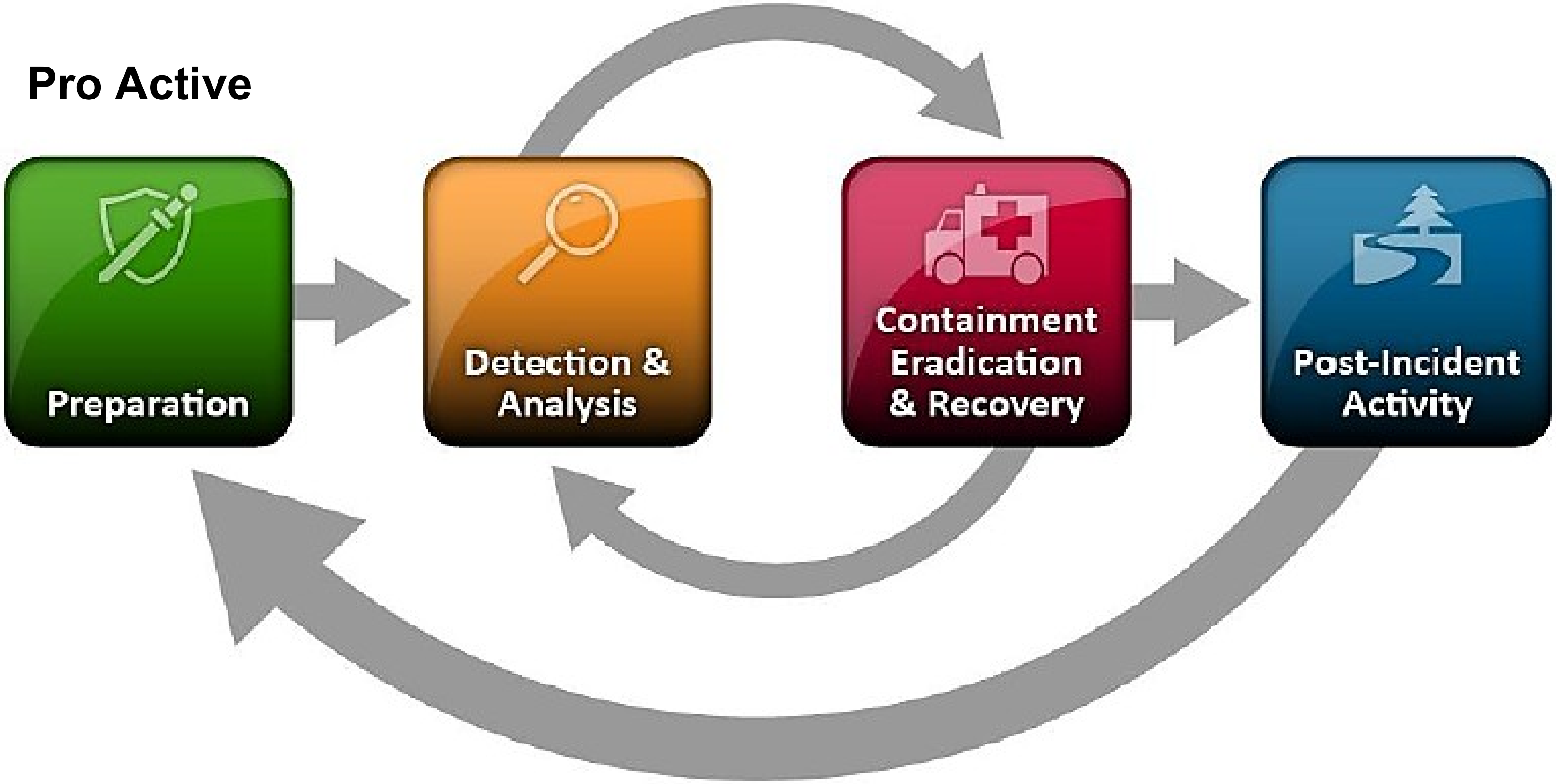
ST2610

Security **P**olicies and **I**ncident **M**anagement

Cyber Incident Response Life Cycle

Pro Active



Life Cycle – Preparation

- Main goal of preparation phase is to prevent incidents by ensuring that systems, networks, and applications are sufficiently secure in-advance
- Designing the systems securely
- Implementing defense mechanisms
- Proactively looking for threats

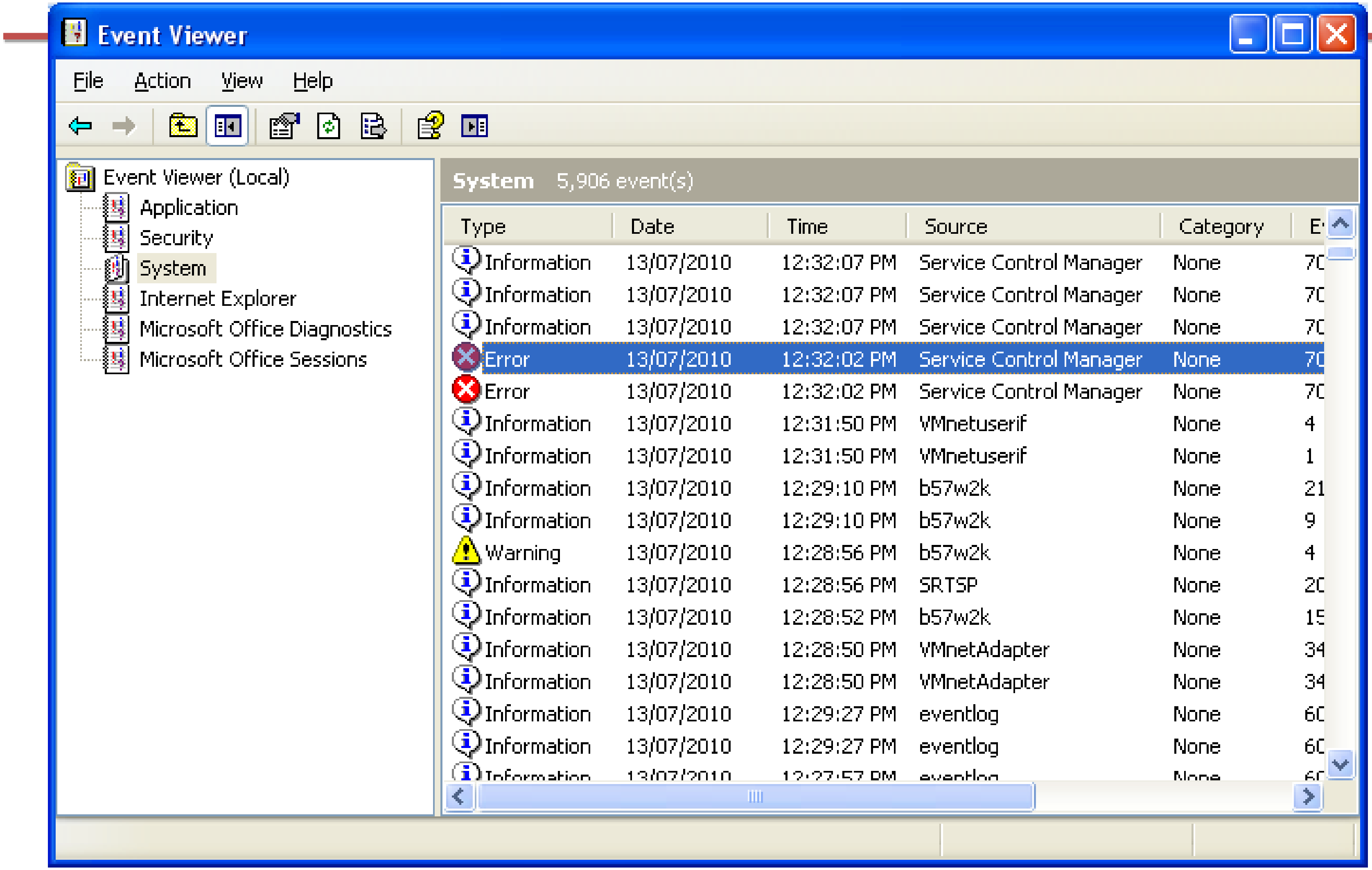
Life Cycle – Detection

- Collection and processing data from the system sources (SIEM, IDPSs, Antivirus software and log analyzers)
- Classification of cyber incidents by types
- Prioritizing cyber incidents
- Managing incidents investigation
- Incident documentation

Signs of incidents

- A **precursor** is a sign that an incident may occur in the future.

- An **indication** is a sign that an incident may have occurred or may be occurring now



System 5,906 event(s)

Type	Date	Time	Source	Category	E
Information	13/07/2010	12:32:07 PM	Service Control Manager	None	70
Information	13/07/2010	12:32:07 PM	Service Control Manager	None	70
Information	13/07/2010	12:32:07 PM	Service Control Manager	None	70
Error	13/07/2010	12:32:02 PM	Service Control Manager	None	70
Error	13/07/2010	12:32:02 PM	Service Control Manager	None	70
Information	13/07/2010	12:31:50 PM	VMnetuserif	None	4
Information	13/07/2010	12:31:50 PM	VMnetuserif	None	1
Information	13/07/2010	12:29:10 PM	b57w2k	None	21
Information	13/07/2010	12:29:10 PM	b57w2k	None	9
Warning	13/07/2010	12:28:56 PM	b57w2k	None	4
Information	13/07/2010	12:28:56 PM	SRTSP	None	20
Information	13/07/2010	12:28:52 PM	b57w2k	None	15
Information	13/07/2010	12:28:50 PM	VMnetAdapter	None	34
Information	13/07/2010	12:28:50 PM	VMnetAdapter	None	34
Information	13/07/2010	12:29:27 PM	eventlog	None	60
Information	13/07/2010	12:29:27 PM	eventlog	None	60
Information	13/07/2010	12:27:57 PM	eventlog	None	60

Indications of Incident

- The network intrusion detection sensor alerts when a buffer overflow attempt occurs against an FTP server.
- The antivirus software alerts when it detects that a host is infected with a worm.
- The Web server crashes.
- Users complain of slow access to hosts on the Internet.
- The application logs multiple failed login attempts from an unfamiliar remote system.
- The email administrator sees a large number of bounced emails with suspicious content.
- The network administrator notices an unusual deviation from typical network traffic flows.
- Any more examples?

Incident detection techniques

- Feedback from customers
- Feedback from staff
- System logs and application logs
- Security events log
- Anti-virus, anti-spyware alerts
- File integrity checking software
- Network-based Intrusion detection system
- Host-based Intrusion detection system
- Third-party monitoring service

Life Cycle –Analysis

- Inspecting alerts, raw events, application and system logs
- Working quickly to analyze and validate each incident, following a pre-defined process and documenting each step taken
- Identifying the attacker and targets
- Assessing the risk to business processes
- Escalating to relevant personnel for further analysis
  - Analyze if it is a targeted attack or an in-the-wild threat (stay silent?)
    - **Analysis steps:**
    - <u>Correlation</u>
  - Identify if the detected activity is a characteristic of an intrusion attempt
    - <u>Structural Analysis</u>
  - Identify if the detected activity is a characteristic of a known intrusion path
    - <u>Intrusion Path Analysis</u>
  - Identify if the intended target is vulnerable to the detected activity
    - <u>Behavior Analysis</u>
  - Identify if the detected ability is permitted by security policy

Life Cycle – Containment / Eradication

- Contain the threat
- If it is of a spreading nature prevent it from spreading further
- Prevent data leakage to the attacker (block communication, disable accounts…)
- Elimination of incident components
- Clean infected machines
- Disable breached accounts
- Evidence should be collected according to procedures that meet all applicable laws and regulations
- If the alert is of a known issue act of predefined knowledge base and decision support.

Life Cycle – Recovery

- Restore systems to normal operation
- Revert any limitations that were used for isolation (fw) firewall
- Confirm that the systems are functioning normally
- If needed restoring systems and/or files from clean backups

Life Cycle – Post-Incident Activity (AR)

Accident Reporting

- AR meetings with all involved parties after a major incident
  - Chain of events (events and times)
  - Findings – what actually happened (unauthorized access)
  - Conclusions – what is the problem that allowed it (open port, weak password…)
  - Recommendations
    - what needs to be done (action items. Close ports, stronger password…
    - Proactive updates (security policy update, training, new product)
- Updating the knowledge base with the specific incident details for next time handling
- Recognize security weaknesses and threats
- Identifying and mitigating all vulnerabilities that were exploited

Incident Handling Boundaries

- Department Manager suspects an employee is using the company's official email to lend credibility to himself, so that he can conduct a profit making businesses.
- Department Manager puts up a request to :
- Access a staff member's email
- Track a staff members activities
- Copy a staff member's hard drive when he is away

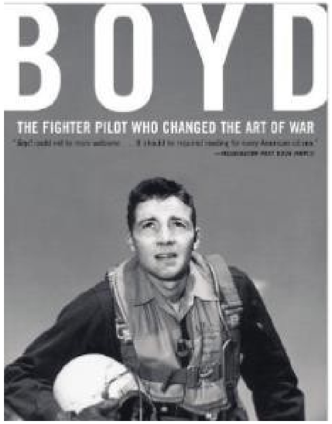
- Should we do that?

OODA loop

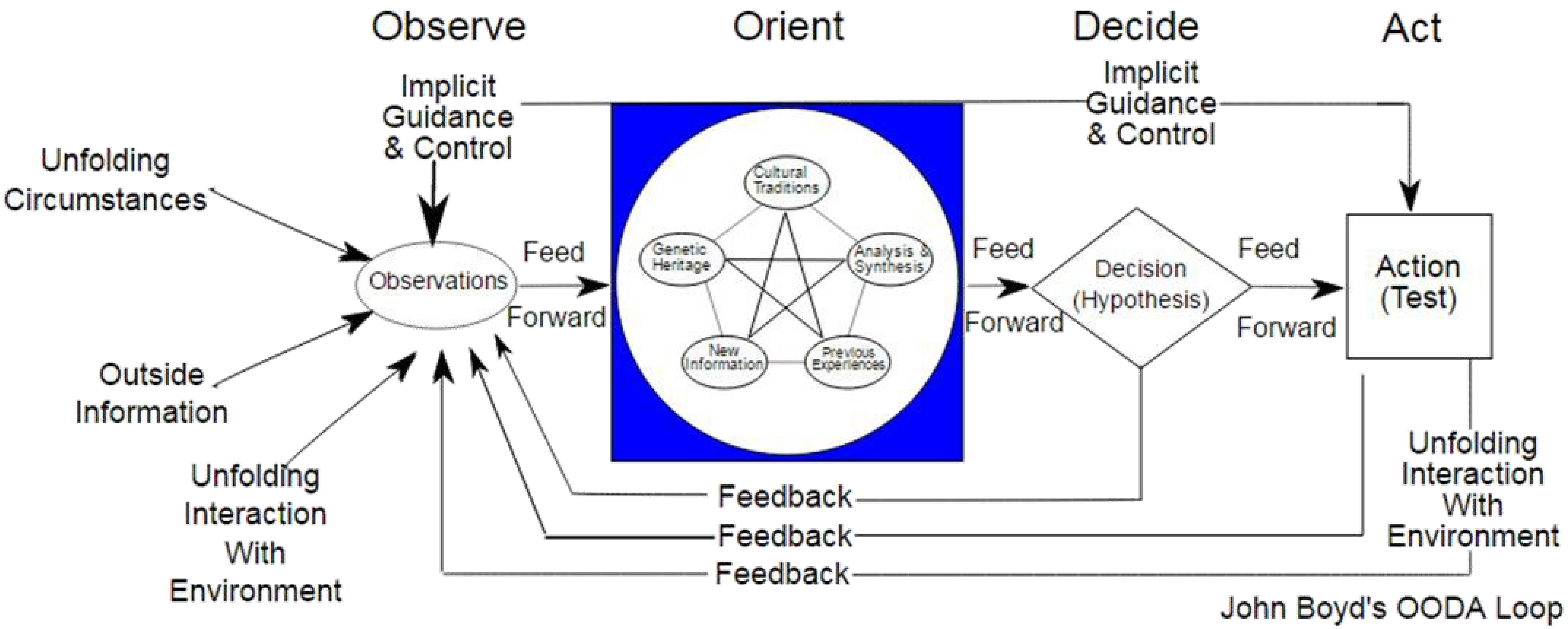
Concepts developed by USAF **Colonel John Boyd** for air- to-air combat, later extended to organizations.

Decision-making occurs in a recurring cycle of **observe-orient-decide-act**.

An entity (whether an individual or an organization) that can process this cycle quickly, observing and reacting to unfolding events more rapidly than an opponent can thereby "get inside" the opponent's decision cycle and gain the advantage.



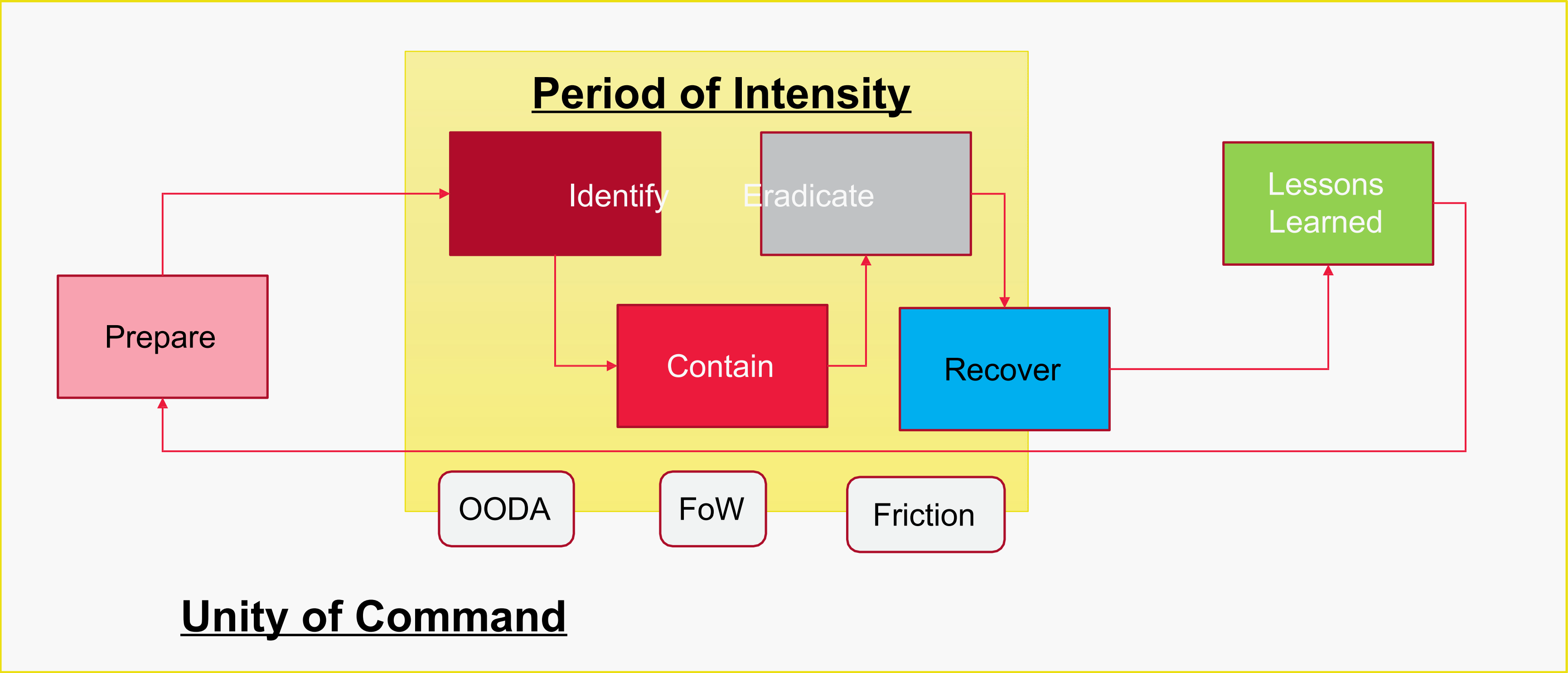
OODA Loop



John Boyd's OODA Loop

https://commons.wikimedia.org/w/index.php?curid=3904554

Conflict in Incident Handling



Real Example of Detection, Analysis and Response – Silicon SOC

Detection :Silicon SOC received an corelated alert on Exploit.url.MVX – Host IP: 10.67.25.197 Date: 26 Feb 2016 10.22:06 SGT

These behaviours were observed: Suspicious JS Activity, Exploit Code Generic Detection, Evasion Behaviour, Exploit code Activity

Analysis: The incident was analysed and the compromised site that was surfed by the user is summarised as such

- GET Request: *hxxp://super.koumas.net/boards/viewforum.php?f=a87&sid=59_huz5pl0p9v1d4a07t7zyzgp7g7tklnwawie7lofiwwz9xsb3-5txyiettf5k23nn2sqs3_36eujtvflqgx4z3nfl5lgj2q*

- Referrer : *hxxp://news.geltuihameleon.info/hellomylittlepiggy/search/?keyword=84190*

- Malicious Host:
  hxxp://super.koumas.net

Real Example of Detection, Analysis and Response – Silicon SOC

Further analysis shows that the user is browsing the website "*hxxp://www.acetraining.com.sg/index.php/course/photoshop-cc-camera-raw/*“”,

which causes the first redirect to an encoded URL of "*hxxp://news.geltuihameleon.info/hellomylittlepiggy/?tLEYInzXIL=mOgjKAPr&Xyatnm=fuObOsjP&keyword=269d169903fd859965d8673c54354c75&ARumlXdxCbVUns=sbSfsvHL&TmxBJHkoPDGfcO=suBKPjPgciz&JQkHhCEwi=EYOgToHPvYlPfpeY&pXfiYXbpSuoPlkJRkKQ=LkiqOynEXw&aruMGr=BpkBhIRsugmGyV&muOdlOBZeP=SZGZaHy&aMzXzkZpcsAAueRtE=KgZimbmwemCXpS*" being served to the user.

- From the first redirect URL, it goes to the second redirect URL "*hxxp://news.geltuihameleon.info/hellomylittlepiggy/search/?keyword=84190*“

- After which, it redirects again to the infected URL

“*hxxp://super.koumas.net/boards/viewforum.php?f=a87&sid=59_huz5pl0p9v1d4a07t7zyzgp7g7tklnwawie7lofiwwz9xsb3-5txyiettf5k23nn2sqs3_36eujtvflqgx4z3nfl5lgj2q*"
“*hxxp://super.koumas.net/to.jss?go=nJmE29EALJ&suppose=&game=N1-W&eye=&rule=NvZw&watch=rpLPWf3YFCQXH__XX3XOnL9HnU9vxn*"
“*hxxp://super.koumas.net/change.wrf?out=&ask=lhOwwlz&drive=&respect=JDTia&literature=spKn&direct=tx-IdT&however=&close=fiWaF&meeting=kcs8umaaGXwD3xtMwpXeX*"

Real Example of Detection, Analysis and Response – Silicon SOC

Response Phase:

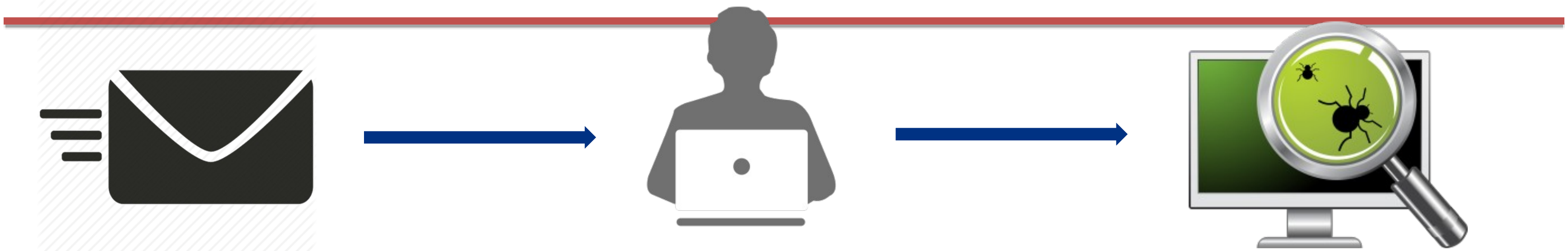
- Containment

- Blacklist the malicious URLs: **hxxp://super.koumas.net**, and **hxxp://news.geltuihameleon.info/hellomylittlepiggy/**
- Disconnect and isolate the host from the network
- Backup

- Eradication and Recovery

- Format and do a clean reinstallation of the operating system
- Update to the latest version of flash player for all the end hosts

Recent Real World Incidents



Attacker sends a Dridex malware infected attachment spoofed as a copier email.

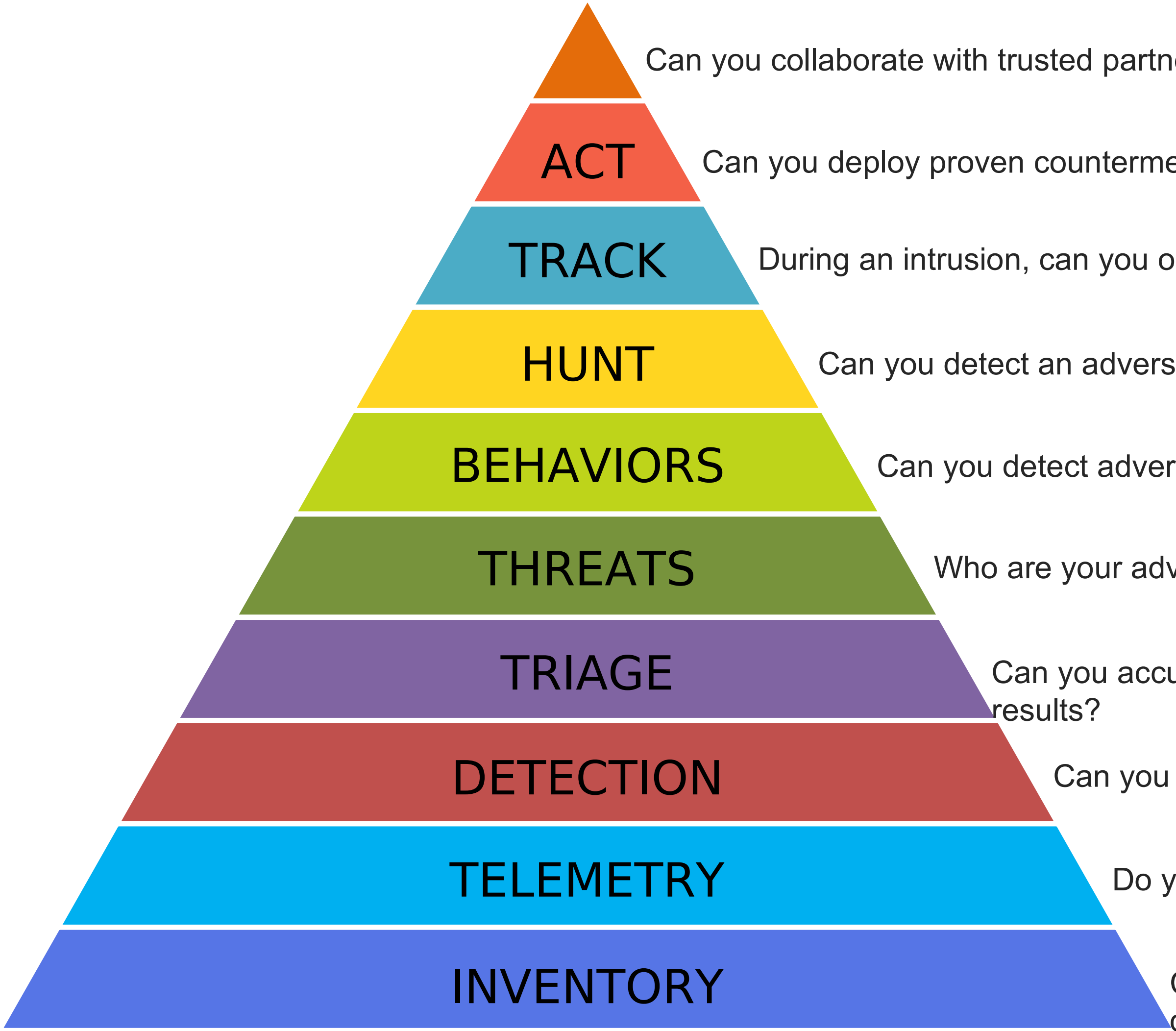
Victim unknowingly opens attachment due to the email seemingly coming from a known source

Computer becomes compromised by malware hidden in attachment

Dridex is a strain of banking malware that leverages macros in Microsoft Office to infect systems.

- The attacker uses a Microsoft Office document embedded with the Dridex malware,if macros are enabled, the document will try to drop malware and infect the Windows host.
- Once the malware is installed, the attacker can steal banking credentials and create fraudulent transactions.
- “Word Exploit CVE-2015” were used to embed these malwares and the attachment has no threat detection.

IR Hierarchy of Capabilities



Can you collaborate with trusted partners to disrupt adversary campaigns?

ACT — Can you deploy proven countermeasures to evict and recover?

TRACK — During an intrusion, can you observe adversary activity in real time?

HUNT — Can you detect an adversary that is already embedded?

BEHAVIORS — Can you detect adversary activity within your environment?

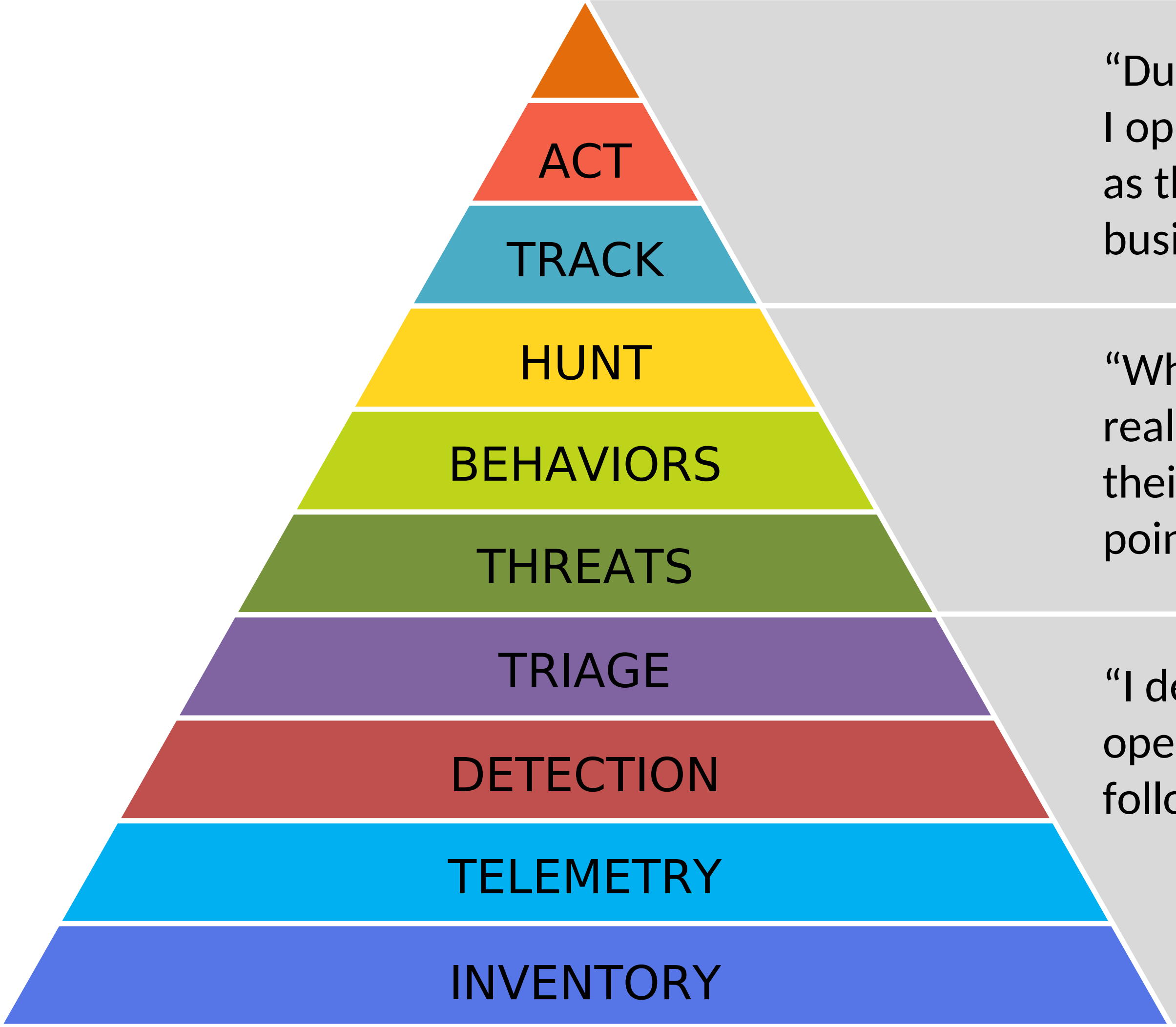
THREATS — Who are your adversaries? What are their capabilities?

TRIAGE — Can you accurately classify detection results?

DETECTION — Can you detect unauthorized activity?

TELEMETRY — Do you have visibility across your assets?

INVENTORY — Can you name the assets you are defending?



“During incident response,
I operate at the same tempo
as the adversary to protect my
business assets.”

“When my red team emulates a
real-world adversary, I detect
their intrusion at multiple
points along the kill chain.”

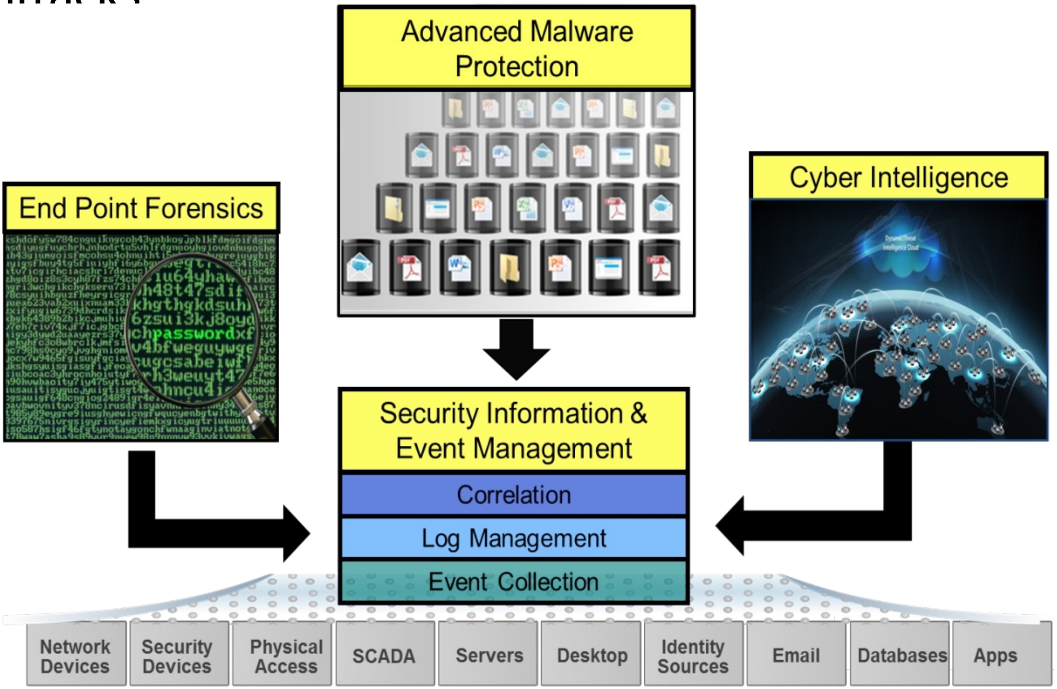
“I detect hygiene issues and
operator activity that does not
follow best practices.”

What is a Security Operation Centre?

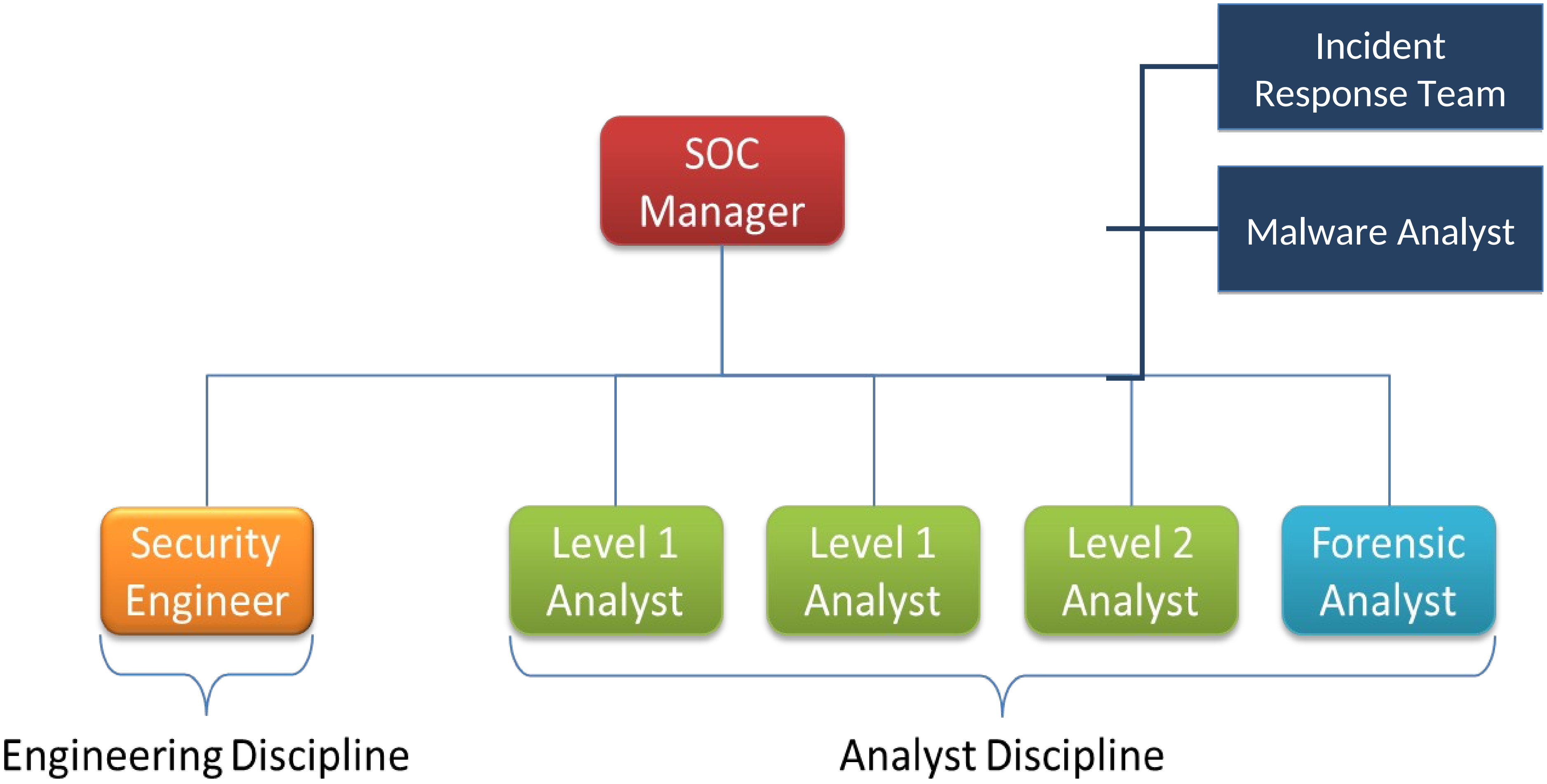
Centralised facility that collects information on threats, and protect an organisation’s IT systems against attacks:

- Internal Threats
- External threats
- User Activities
- Policy Violation
- Systems Availability

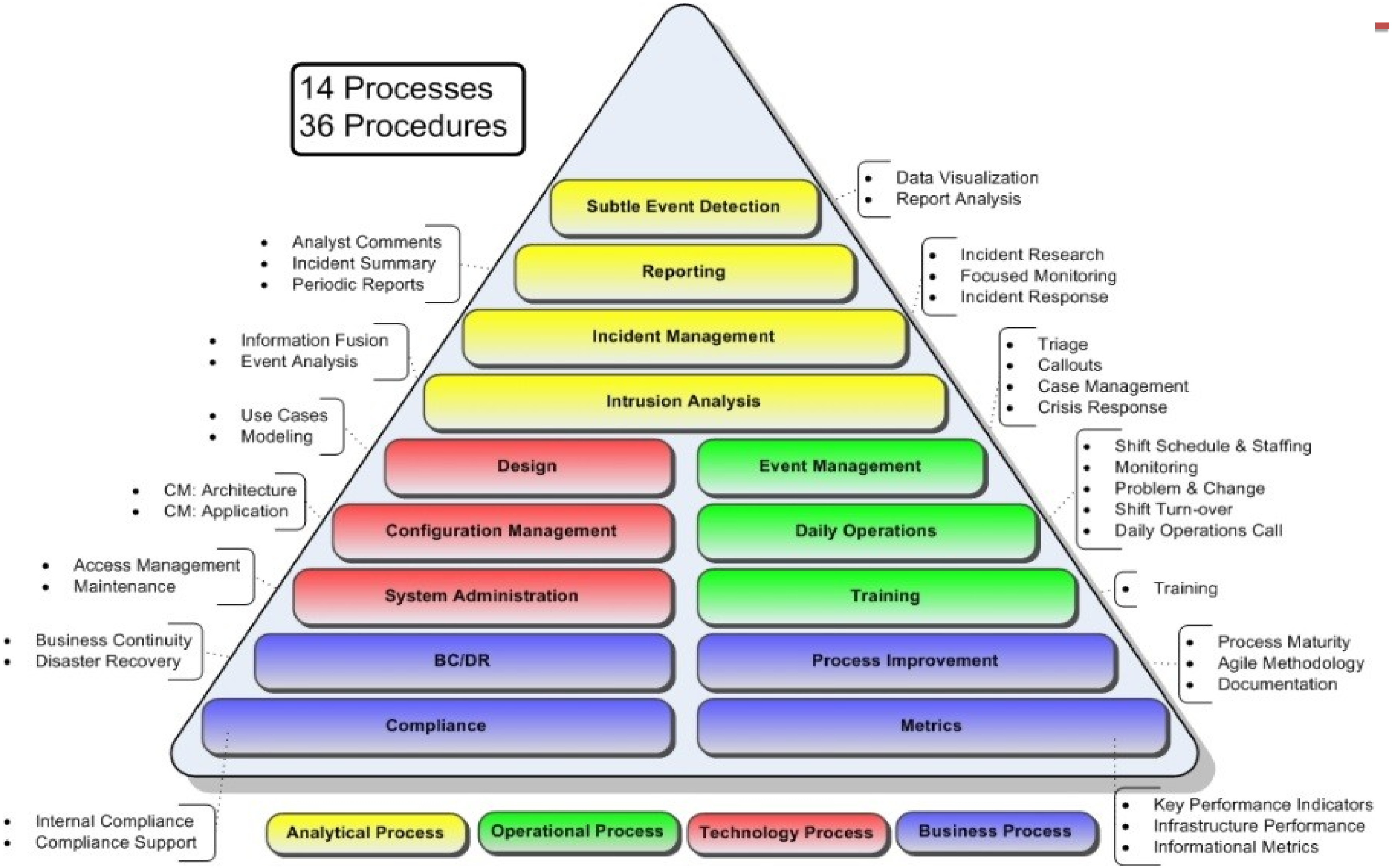
A SOC also provides for capabilitie



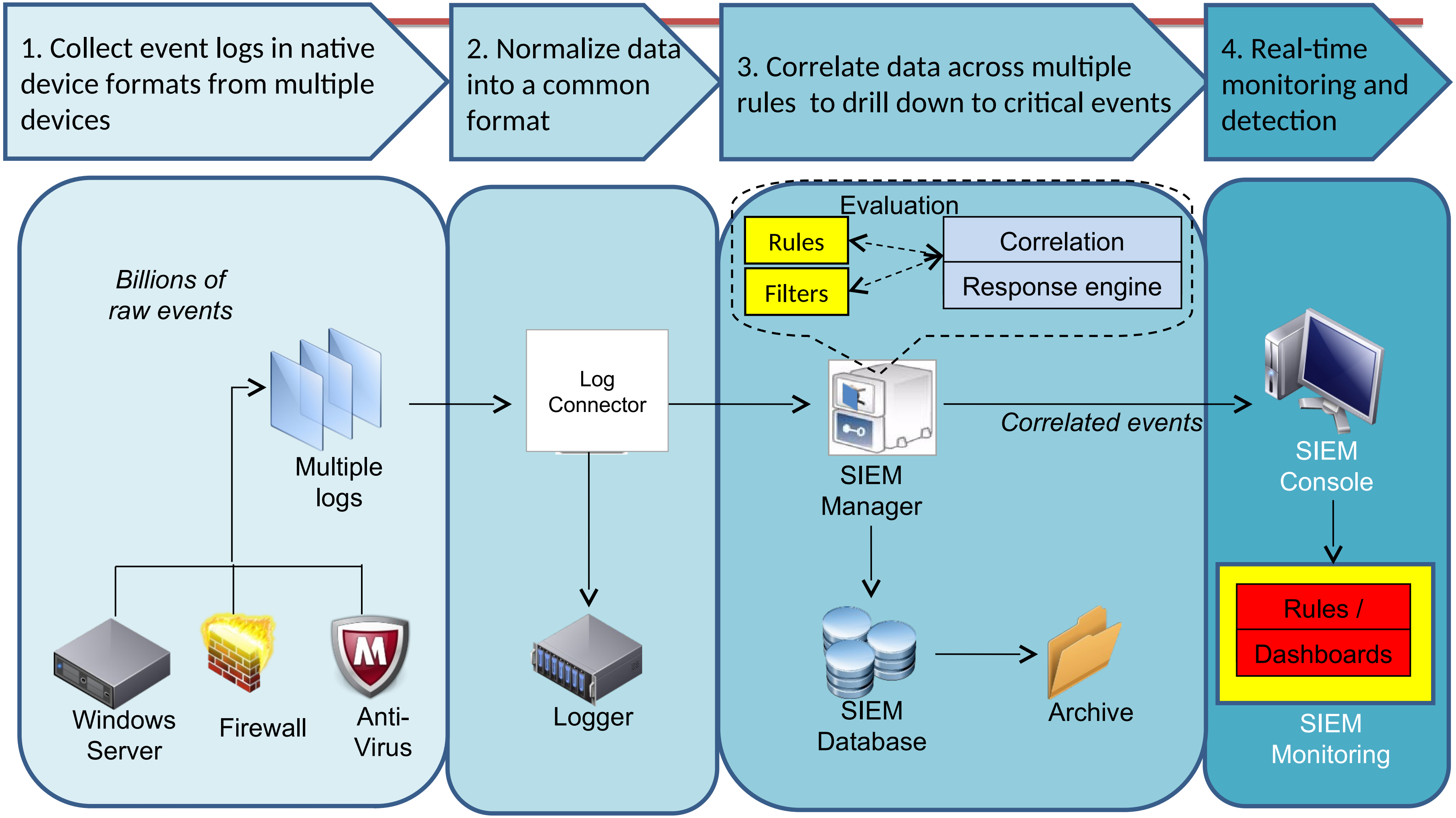
People - Typical SOC Staffing



Processes in a SOC



Technology - From Raw Logs to Correlated Security Events



The Need for An Incident Response Plan

- Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented.

- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

- An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring business services

Incident Management Guidelines

In order to facilitate an efficient and effective incident response capability, the following actions are recommended:

- Defining incident response policy and plan
- Procedures planning for incident handling and reporting
- Setting guidelines for communicating with internal\external groups regarding incidents
- Selecting and staffing an incident response team according to pre-defined structure and staffing model
- Determining the services provided by the incident response team
- Training plans for the incident response team.

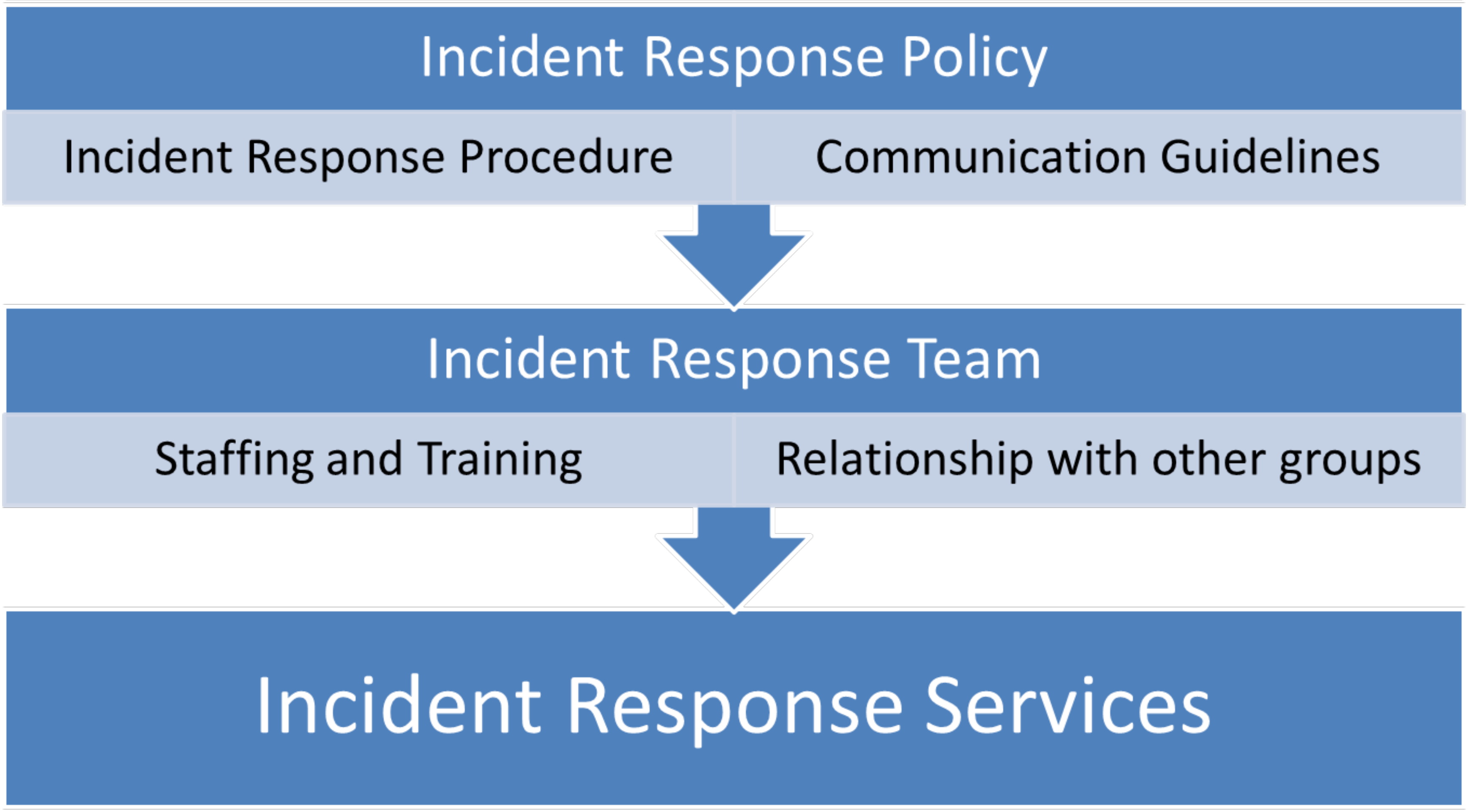
Why Incident Response?

- Preventative activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented.
- An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Need for Incident Response and its Benefits

- Responding to incidents systematically so that the appropriate steps are taken
- Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information, and disruption of services
- Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
- Dealing properly with legal issues that may arise during incidents.

Information Security Incident Management Framework



Incident Response Policy

Incident Response Procedure

Communication Guidelines

Incident Response Team

Staffing and Training

Relationship with other groups

Incident Response Services

Establish an Incident Response Team

- Incident response team personnel
- Incident response team staffing
- Selection of team models
- Outsourcing contractor issues
- Dependencies within organizations

Incident Response Team Personnel

- Team manager and duty team manager
  - Regardless of which incident response model an organization chooses, a single employee should be in charge of incident response.
  - In a fully outsourced model, team manager is responsible for overseeing and evaluating the outsourcer’s work.
  - In all other models, this responsibility is generally achieved by having a team manager and a deputy team manager who assumes authority in the absence of the team manager.
- Technical lead
- Team members with good technical and communication skills

Incident Response Team Staffing

- Employees
  - The organization performs all of its incident response work, with limited technical and administrative support from contractors

- Partially Outsourced
  - The organization outsources portions of its incident response work.
  - The most prevalent arrangement is for the organization to outsource 24-hour-a-day, 7-day-a-week (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite managed security services provider
  - Some organizations perform basic incident response work in-house and call on contractors to assist with handling incidents, particularly those that are more serious or widespread. The services most often performed by the contractors are computer forensics, advanced incident analysis, incident containment and eradication, and vulnerability mitigation.

Incident Response Team Staffing

- Fully Outsourced
  - The organization completely outsources its incident response work, typically to an onsite contractor.
  - This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees.

Training

- Regular mock-up incident response exercise
- Walkthrough the incident response policy and procedures
- Attend external training courses
- Drafting new incident response procedures
- After a major incident has been handled, the organization should hold a lessons learned meeting to review how effective the incident handling process was and identify necessary improvements to existing security controls and practices.
- Lessons learned meetings should also be held periodically for lesser incidents. The information accumulated from all lessons learned meetings should be used to identify systemic security weaknesses and deficiencies in policies and procedures.
- Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes but also for reference in handling future incidents and in training new incident response team members.
- An incident database, with detailed information on each incident that occurs, can be another valuable source of information for incident handlers.

Selection of Team models

- Central Incident Response Team
  - A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for large organizations with minimal geographic diversity in terms of computing resources
- Distributed Incident Response Teams
  - An organization has multiple incident response teams, each responsible for handling incidents for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations
- Coordinating Team
  - An incident response team provides guidance and advice to other teams without having authority over those teams

Factors to be considered when selecting team model

- The Need for 24/7 Availability
  - Larger organizations, as well as smaller ones that support critical infrastructures, usually need incident response staff to be available 24/7
- Full-Time Versus Part-Time Team Members
  - Organizations with limited funding, staffing, or incident response needs may have only part-time incident response team members. In this case, the incident response team can be thought of as a volunteer fire department.
- Cost
- Staff Expertise

Factors to be considered when selecting team model

- Employee Morale
  - Incident response work is very stressful, as are the on-call responsibilities of most team members. This combination makes it easy for incident response team members to become overly stressed. Many organizations will also struggle to find willing, available, experienced, and properly skilled people to participate, particularly in 24-hour support.
- Organizational Structures
  - If an organization has three departments that function **independently**, incident response may be more effective if each department has its own incident response team. The main organization can host a centralized incident response entity that facilitates standard practices and communications among the teams.

Outsourcing Contractor Issues

- Sensitive Information Revealed to the Contractor
- Current and Future Quality of Work of the contractor
- Division of Responsibilities
- Lack of Organization-Specific Knowledge.
- Lack of Correlation -
  - If the intrusion detection system records an attempted attack against a Web server, but the outsourcer has no access to the Web logs, it may be unable to determine whether the attack was successful.

Outsourcing Contractor Issues

- Handling Incidents at Multiple Locations
  - If the outsourcer is offsite, consider where the outsourcer is located, how quickly it can have an incident response team at any facility, and how much this will cost.
- Maintaining Incident Response Skills In House
  - Organizations that completely outsource incident response should strive to maintain basic incident response skills in house. Situations may arise in which the outsourcer is unavailable. E.g. outsourcer is busy handling incidents at other customers' sites.

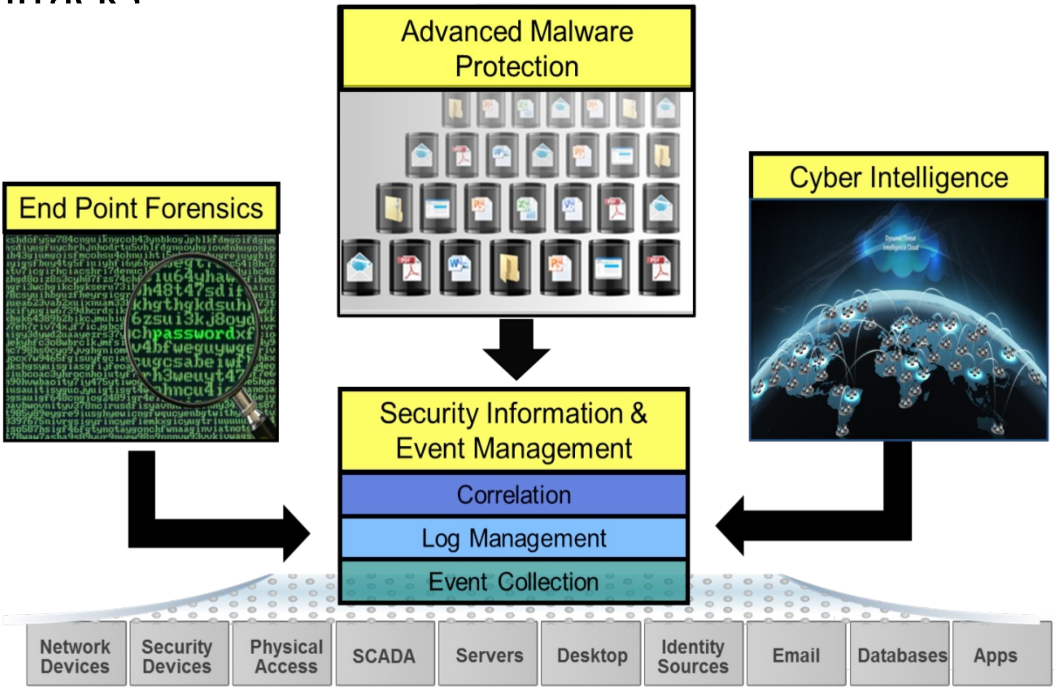
Dependencies Within Organizations

- Incident response team relies on the expertise, judgment, and abilities of others, including
  - Management
  - Information security
  - Telecommunications
  - IT support
  - Legal department
  - Public affairs and media relations
  - Human resources
  - Physical security and facility management
  - Business continuity planning

What is a Security Operation Centre?

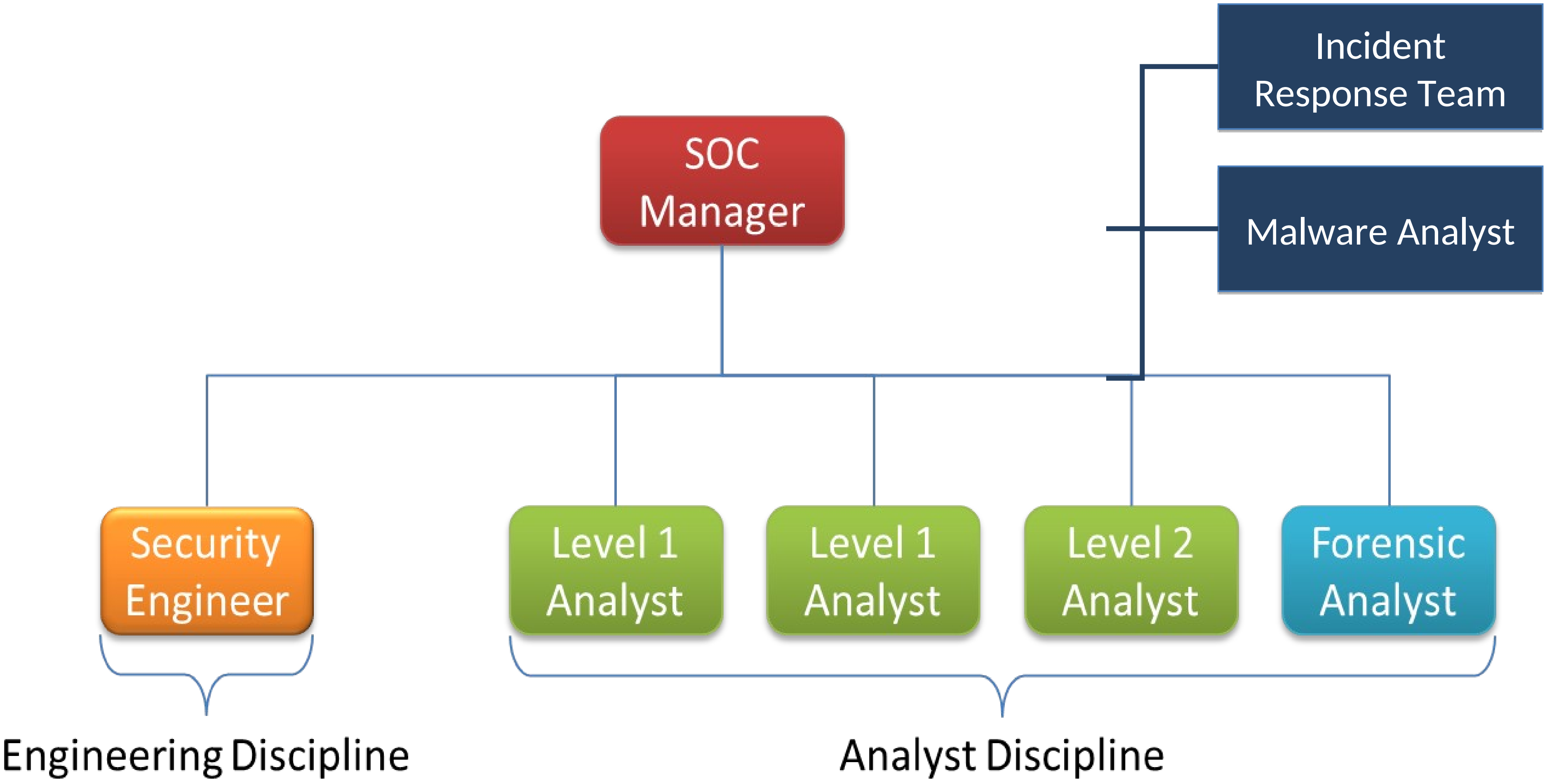
Centralised facility that collects information on threats, and protect an organisation's IT systems against attacks:

- Internal Threats
- External threats
- User Activities
- Policy Violation
- Systems Availability

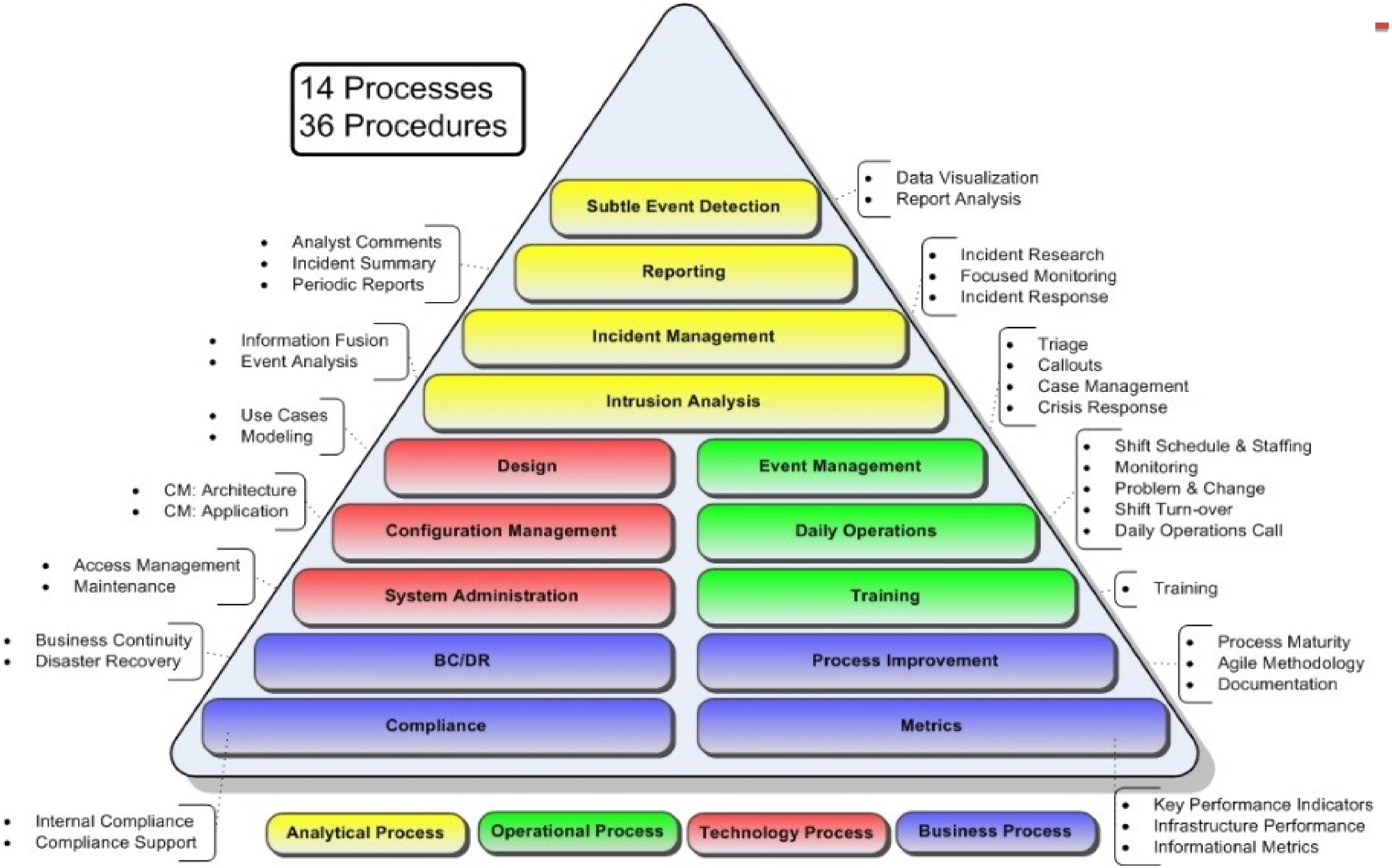


A SOC also provides for capabilitie

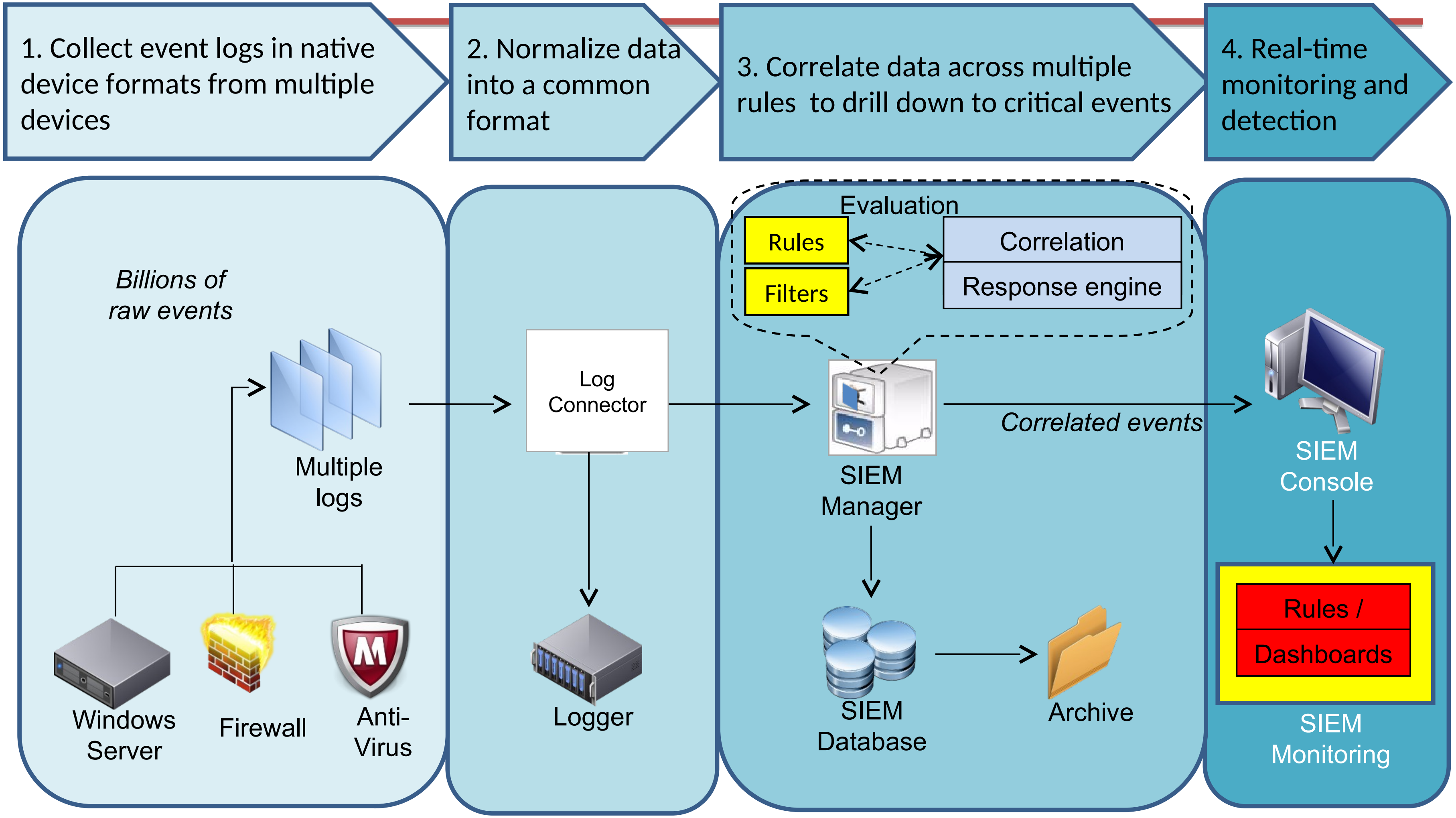
People - Typical SOC Staffing



Processes in a SOC



Technology - From Raw Logs to Correlated Security Events



www.sp.edu.sg

Singapore Polytechnic
500 Dover Road
Singapore 139651

tel. (65) 6775 1133
fax. (65) 6870 6189