SECURITY OPERATION CENTER

Agenda

- What is Security Management
- What is Security Operation Center
- The need of Security Operation Center
- How SOC helps in building better security
- The traditional idea of SOC

REDTEAM®
HACKER ACADEMY

What is Security Management?

Security management is the identification of an organization's assets, followed by the development, documentation, and implementation of policies and procedures for protecting these assets.

REDTEAM®
HACKER ACADEMY

What is Security Operation Center?

A security operations center (SOC) is a centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology. Typically, a SOC is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers.

The need of security operation center

- **Proactive detection**
- **Threat awareness**
- **Vulnerability management**
- **Awareness of hardware and software assets**
- **Log management**

REDTEAM®
HACKER ACADEMY

Why build SOC

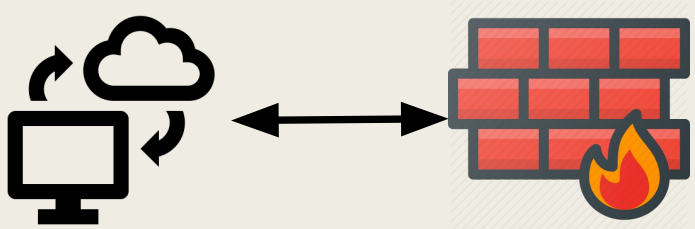
SOC Goals

Aligned with Business goals

Shared service to reduce cost

Improves Risk posture

How SOC helps in building better security



The Traditional Idea of SOC

Machine Logs

```
[Fri Dec 16 01:46:23 2005]
[error] [client 1.2.3.4]
Directory index forbidden by
rule: /home/test/
[Fri Dec 16 01:54:34 2005]
[error] [client 1.2.3.4]
Directory index forbidden by
rule: /apache/web-data/test2
[Fri Dec 16 02:25:55 2005]
[error] [client 1.2.3.4] Client
sent malformed Host header
[Mon Dec 19 23:02:01 2005]
[error] [client 1.2.3.4] user
test: authentication failure for
"/~dcid/test1": Password Mismatch
```

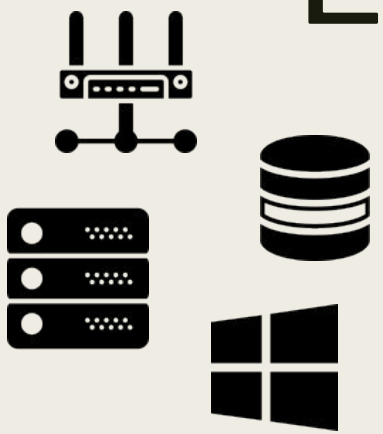
Security Information Event Management

Optimization
Metrics Prioritizing Reporting
Identify Learning Recovery Detection
Response Correlation Authority
Dashboard Consolidation Alerting
Monitoring Containment
Communication Intelligence Escalation
Forensic Investigation
Analysis

External Data

- Website
- Discussion Forum
- Social Media
- Darknet
- Darkweb
- Threat Intel
- Etc

Machine Logs



- **Application Logs**
- **Service Logs**
- **Event Logs**
- **System Logs**

```
192.168.2.20 - - [28/Jul/2006:10:27:10 -0300] "GET /cgi-
bin/try/ HTTP/1.0" 200 3395
127.0.0.1 - - [28/Jul/2006:10:22:04 -0300] "GET /
HTTP/1.0" 200 2216

x.x.x.90 - - [13/Sep/2006:07:01:53 -0700] "PROPFIND
/svn/[xxxx]/Extranet/branches/SOW-101 HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:07:01:51 -0700] "PROPFIND
/svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587  x.x.x.90
- - [13/Sep/2006:07:00:53 -0700] "PROPFIND
/svn/[xxxx]/[xxxx]/2.5 HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:07:00:53 -0700] "PROPFIND
/svn/[xxxx]/Extranet/branches/SOW-101 HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:07:00:21 -0700] "PROPFIND
/svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587  x.x.x.90
- - [13/Sep/2006:06:59:53 -0700] "PROPFIND
/svn/[xxxx]/[xxxx]/2.5 HTTP/1.1" 401 587
x.x.x.90 - - [13/Sep/2006:06:59:50 -0700] "PROPFIND
/svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587  x.x.x.90
- - [13/Sep/2006:06:58:52 -0700] "PROPFIND
/svn/[xxxx]/[xxxx]/trunk HTTP/1.1" 401 587  x.x.x.90
- - [13/Sep/2006:06:58:52 -0700] "PROPFIND
/svn/[xxxx]/Extranet/branches/SOW-101 HTTP/1.1" 401 587
[Fri Dec 16 01:46:23 2005] [error] [client 1.2.3.4]
Directory index forbidden by rule: /home/test/  [Fri
Dec 16 01:54:34 2005] [error] [client 1.2.3.4]
Directory index forbidden by rule: /apache/web-
data/test2
[Fri Dec 16 02:25:55 2005] [error] [client 1.2.3.4]
Client sent malformed Host header
[Mon Dec 19 23:02:01 2005] [error] [client 1.2.3.4] user
test: authentication failure for "/~dcid/test1":  Password
Mismatch
```

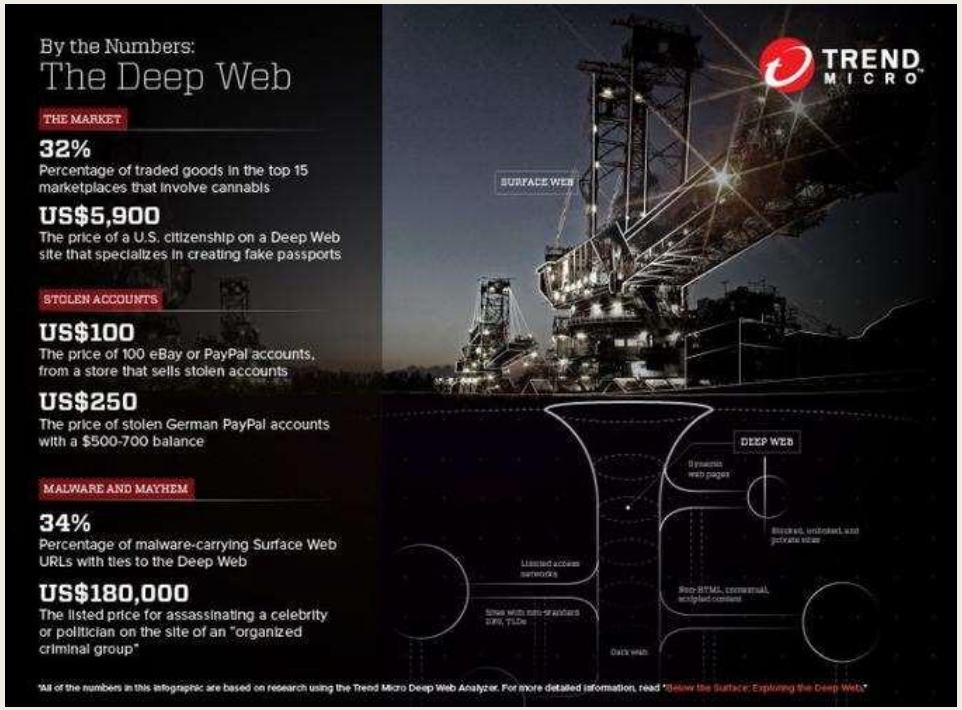
Security Information Event Management

"Traditional SOC put more weight on people by introducing 24/7 security monitoring activities"

CERTIFIED ISO 9001:2015 COMPANY

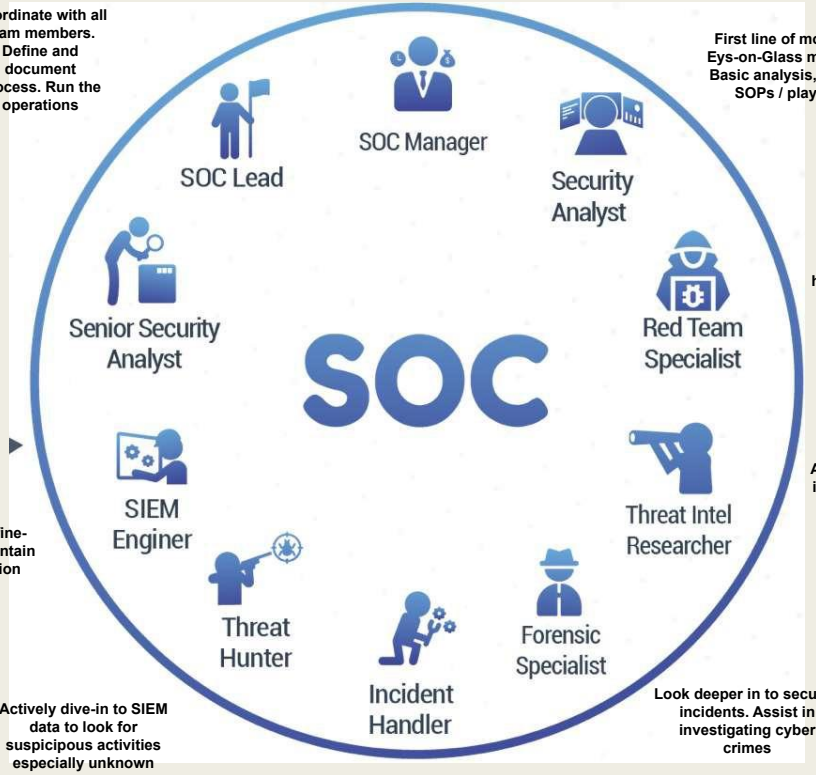
REDTEAM HACKER ACADEMY

External Data



Magic Word: Threat Intelligence

People-Centric SOC



CERTIFIED ISO 9001:2015 COMPANY

REDTEAM® HACKER ACADEMY

People-Centric SOC

"People-Centric SOC introduce painful issue to organisation"

"Don't you think it is inhuman to let people watch the screen for 8 hours especially in the middle-of night"?

"It is industry 4.0 era"

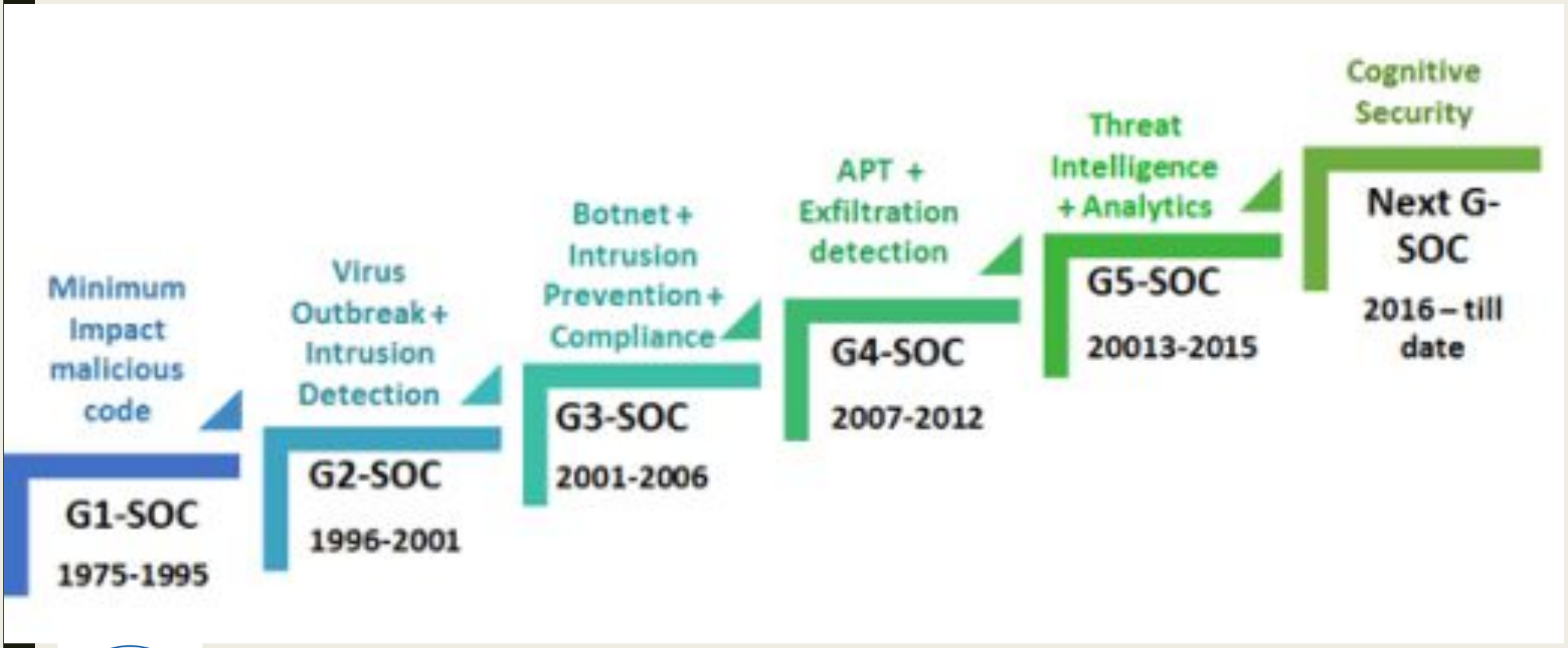
CERTIFIED ISO 9001:2015 COMPANY

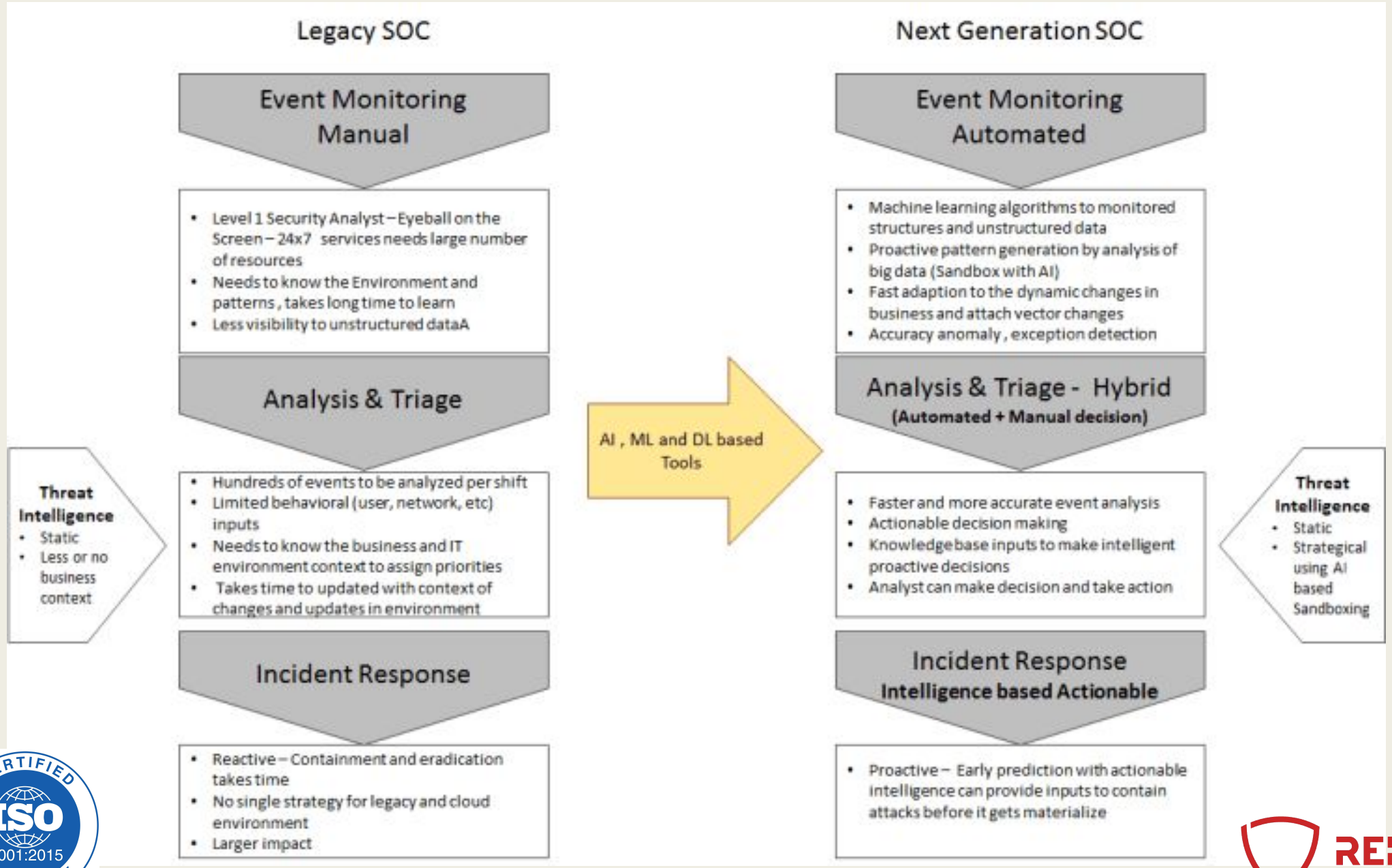
CERTIFIED ISO 9001:2015 COMPANY

REDTEAM® HACKER ACADEMY

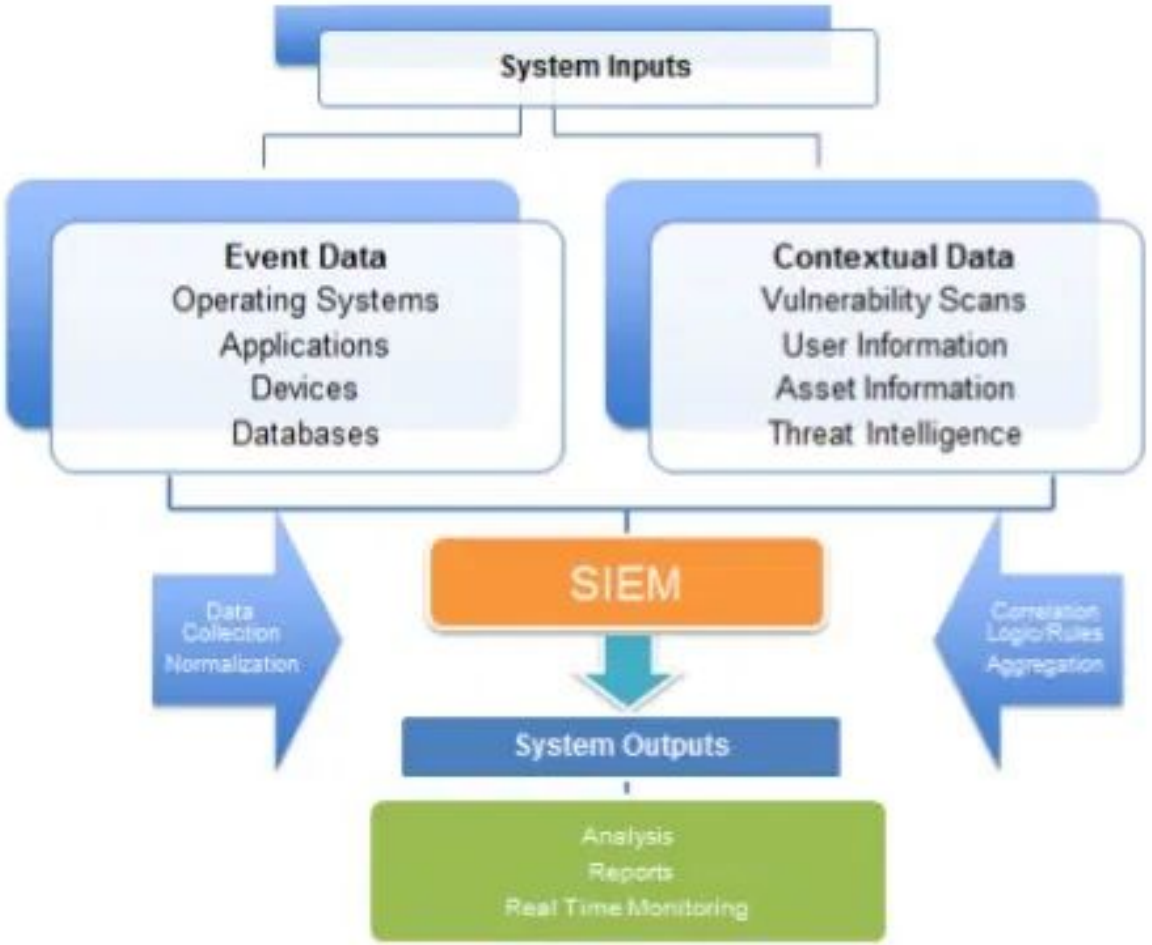
“Next-Gen Security Operation Center vision is to improve technology, people, and process in Traditional SOC”

REDTEAM®
HACKER ACADEMY





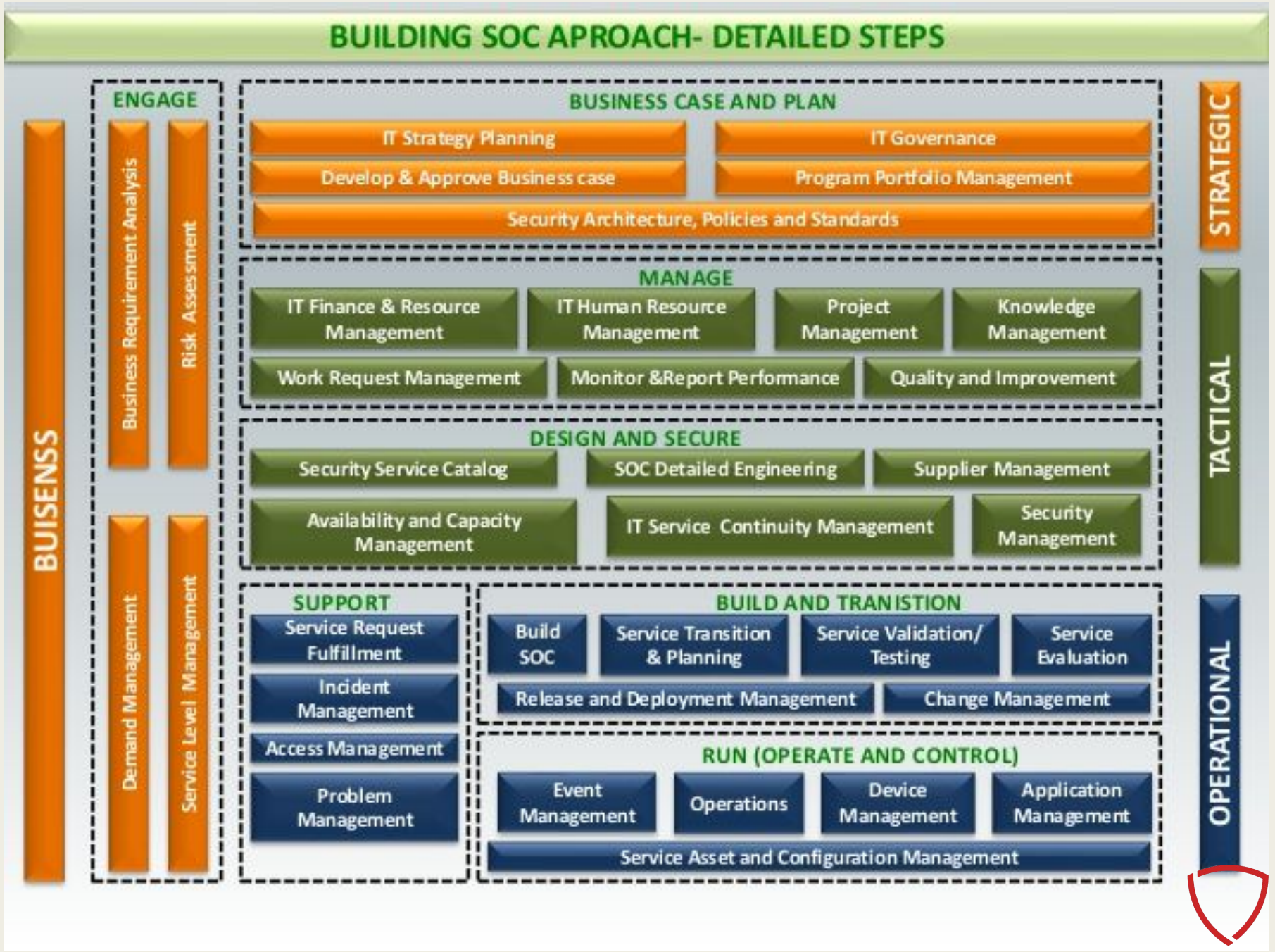
SIEM Architecture

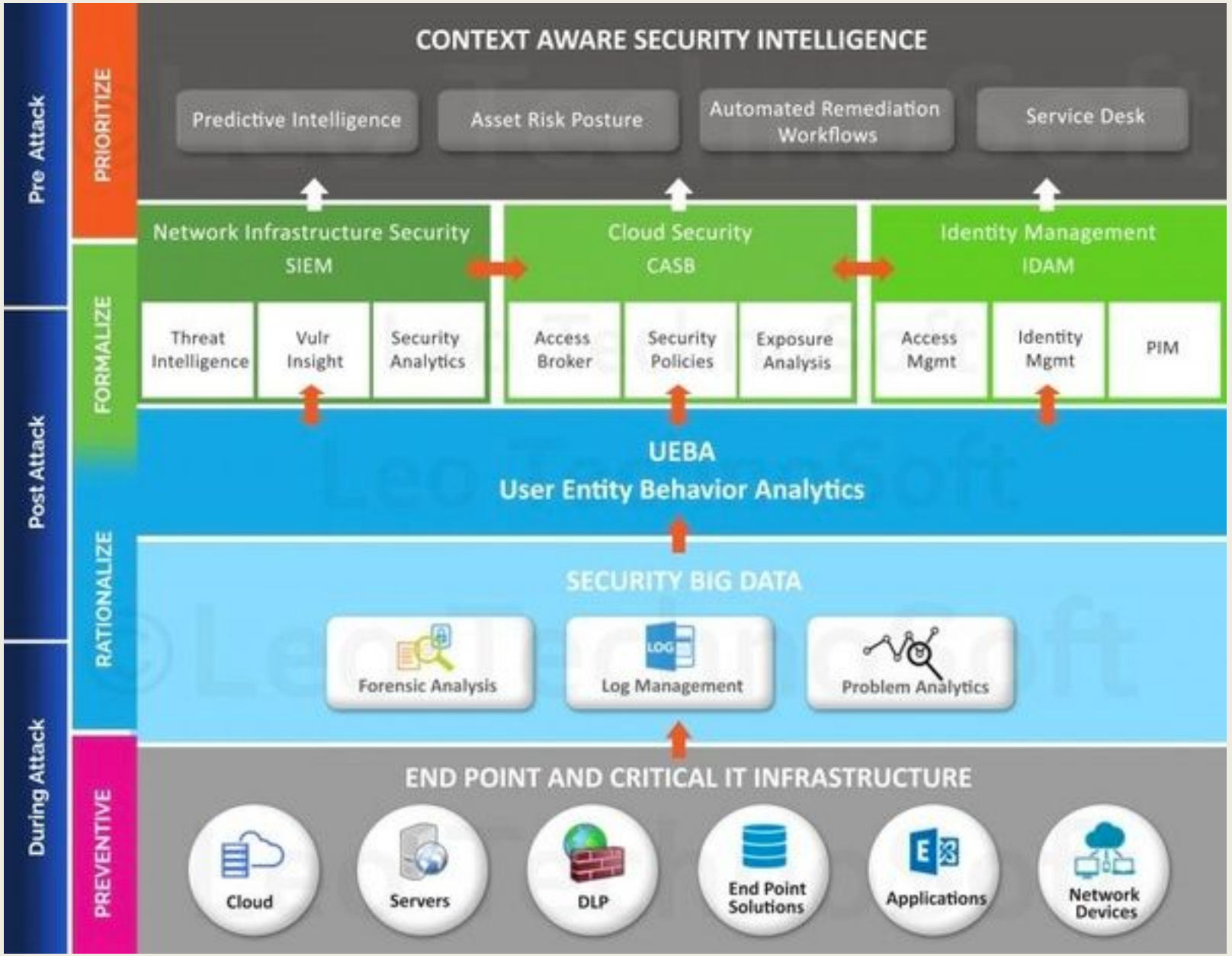


- Log Collection
- Log Analysis
- Log Correlation
- Log Forensics
- IT Compliance
- Application Log Monitoring
- Object Access Auditing

SIEM

- "Real-time" Alerting
- User Activity Monitoring
- Dashboards
- Reporting
- File Integrity Monitoring
- System & Device Log Monitoring
- Object Access Auditing





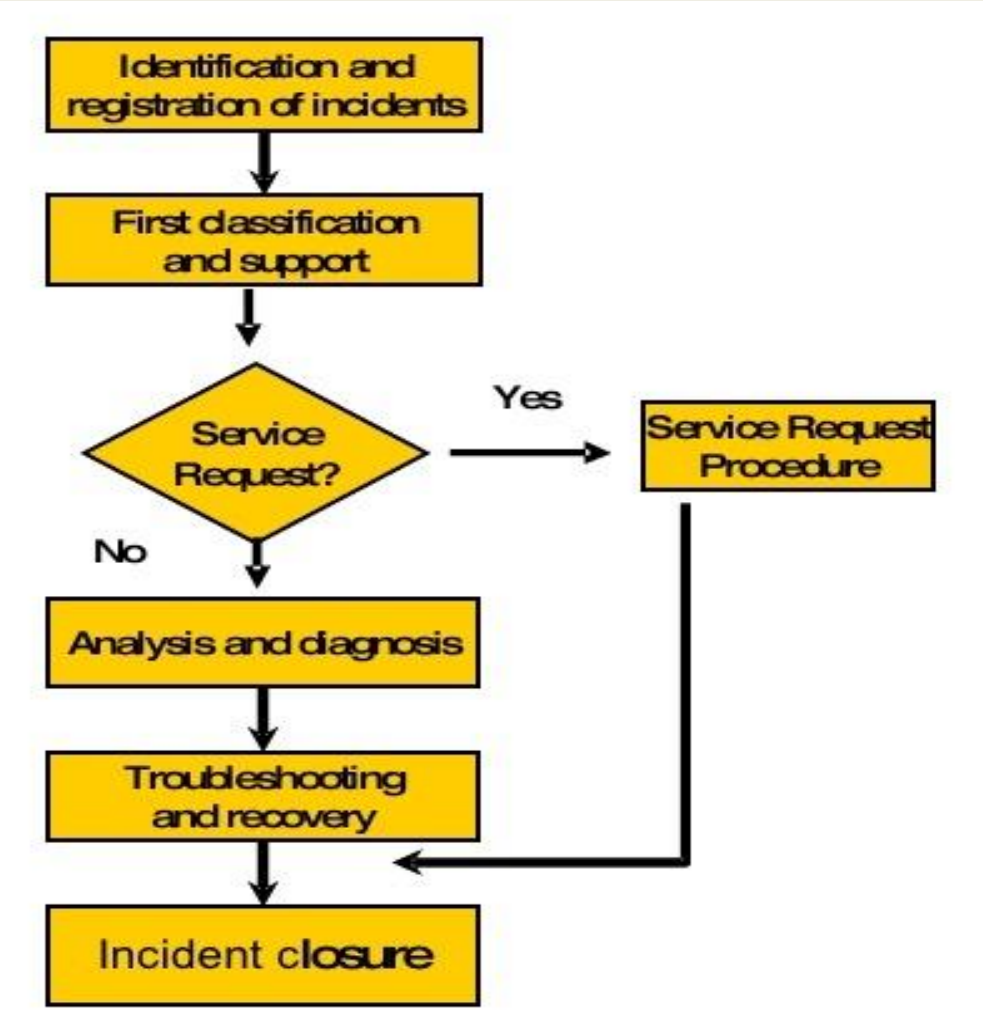
What is Incident Management

The Incident Management can be defined by it's primary objective that is to restore normal service operations, with Service Level Agreement limits, as quickly as possible after an incident has occurred to that service and minimize the adverse impact on the business operations

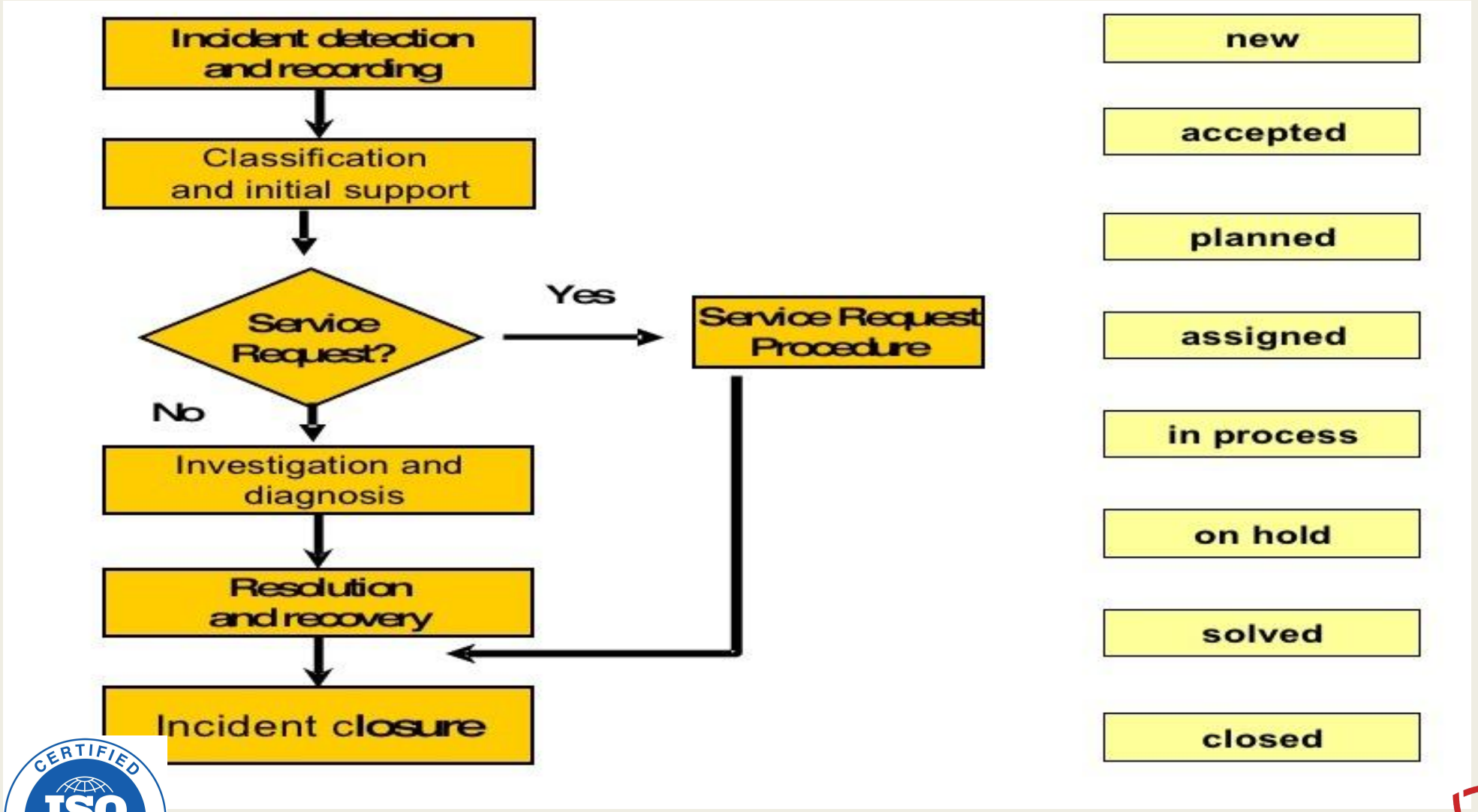
The main goals of Incident Management processes are:

- Restore the service as quickly as possible
- Minimum disruption to users' work
- Management of an incident during its entire lifecycle
- Support of Related Operational Activities

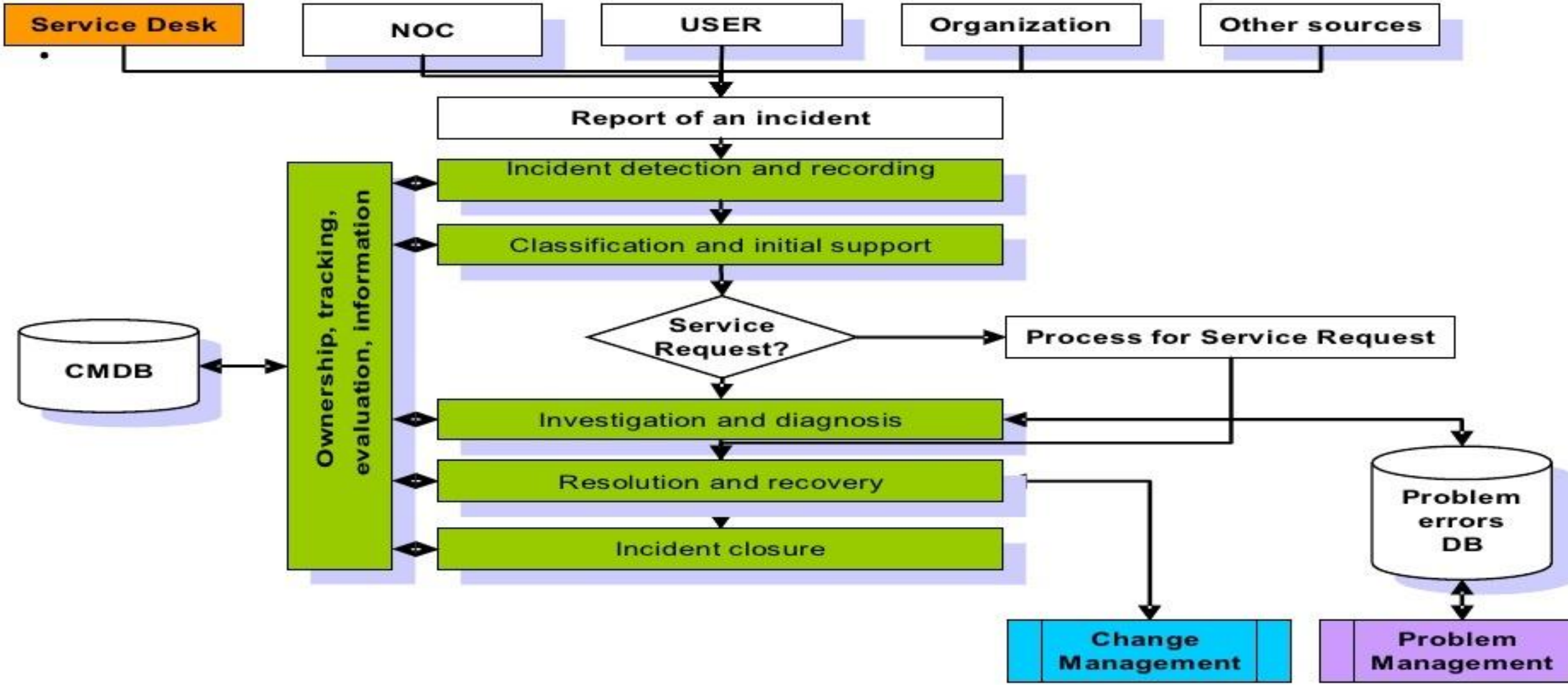
Core Activities of Incident Management process



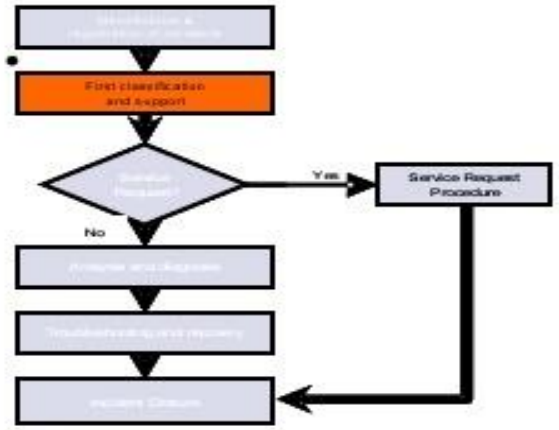
Lifecycle of an Incident



Incident Management : Activities



Incident Management Classification: Find service affected, Match against SLA, and Assign Priority



Classification:

- Impact
  - Reflects business criticality of the incident
  - Reflects extent to which an incident leads to degradation of SLA, such as number of users that suffer
- Urgency
  - Reflects required speed of solving an incident
- Workload
  - Reflects expected effort to solve the incident
- Priority
  - Reflects order in which to solve the incidents

Priority = Impact + Urgency

Incident Management :Escalation

- Objective of an escalation or escalation procedure is the avoidance or minimizing of material or immaterial damage. The definition of an escalation comprises:
-
  - *escalation trigger*
  - *escalation measures*
  - *escalation levels*

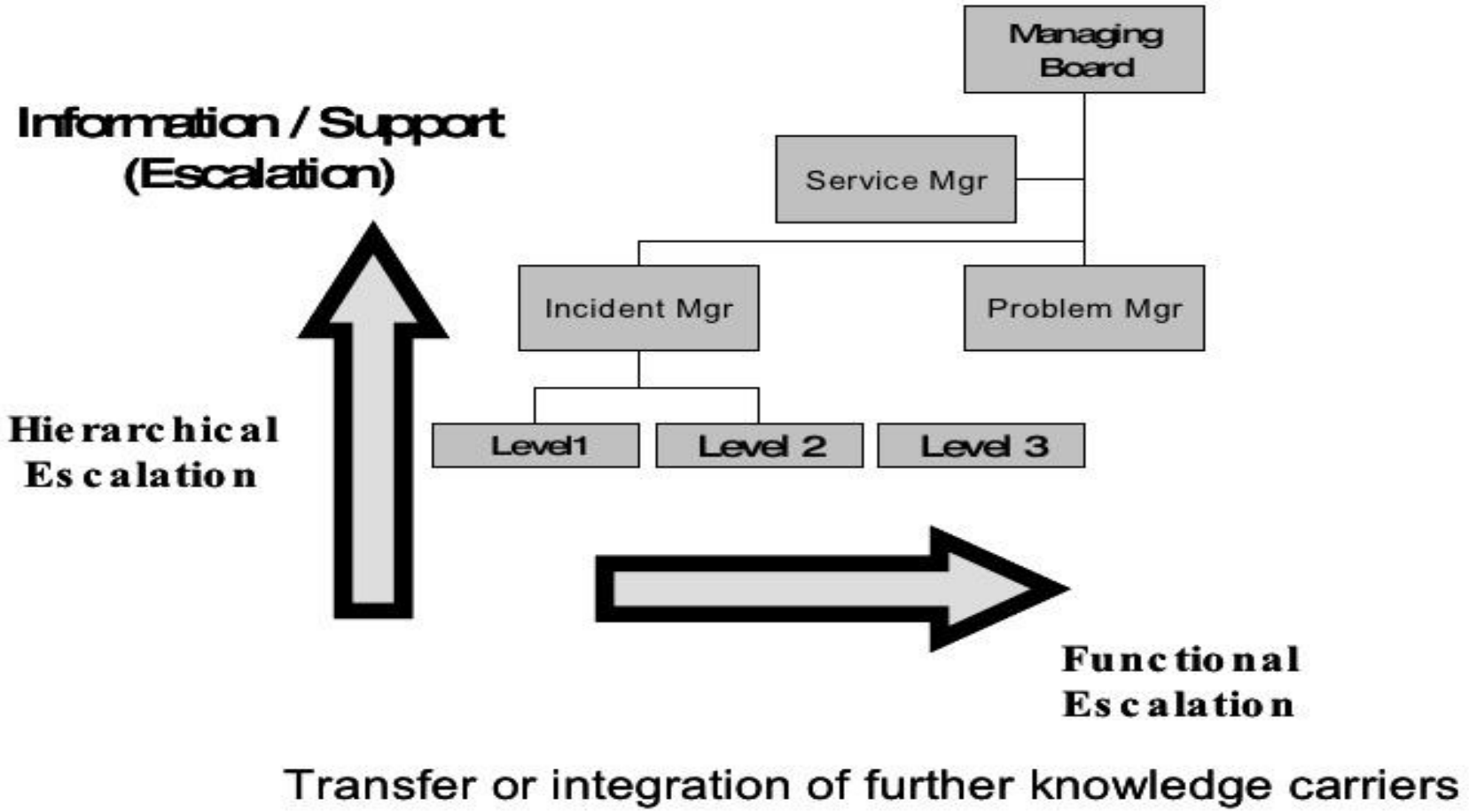
- The combination of the three keys results in an
  - *escalation matrix with escalation paths*

- The escalation procedures should be clearly agreed between all involved parties. Escalation can usefully improve service provision only if it is accepted by all parties.

Escalation should not be misused as a proof of guilt.

Incident Management: Types of Escalation

Functional versus hierarchical escalation



Transfer or integration of further knowledge carriers

Incident Management
Input and Output

Input

- Incident reports from Service Desk and Monitoring
- Information about users, system configuration, service levels
- Information about solutions, tested workarounds
- Information about changes performed

Output

- Requests for change to Change Management
- Information about incidents or problems to Problem Management
- Solved and closed incidents
- Information to the user
- Reports to management

Incident Management :Benefits

- Reduced business impact of incidents by timely resolution
- Proactive identification of possible enhancements
- Management information related to business-focused SLA
- Improved monitoring
- Improved management information related to aspects of service
- Better staff utilization: no more interruption-based handling of incidents
- Elimination of lost incidents and service requests
- Better and accurate CMDB information
- Better user/customer satisfaction

Key Performance indicators

- Total number of Incidents
- Average time to restore service from point of first call
- Percentage of incidents Handled within agreed response time
- Number of Incidents broken down by Priority and category
- Number of Incidents escalated by service desk
- Number of incidents re-opened
- Number of Incidents by Passing service desk
- Number of Incidents Incorrectly escalated

Incident management Roles and Responsibilities

- **Incident Manager**
  - driving the efficiency and effectiveness of the Incident Management process
    - -producing management information
    - -managing the work of Incident support staff (first-and second-line)
    - - monitoring the effectiveness of Incident Management and making recommendations for improvement
    - - developing and maintaining the Incident Management systems.
- **Incident Analyst (first Line)**
  - Incident registration
    - -routing service requests to support groups when Incidents are not closed
    - -initial support and classification
    - -ownership, monitoring, tracking and communication
    - -resolution and recovery of Incidents not assigned to second-line support
    - -closure of Incidents

Incident management Roles and Responsibilities

- **Incident Analyst (second line)**
  - -Handling service requests
  - -monitoring Incident details, including the Configuration Items affected
  - -Incident investigation and diagnosis (including resolution where possible)
  - -detection of possible Problems and the assignment of them to the Problem -Management team for them to raise Problem records
  - - the resolution and recovery of assigned Incidents.

- **Subject Matter expert**
  - -Analyzes incidents to identify service restoration actions to be taken
  - -Takes Incident resolution actions to restore services to customers
  - -Assists incident management staff with identifying the impact of the incidents

Key Relationships

- Problem Management
- Configuration Management
- Change Management
- Service level Management
- Availability Management
- Capacity Management

Tool requirements

- Tool for incident logging and recording
- Automatic Escalation Facilities
- Automatic extraction of Configuration data from CMDB
- ACD systems for automatically registering names and phone Numbers of users

Incident Management Summary:

- The goal of incident management is to restore normal service operation, within Service Level Agreement limits, as quickly as possible, after an incident has occurred to that service, and to minimize the adverse impact on business operations.
- Incident Management process Activities
  - Incident detection and recording
  - Classification and initial support
  - Investigation and diagnosis
  - Resolution and recovery
  - Incident closure
- Prioritization primarily determined by impact on business and urgency with which a resolution or workaround is needed; correct prioritization enables optimum staffing and use of other resources to customer satisfaction.
- Escalation (functional and hierarchical)

Log Management

REDTEAM®
HACKER ACADEMY

What is Log Management?

Log management comprises an approach to dealing with large volumes of computer-generated log messages. Log management generally covers: Log collection Centralized log aggregation Long-term log storage and retention Log rotation Log analysis Log search and reporting.

WHAT ARE LOG?

REDTEAM®
HACKER ACADEMY

What Logs?

- Audit logs
- Transaction logs
- Intrusion logs
- Connection logs
- System performance records
- User activity logs
- Various alerts and other messages

From Where?

- Firewalls/intrusion prevention
- Routers/switches
- Intrusion detection
- Servers, desktops, mainframes
- Business applications
- Databases
- Anti-virus
- VPNs

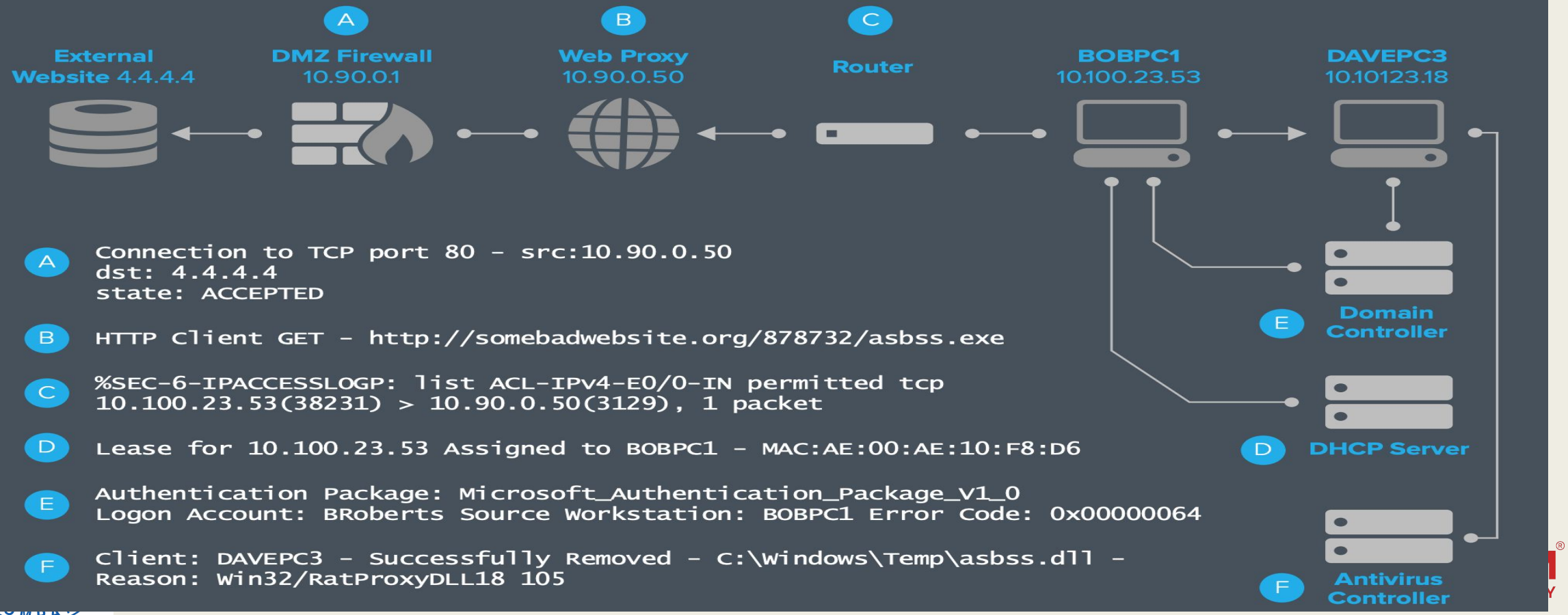
LOGS HAVE CHAOS

- NO STANDARD SCHEMA
- NO STANDARD TRANSPORT MECHANISM
- NO STANDARD MEANING

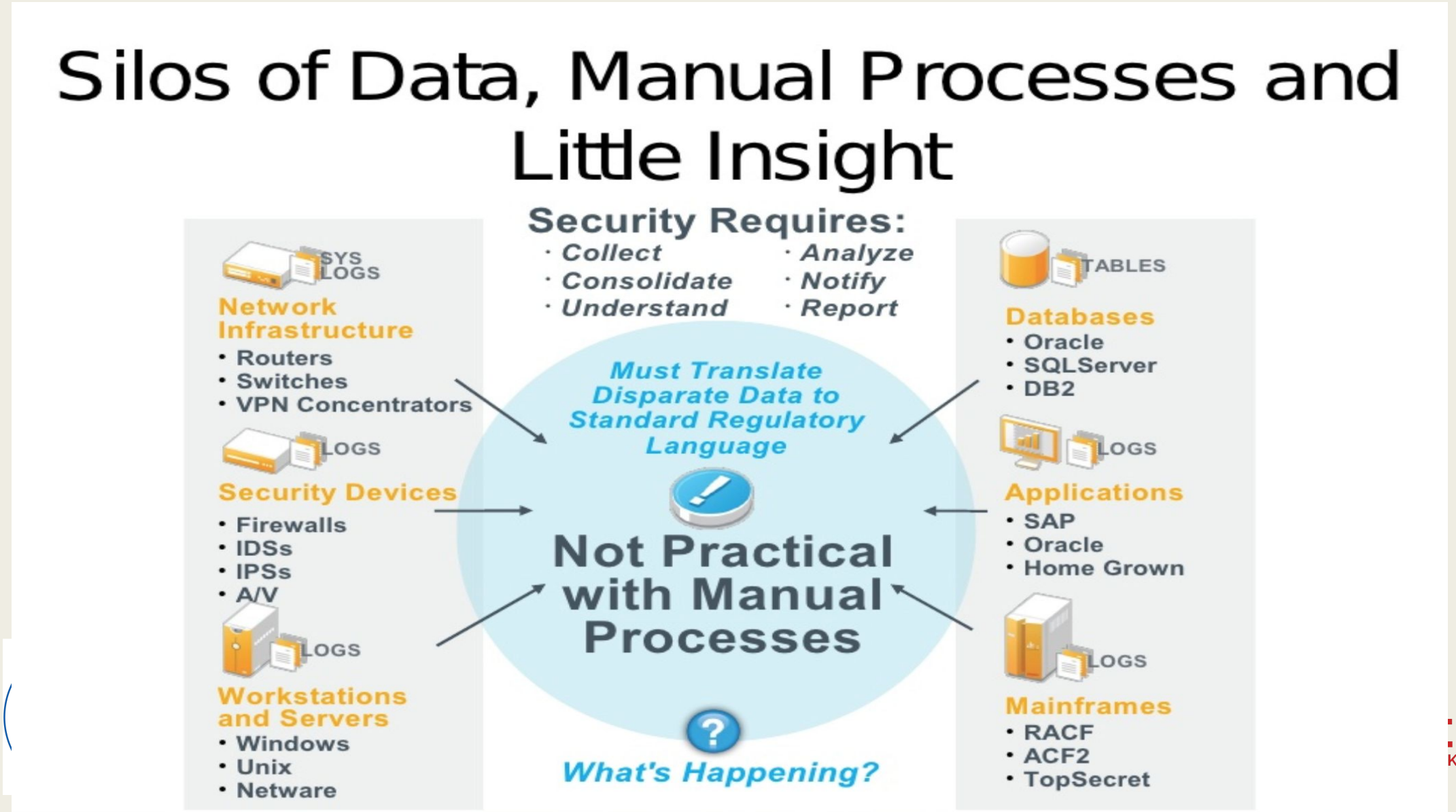
UNDERSTANDING LOGS IN AN ACTIVE ATTACK

Bob's Machine was compromised by asbss.exe which originated from a malicious website, this malware then used Bob's account to try and infect DAVEPC3, but antivirus caught it. Bob's machine "BOBPC1" is likely still compromised, however.

We should block the malicious domain and sanitize Bob's workspace, ASAP



How Log Management Helps



Basic Log Management Functions

- **Collecting** logs from various network devices, security applications, and business applications
- **Storing** these logs for some defined retention period – ideally at the lowest possible cost
- **Searching** through the stored logs on an ad-hoc basis for forensics, to find anomalies, etc.
- Sending **Reports** to analysts, managers, etc. at periodic intervals to fulfill operational or regulatory requirements

What's In a Log?

- Certain activities that take place on a system generate an event or log file
  - Successful and failed login
  - Ports open/close
  - Privelege Escalation
- Syslog is a standard for taking these log files and streaming them to a central location
  - Wikipedia - "Syslog ... allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate, a means to notify administrators of problems or performance."
- If syslog is just a stream of information – how to make it useful?
  - Not much provided by default
  - Can save syslog to a file, grep through it – a completely manual effort

Using Log Management for Prevention

- Log management provides the transparency required to discover potential threats and vulnerabilities
  - Requires a certain amount of diligence
- Use log management to discover
  - If devices or software are misconfigured
  - Who is accessing data or files
  - Who is changing configurations
  - Who has access to sensitive data and systems (and then go and limit those with access where possible)
  - Whether administrators are sharing passwords or abusing privileged access

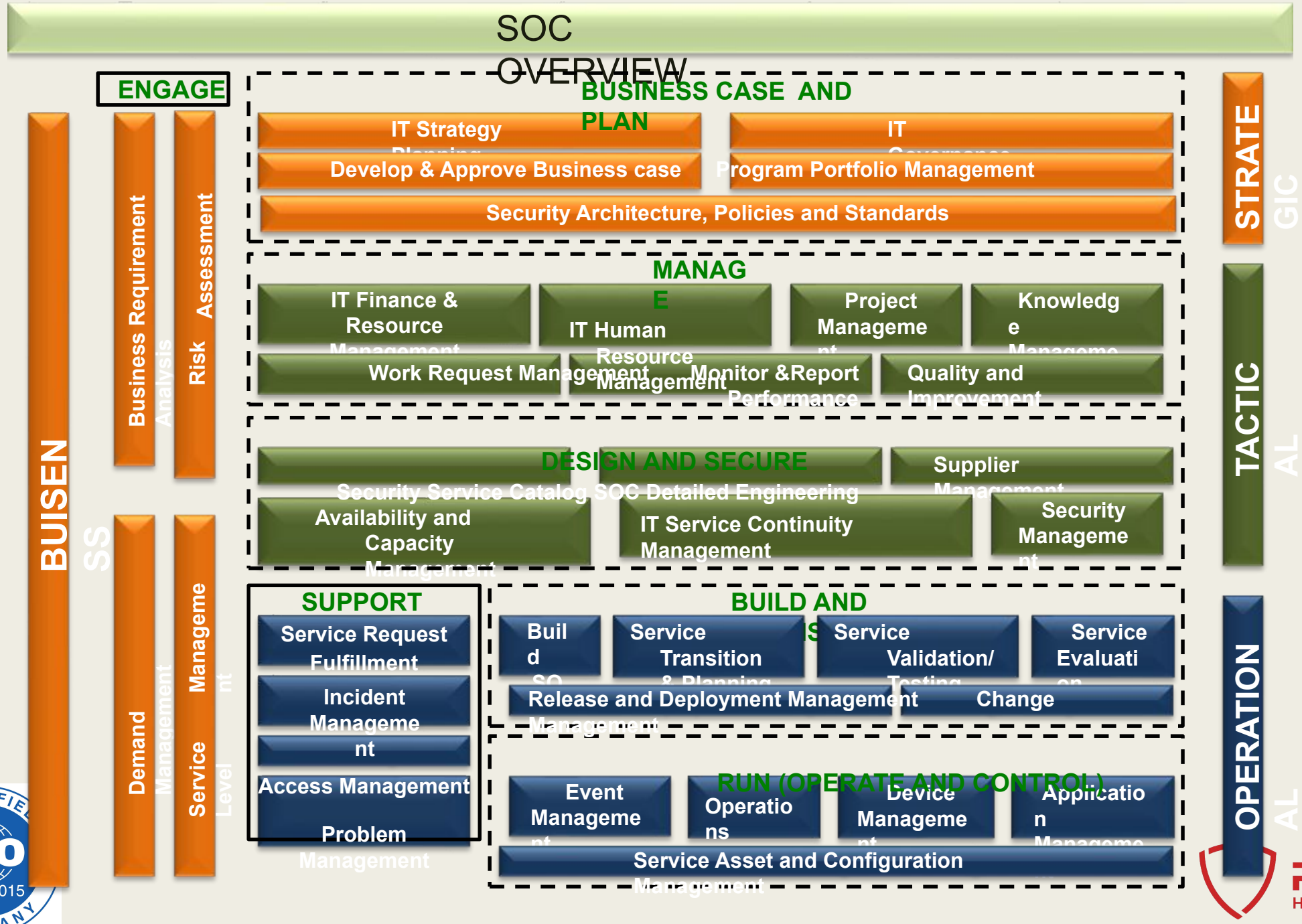
Using Log Management for Detection

- Log management can help determine whether a breach event has occured
  - Knowing that you've been breached is often extremely difficult
- Diligent log management tell you
  - If a new user was unexpectedly created
  - Who has elevated permissions
  - If the volume of attacks increases
  - If a vulnerable system was targeted with an exploit
  - Whether a configuration was tampered with

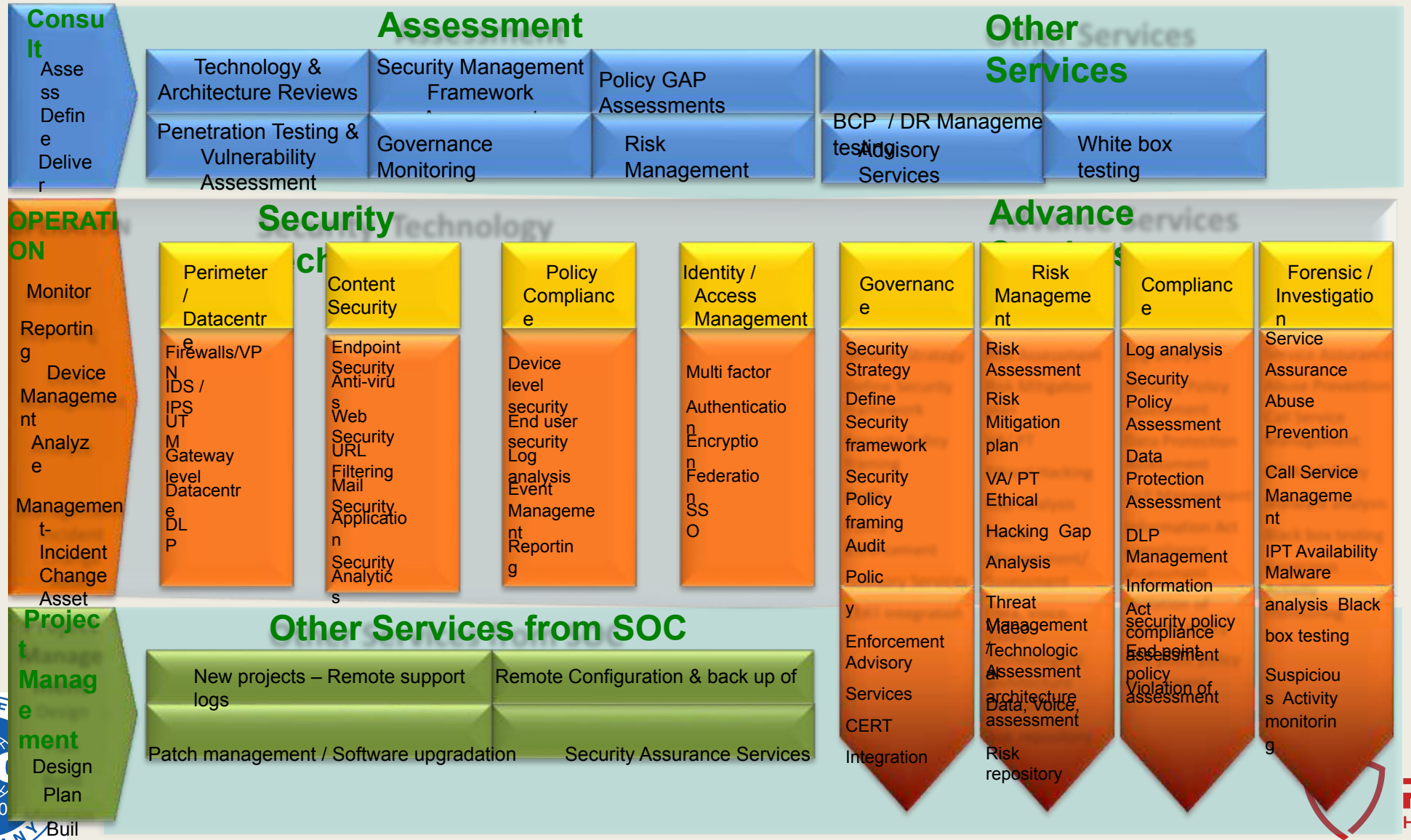
Using Log Management for Investigation

- Event logs are the most critical footprints within the enterprise to reconstruct an actual breach
  - Log Management provides visibility across all your IT infrastructure
  - Allows root cause analysis
- Use log management to determine what happened and how it happened to remediate or mitigate:
  - Which systems and applications were compromised
  - The attack vector that was used
  - Which security systems failed
  - If the attack was detected but not acted on

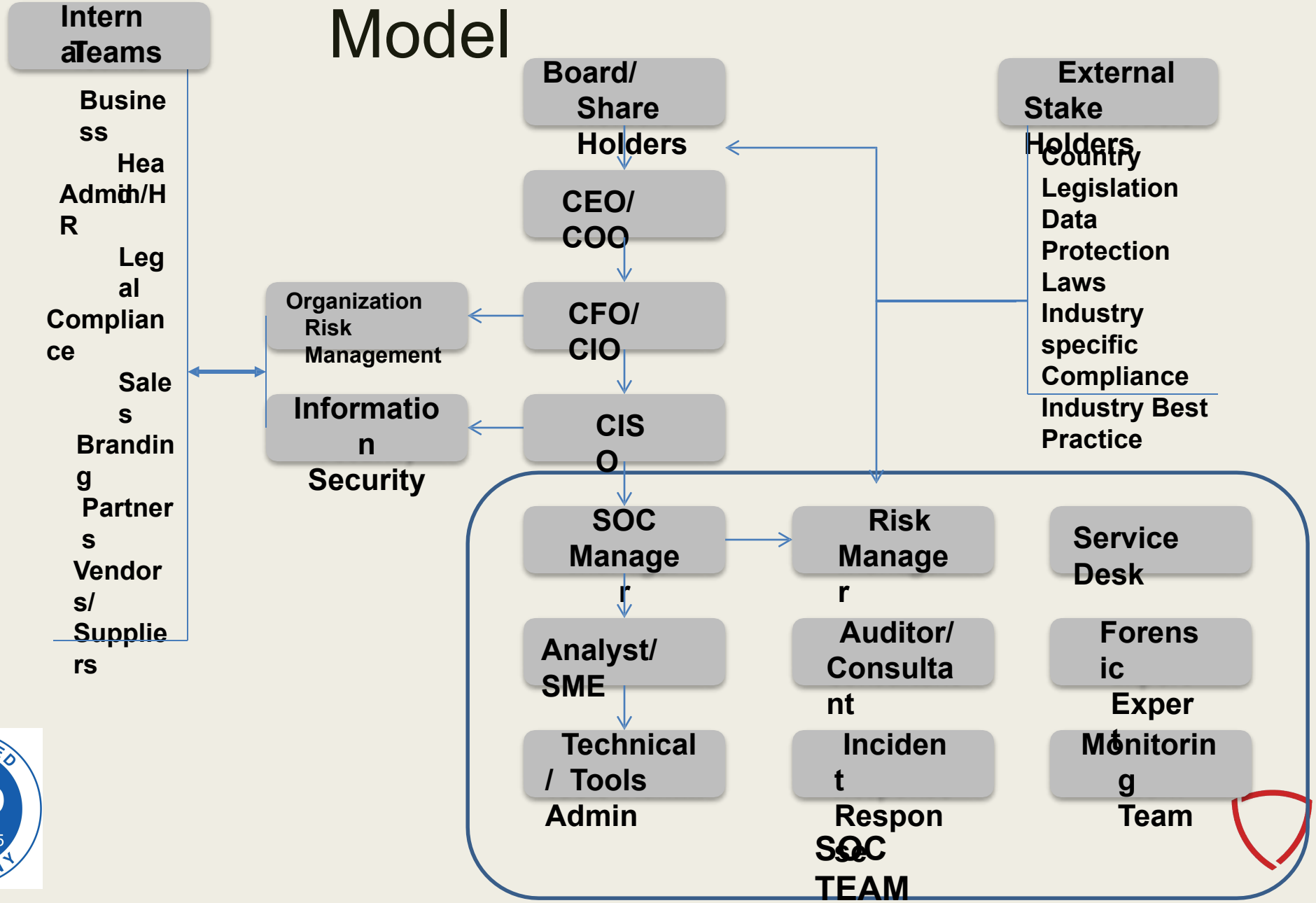
SOC OVERVIEW



Services inside a SOC



SOC Governance Model



SOC PEOPLE

Analyst

- Expert of Security Technology and process
- Understand attacks and threat matrix
- Good at low level programming language
- Extremely good at reaching to root cause
- Think out of box
- Understand Virus, Trojans, backdoor, malicious code
- Drive people
- Proactive by nature

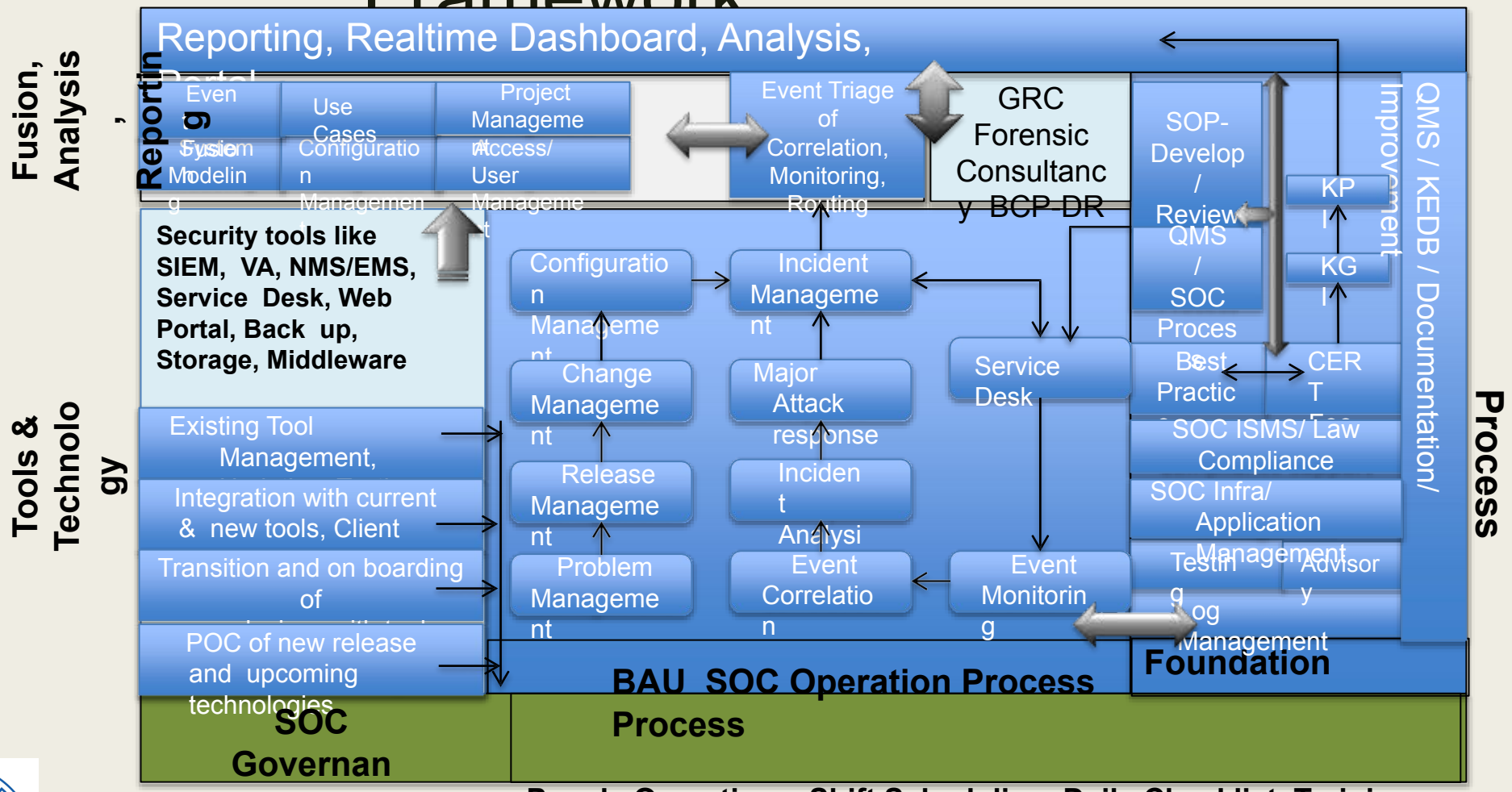
Tech admins

- Expert of Security, OS, Network, Web technology, Database
- Configure tools and security technologies
- Great at low level designing
- Frame and implement security policies in technologies under SOC
- Forensic expert
- Quick at Incident response
- Can interact and drive vendors, OEM, Government bodies

Management

- Leadership to take all stakeholders together
- Stitch the solutions from different teams and drive it to conclusion
- Understand security posture and able to guide the team
- Good communication skills

SOC Process Framework



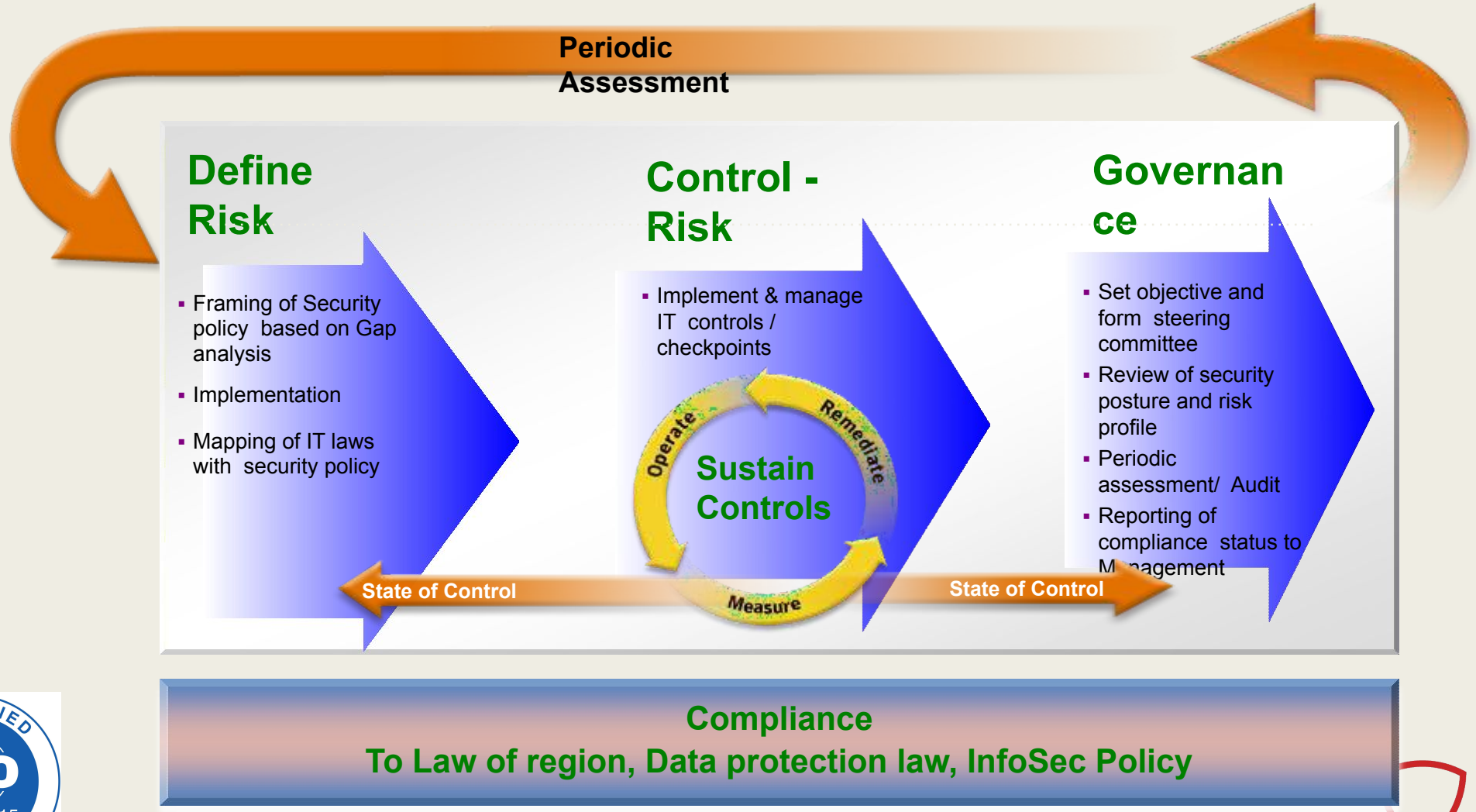
SOC Process

Number of processes and procedures for an SOC is determined by its scope, how many services are offered, the number of customers supported, and the number of different technologies in use. An established global SOC environment may have tens or even hundreds of procedures. At a minimum, the basic procedures that are required for maintaining the SOC are:

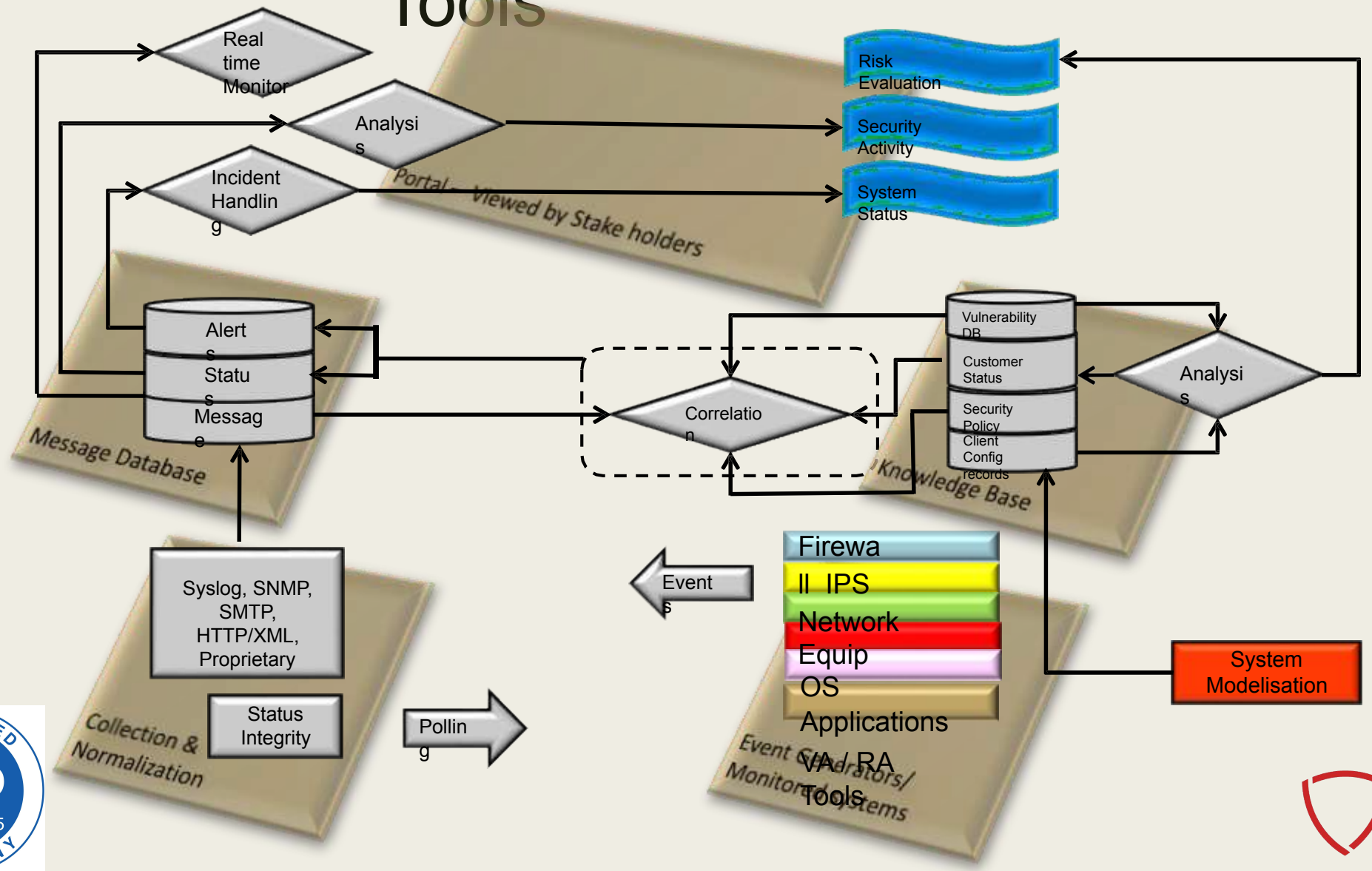
- Monitoring procedure
- Notification procedure (email, mobile, home,
- chat, etc.) Notification and escalation
- processes
- Transition of daily SOC
- services Shift logging
- procedures Incident
- logging procedures
- Compliance monitoring
- procedure Report
- development procedure
- Dashboard monitoring and logging
- procedures
- Network and host IDS/IPS monitoring and
- logging procedures
- Network and host DLP monitoring and
- logging procedures
- Centralized logging platforms
- (syslog, etc.)
- Email and spam gateway and
- filtering Web gateway and
- filtering
- Threat monitoring and
- intelligence Firewall monitoring
- and management
- Application whitelisting or file integrity

SIEM monitoring and correlation rules

GR
C



Working of SOC Tools



Key Tools for SOC

Tools Integration