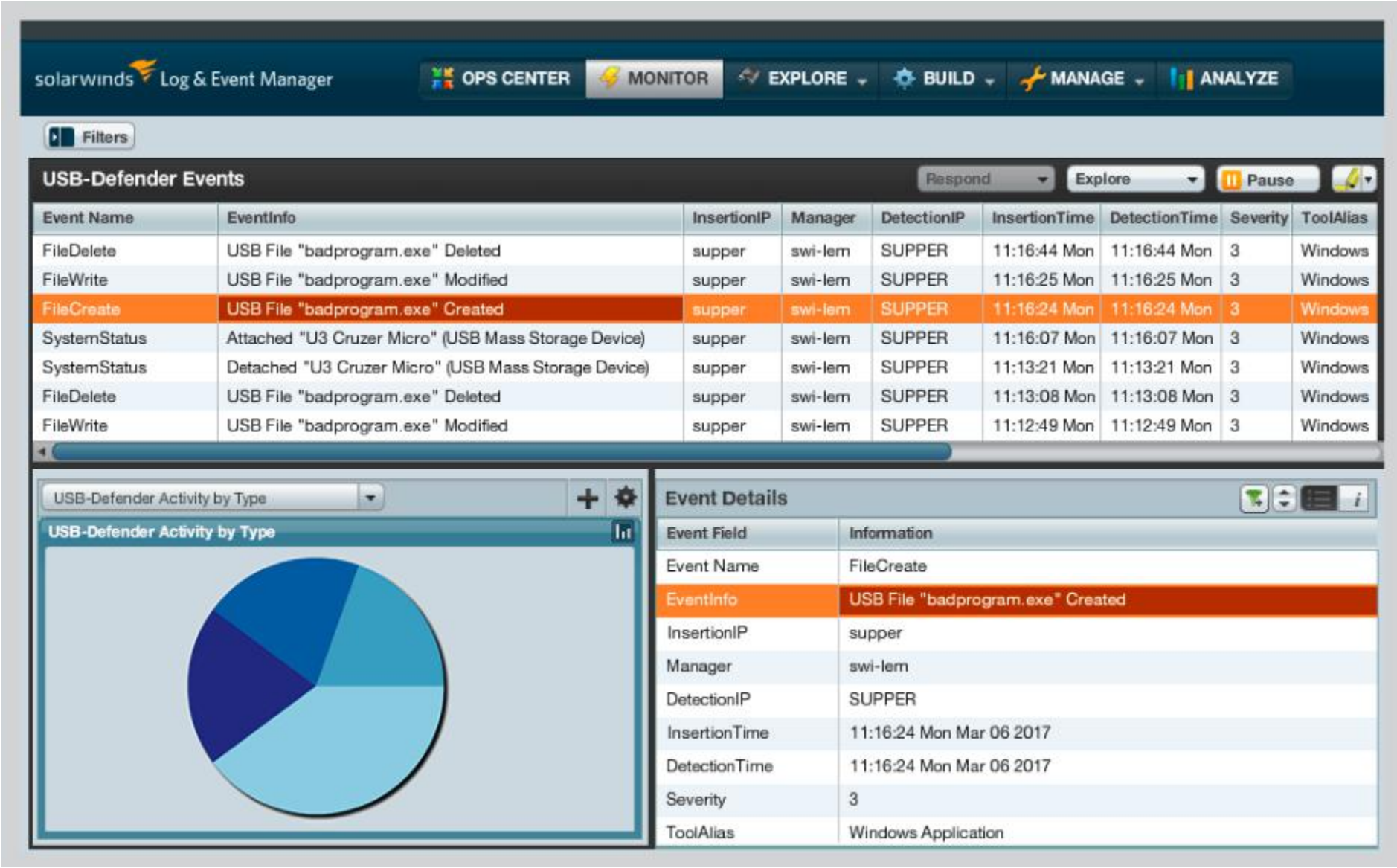
# 二、安全信息和事件管理SIEM

- SIEM演进路线
  - 越来越重视异常检测，如 UEBA: User and Entity Behavior Analytics
  - 强化事件应急响应：SOAR模型（Security Orchestration, Automationand Response，安全编排、自动化和响应）；OODA模型（Observe, Orient, Decide, Act，观察，调整，决策以及行动）

# 二、安全信息和事件管理SIEM



# 二、安全信息和事件管理SIEM



## 内容概要

- 一、入侵检测与防御技术
- 二、安全信息和事件管理SIEM
- 三、安全管理中心SOC
- 四、相关系统和工具

# 三、安全管理中心SOC

- 安全管理中心
  - 集中化
  - 全方位
  - 体系化

# 三、安全管理中心SOC

- 安全管理中心
  - 全方位的安全管理中心
    - 人员
    - 技术
    - 过程

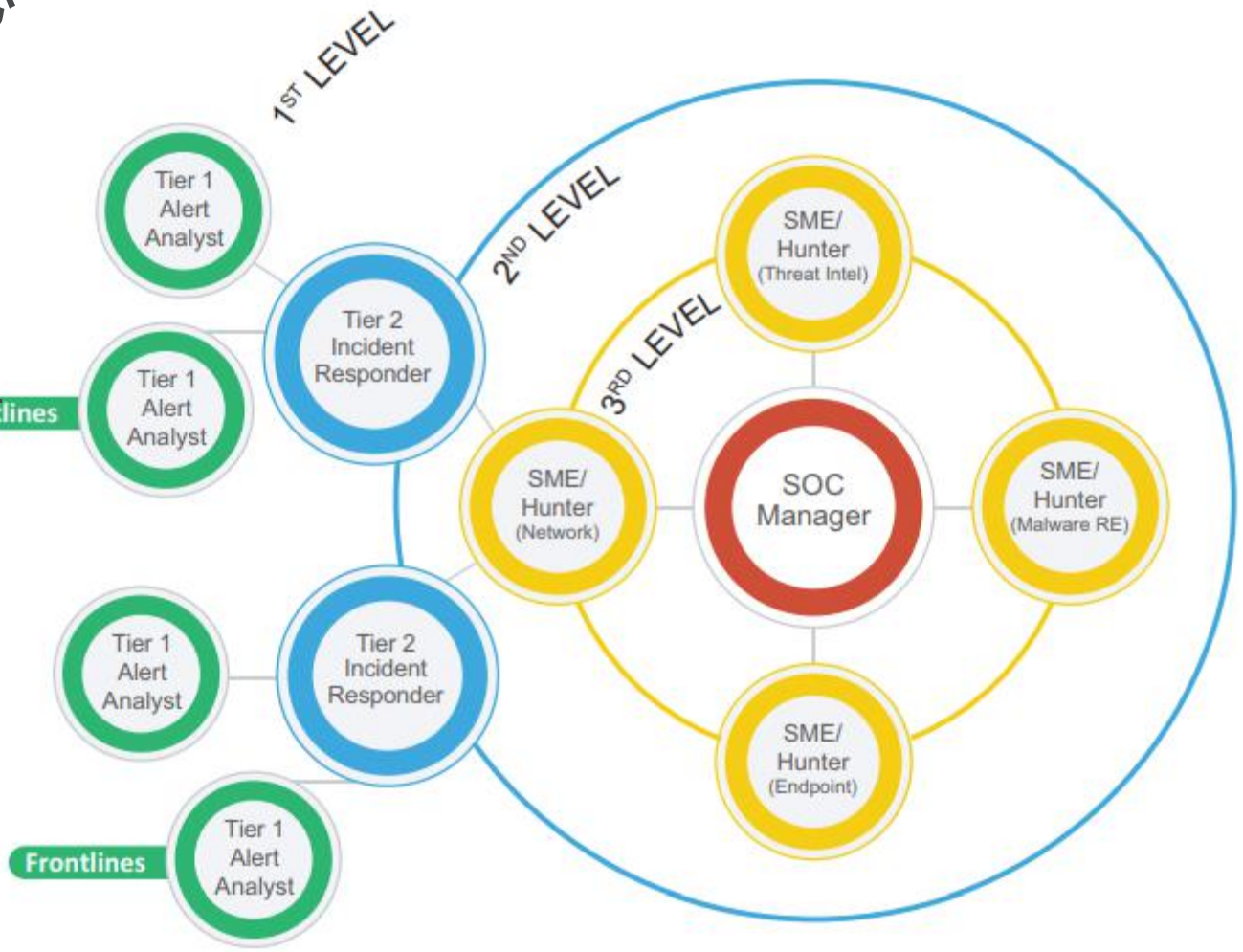

Building a World-Class Security Operations Center: A Roadmap， SANS Institute，2015

## ●必备技术组成


Manage People & Process
Policy & Compliance Controls
Risk Management & Security Accreditation
Business Audit
Technical Audit
Log Collection
Event Monitoring
Privilege User Monitoring
Correlation –by Time across Multiple Channels
Analyse & Identify Incidents
Manage Incidents to Resolution
Forensic & Legal Readiness
Deterrent Controls
威慑式控制技术
Proactive Controls
主动式控制技术
Reactive Controls
被动式控制技术
Retrospective Controls
回顾式控制技术

●安全管理中心组织层次

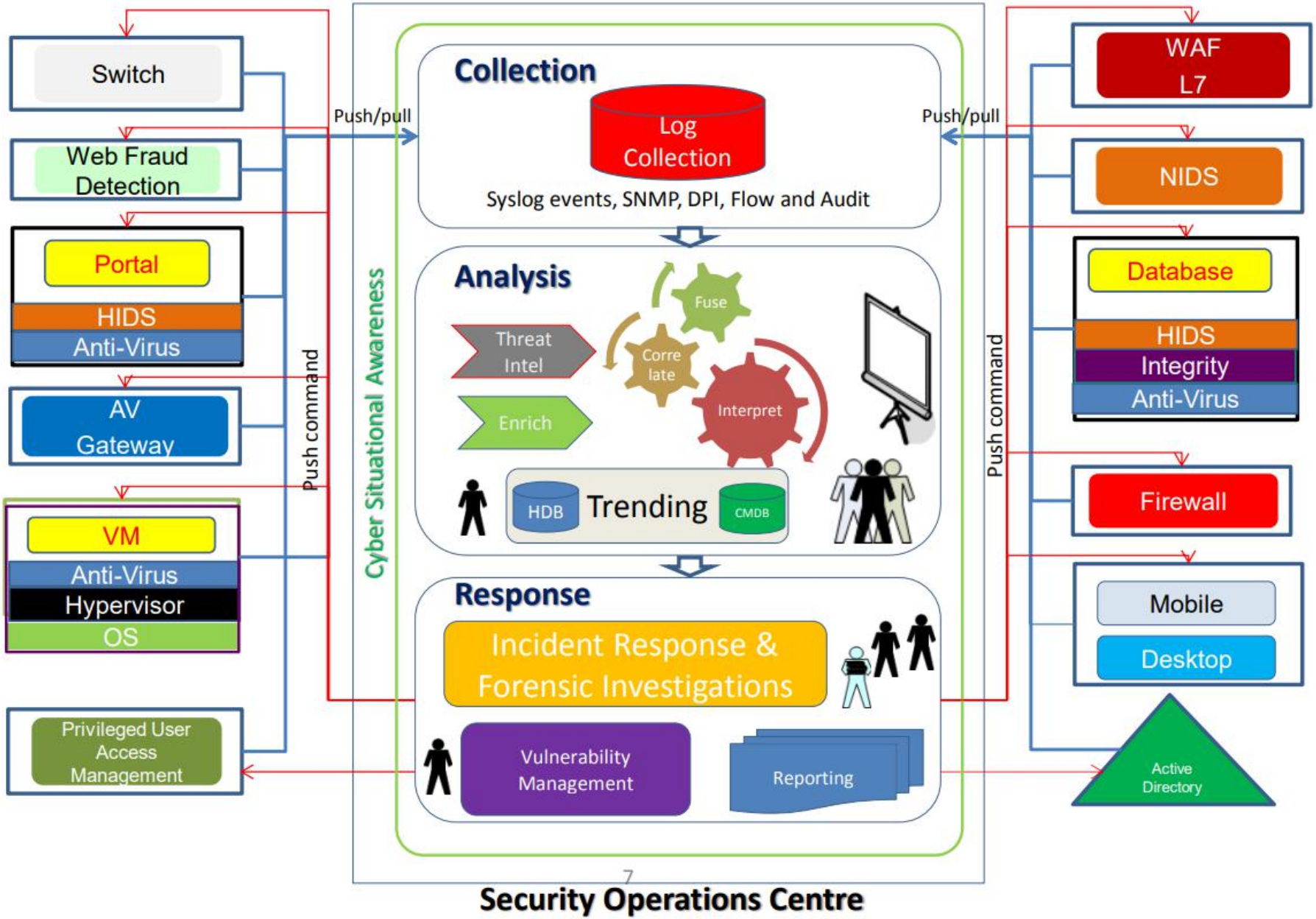
- ●告警分析（IDS/IPS）
- ●事件响应（SIEM）
- ●安全事件管理+俘获



# 三、安全管理中心SOC

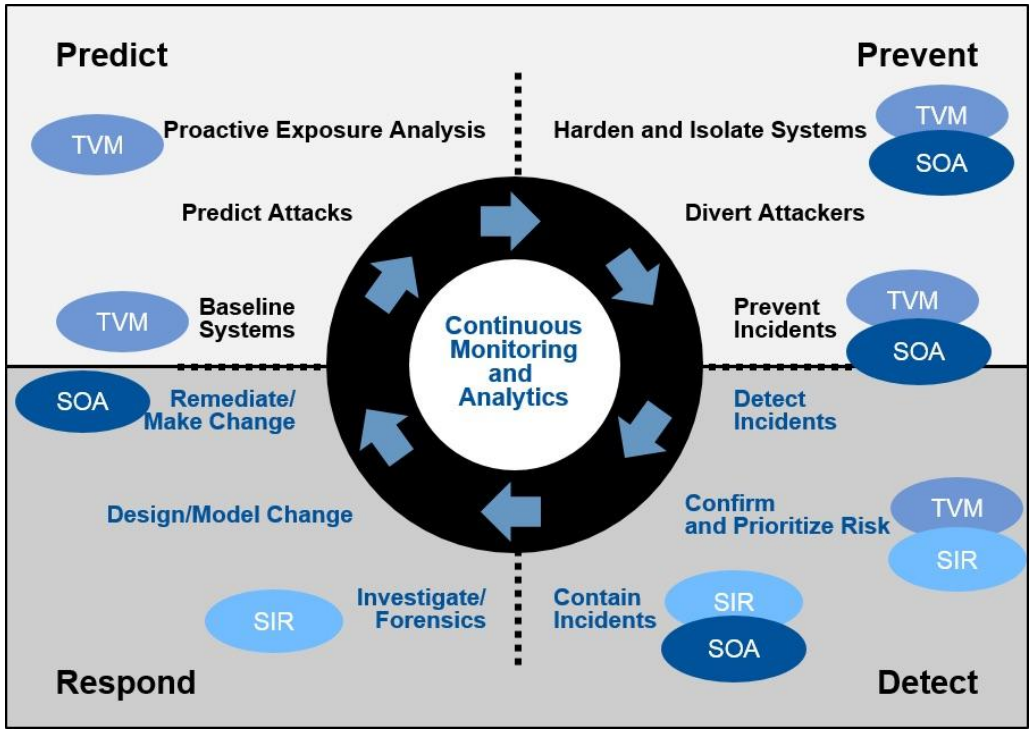

Cybersecurity Operations Center: Cyber Preparedness and Lesson Learned，2017

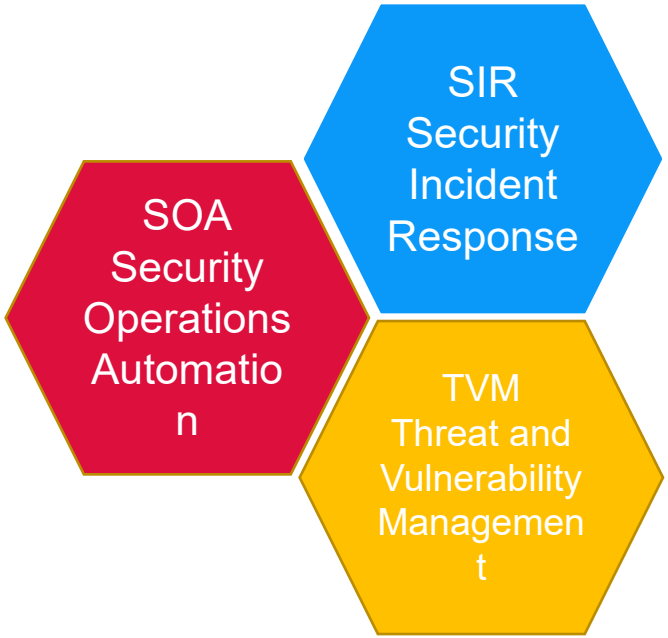
# 三、安全管理中心SOC




CYBER SECURITY OPERATIONS CENTRE，center for multidisciplinary Research，innovation and collaboration，2015

- 安全管理中心实例-Gartner威胁情报驱动的SOC
  - 强调安全管理的自动化
  - 强调安全事件的响应
  - 强调安全威胁和脆弱性的管理




More information: The Five Characteristics of an Intelligence-Driven Security Operations Center, Gartner 2015

- **NASA 的Security Operations Center (SOC)**
  - SOC与NASA的计算机取证和事故分析（CFIA）团队以及网络威胁分析计划（CTAP）并行工作，该计划专注于解决最严重的威胁，将信息映射到美国国家航空航天局的威胁与NASA固有的脆弱性之间
  - SOC还对美国航空航天局进行渗透测试，以确定安全弱点，并在企业范围内识别和响应安全事件
    - 实时检测具有恶意软件感染的NASA系统
    - 有效阻止访问恶意漏洞网站
    - 防止数据丢失
    - 采用有效的多层防御 和极其重要的实时情报
    - 支持多种操作系统
    - 与外部密切合作：包括美国CERT，事件响应和安全小组论坛（FIRST）、海湾地区CSO委员会、FBI和反间谍机构（CI）等

## 内容概要

- 一、入侵检测与防御技术
- 二、安全信息和事件管理SIEM
- 三、安全管理中心SOC
- 四、相关系统和工具

- Snort
  - 最最常用的开源入侵检测和防御工具
  - 已发展成为一个多平台(Multi-Platform),实时(Real-Time)流量分析，网络IP数据包(Pocket)记录等特性的强大的网络入侵检测/防御系统
  - 支持三种工作模式
    - 嗅探器：Snort将在现有的网域内截取数据包，并显示在显示屏上
    - 数据包记录器：Snort将已截取的数据包存入存储媒体中
    - 网络入侵检测系统：Snort可对截取到的数据包做分析的动作，并根据一定的规则来判断是否有网络攻击行为的出现
  - 支持多平台：Linux，FreeBSD，Windows
  - https://www.snort.org/

- OSSEC
  - 开源工具，结合了基于主机的入侵检测系统、日志监控、安全事件管理等
  - 主要功能：日志分析、文件完整性检查、rootkit检测、实时警报和主动响应
  - 支持多种平台：Linux, OpenBSD, FreeBSD, MacOS, Solaris, Windows
  - 具备详细的使用文档，甚至中文版
  - 网站：https://ossec.github.io/

- AlienVault统一安全管理平台
  - 提供了在各种系统中监控、分析和管理系统事件的工具
  - 提供用于漏洞评估和入侵检测（包括网络和基于主机）的工具
  - 提供OSSIM（开源安全信息和事件管理）服务， 包含的开源项目列表包括：
    - FProbe，Munin，Nagios，NFSen / NFDump，OpenVAS，OSSEC，PRADS，Snort，Suricata和TCPTrack

# 传统态势识别技术