Build your first SOC

SOC aka CSOC = Cyber Security Operations Center

@seb@ioc.exchange | NolaCon 2022

Disclaimer

> This presentation focuses on the basics of a SOC – There is much, much more to know about running highly effective SOCs. The goal is to get you started.

> There is no one size fits all SOC, so results may vary.

> Industry uses many different interpretations of terms used within this presentation – It is always good to confirm meaning.

Presentation is intended for educational purposes only and does not replace independent professional judgment. Statements of fact and opinions expressed are those of the participants individually and, unless expressly stated to the contrary, are not the opinion or position of my employer. The speaker does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented. Attendees should note that sessions are audio-recorded and may be published in various media, including print, audio and video formats without further notice.

Why do we need a SOC?

TLDR: Because you need to sleep and have vacation ;-)

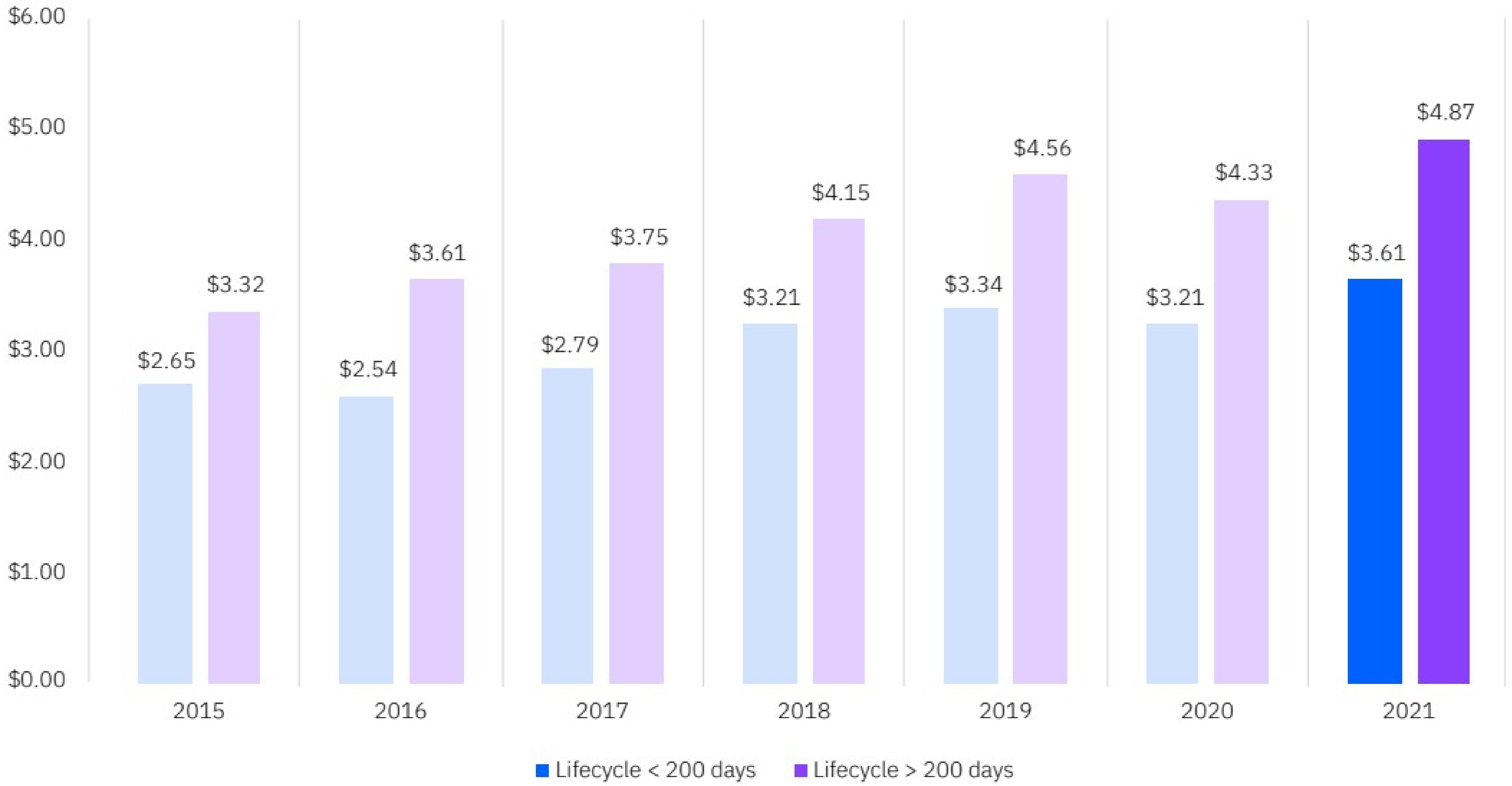
HELP

If you have not had an offline vacation for more than 12 months, you will fail to protect the organization very soon.

If you are the only one, who knows how to investigate alerts, your organization’s data and operations are at risk.

Average total cost of a data breach based on average data breach lifecycle

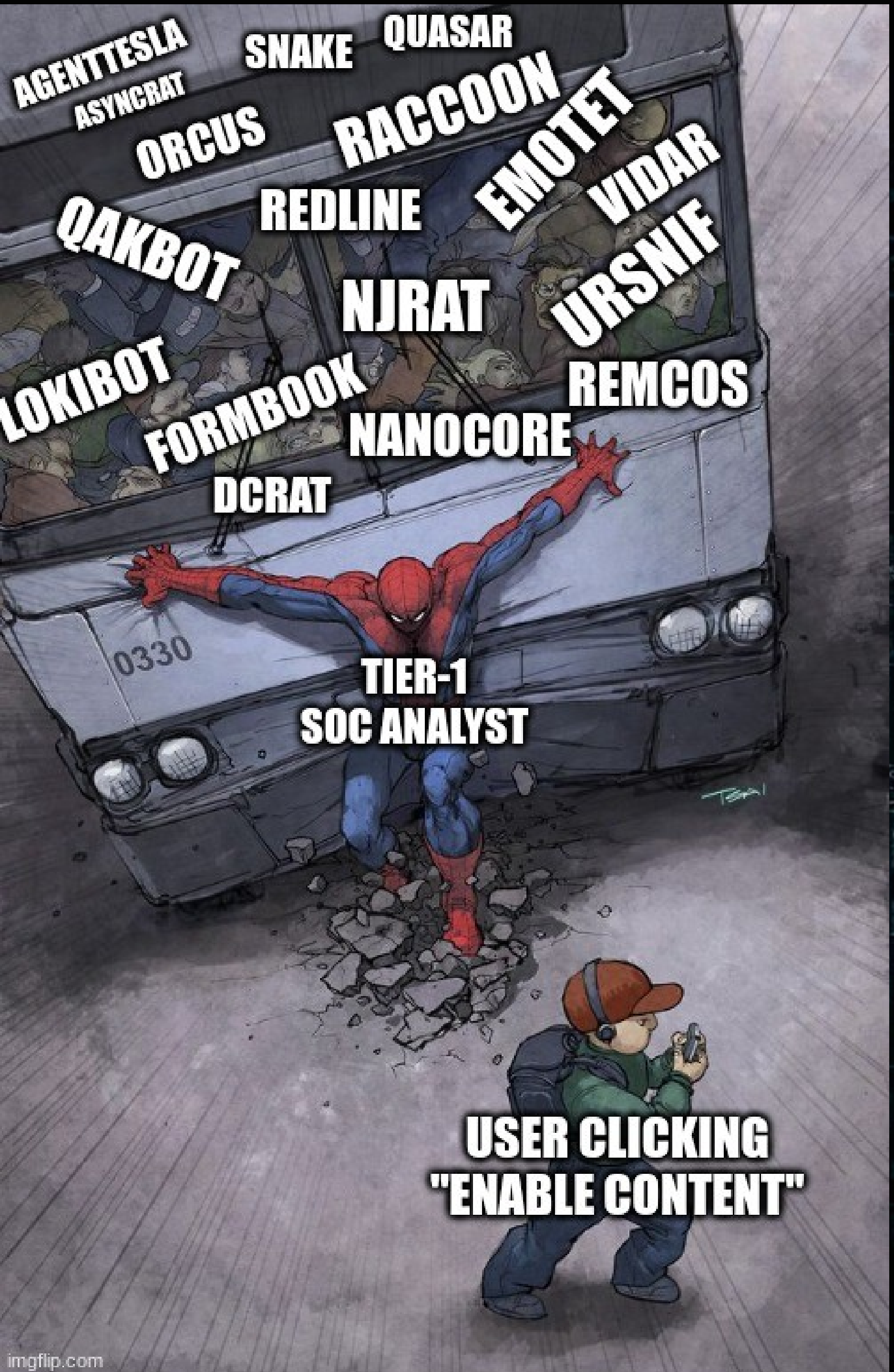
Measured in US$ millions



Cost of Data Breach Report 2021 (IBM Security)
https://www.ibm.com/security/data-breach

What does a SOC do?

TLDR: Detection & Response

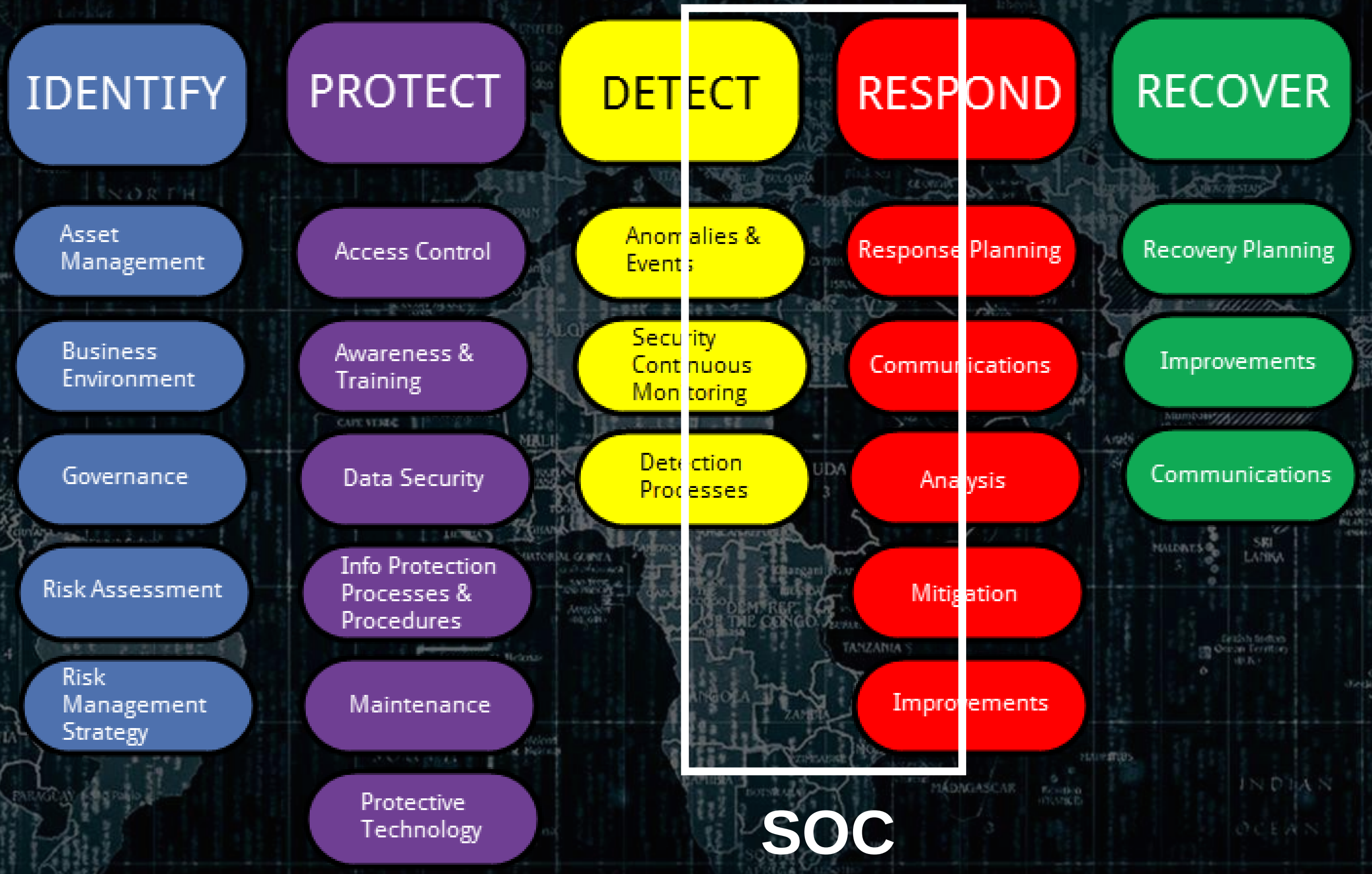


SOC analysts investigate security alerts and take response actions with the goal to **Contain** and **Eradicate** the **Threat**.

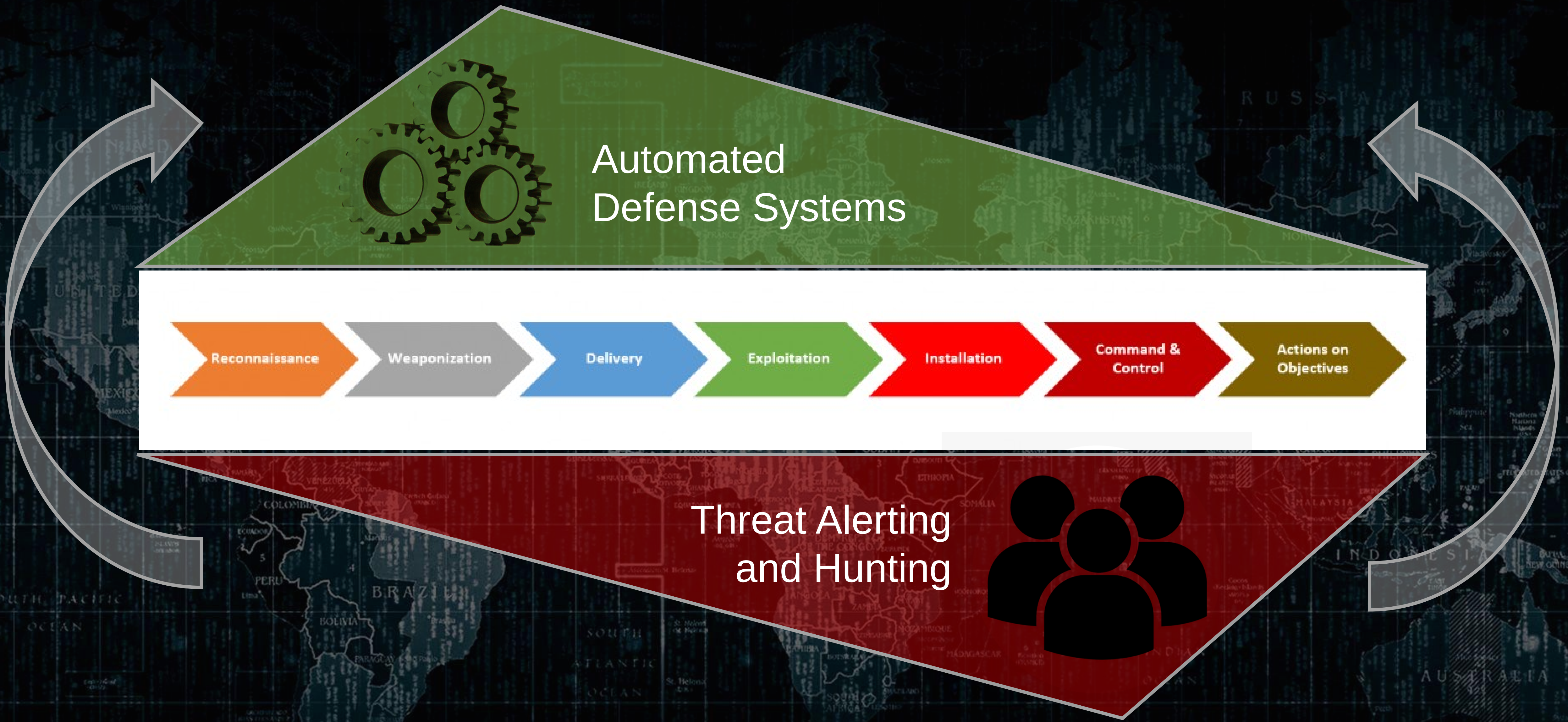
Ideally threat is contained before it impacts the organizations ability to fulfill its mission.

When the SOC cannot contain the malicious activity, it escalates the case to an Incident Response team.

NIST CyberSecurity Framework



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			



Automated Defense Systems

Reconnaissance

Weaponization

Delivery

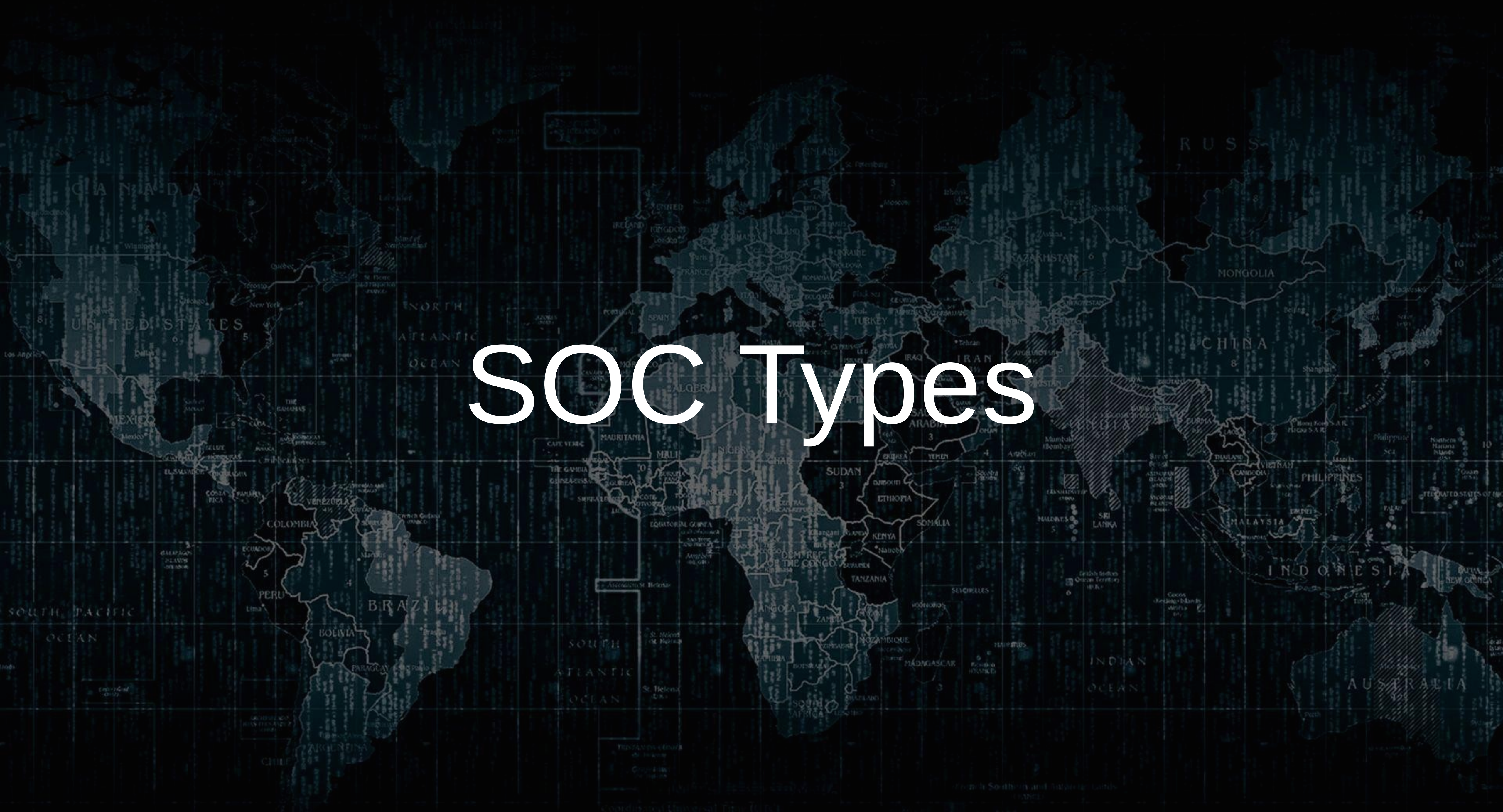
Exploitation

Installation

Command & Control

Actions on Objectives

Threat Alerting and Hunting



SOC Types

MDR vs SOC

MDR

- Often limited to the feature set of the EDR/EPP solution
- Always highly standardized
- Usually comes with pro-active threat hunting based on shared CTI
- Very Low management effort required

SOC

- Can make use of all available security Logs and Tools in the environment
- Flexible in terms of process
- Allows more process integration
- Medium to High management effort required

SOCaaS

- Outsourcing of People, Process & Technology
- High Cost for Provider Change due to effort needed to migrate to new provider’s tech stack
- Low Flexibility in terms of Process Change
- Lowest Operating Cost

Hybrid SOC

- People outsourced
- Process co-owned
- Technology in-house
- Easier to change provider, if needed
- Requires Engineering capacity in-house to maintain tech-stack
- Medium Flexibility & Operating Cost

In-house SOC

- Everything is In-house
- Finding and hiring talent is hard
- High Flexibility in terms of Process Change
- Highest Operating Cost (especially if SOC analysts live in high cost geographies)

SOC People

HELP! THERE'S AN ALERT IN QUEUE!
I'M SO TIRED...
SOC ANALYST 1
SOC ANALYST 2
imgflip.com

GENTLEMAN, IT IS WITH GREAT PLEASURE TO INFORM YOU
THAT TODAY I SIGNED MY FIRST JOB AS CYBER SECURITY ANALYST

SOC Manager

Makes sure that SOC Analysts have everything they need.

SOC Analyst L3

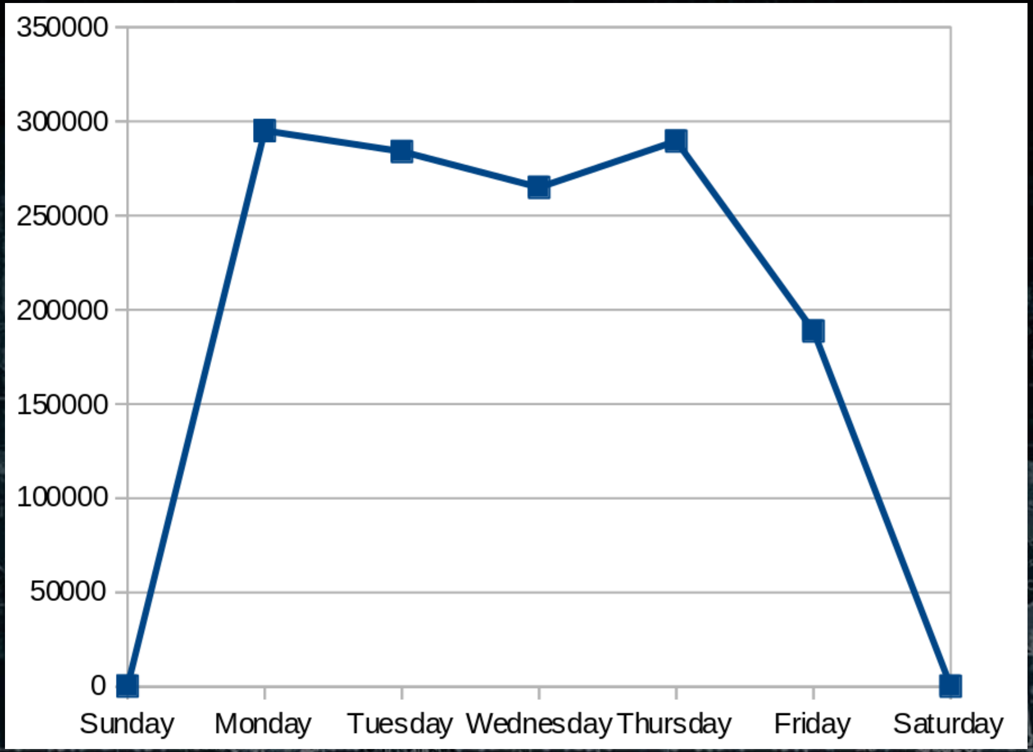
Wise Guy! The dude who has seen it all…

SOC Analyst L2

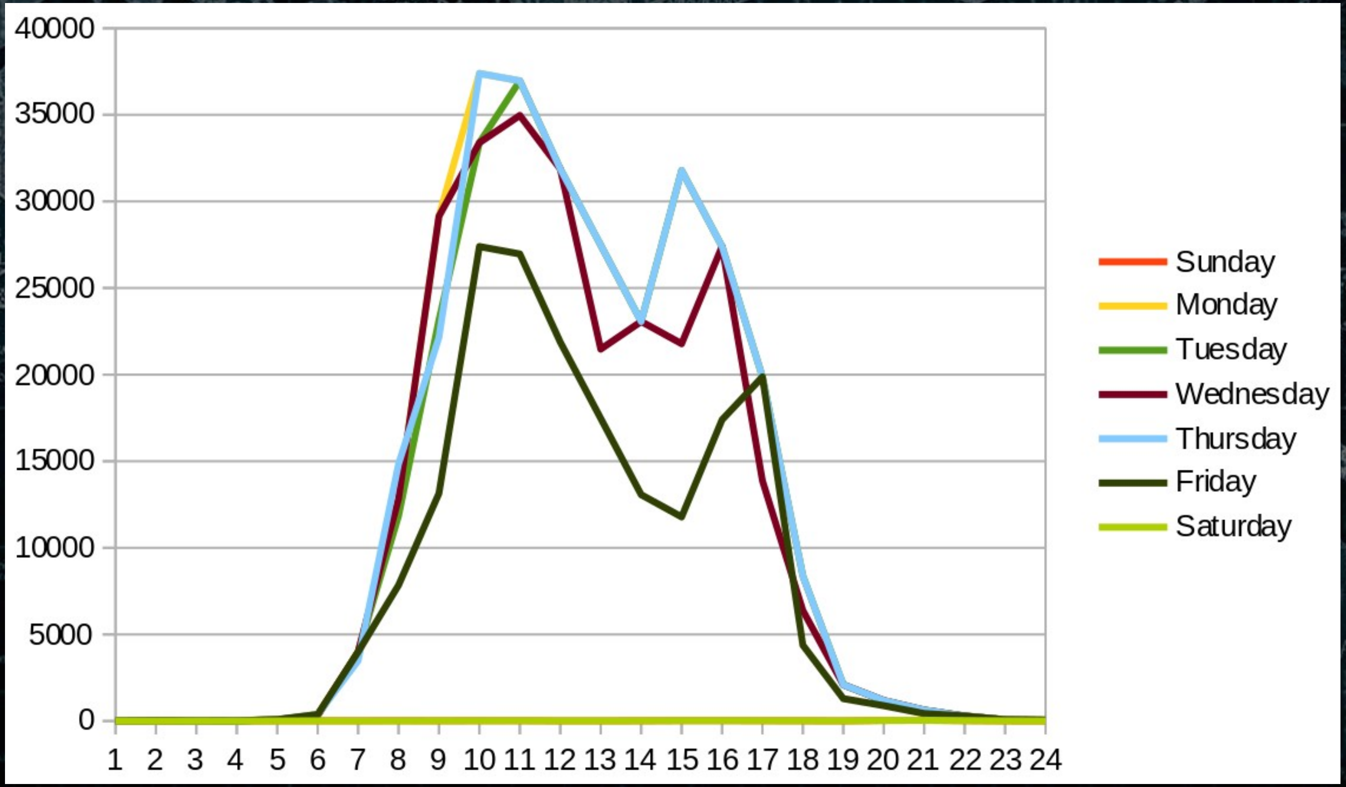
Investigates true positives only and performs Response Actions

SOC Analyst L1

Looks at every incoming alert and decides whether it is worth to be investigated further. (Human False Positive Filter)



Plotting out ALERT VOLUME and/or INCIDENT NUMBERS usually gives an idea about need for investigations and response on different days of the week.



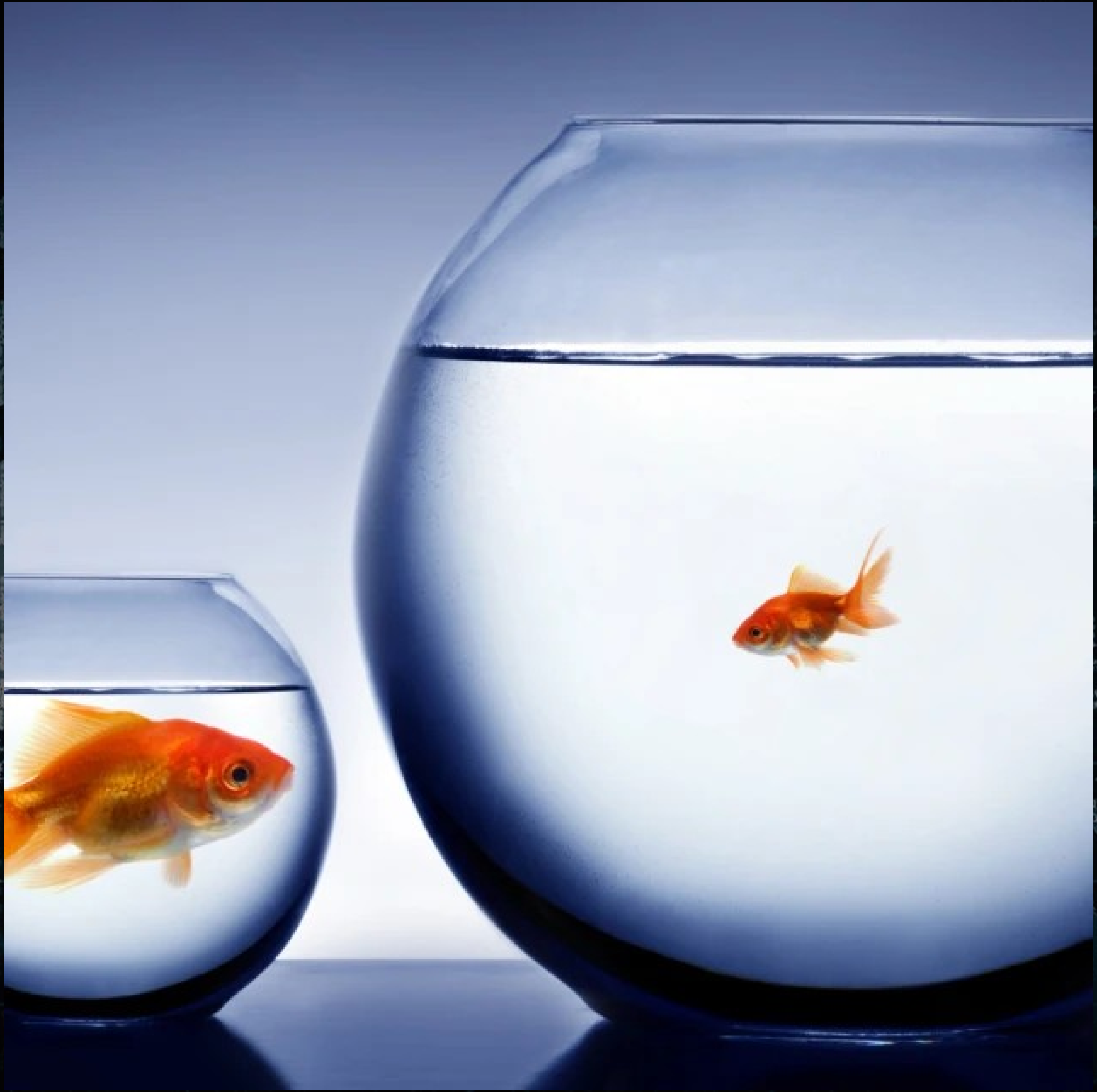
If organization operates in multiple time zones, transform the numbers into the time zone with the most employees.

If your 1st SOC includes provider workers (contractors), choose carefully!

Things to look at:

1. Size of the vendor
2. Dedicated vs Shared SOC
3. Time Zones
4. Language/Culture
5. Compliance Requirements

Before you start comparing prices, make sure that the oranges are well defined!

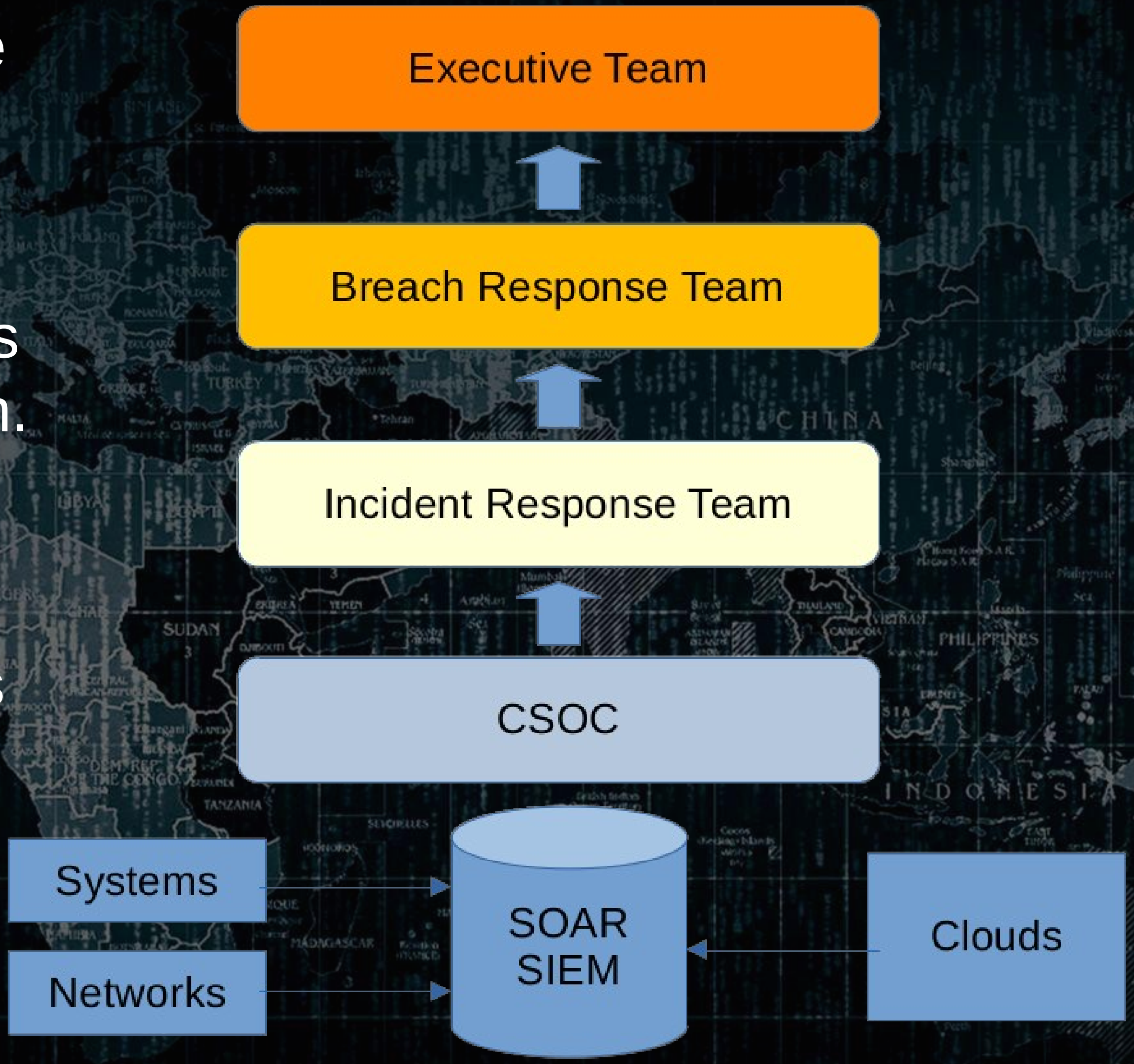


SOC Processes

Breach Response Team deals with the fallout of severe incidents. It includes representatives from Legal, HR, etc.

Incident Response Team (aka CIRT) is the technical team with the widest reach. CIRT executes large scale Response Actions (incl. cutting off the Internet).

In your Incident Response Plan, **SOC** is the beginning of the Escalation Path.

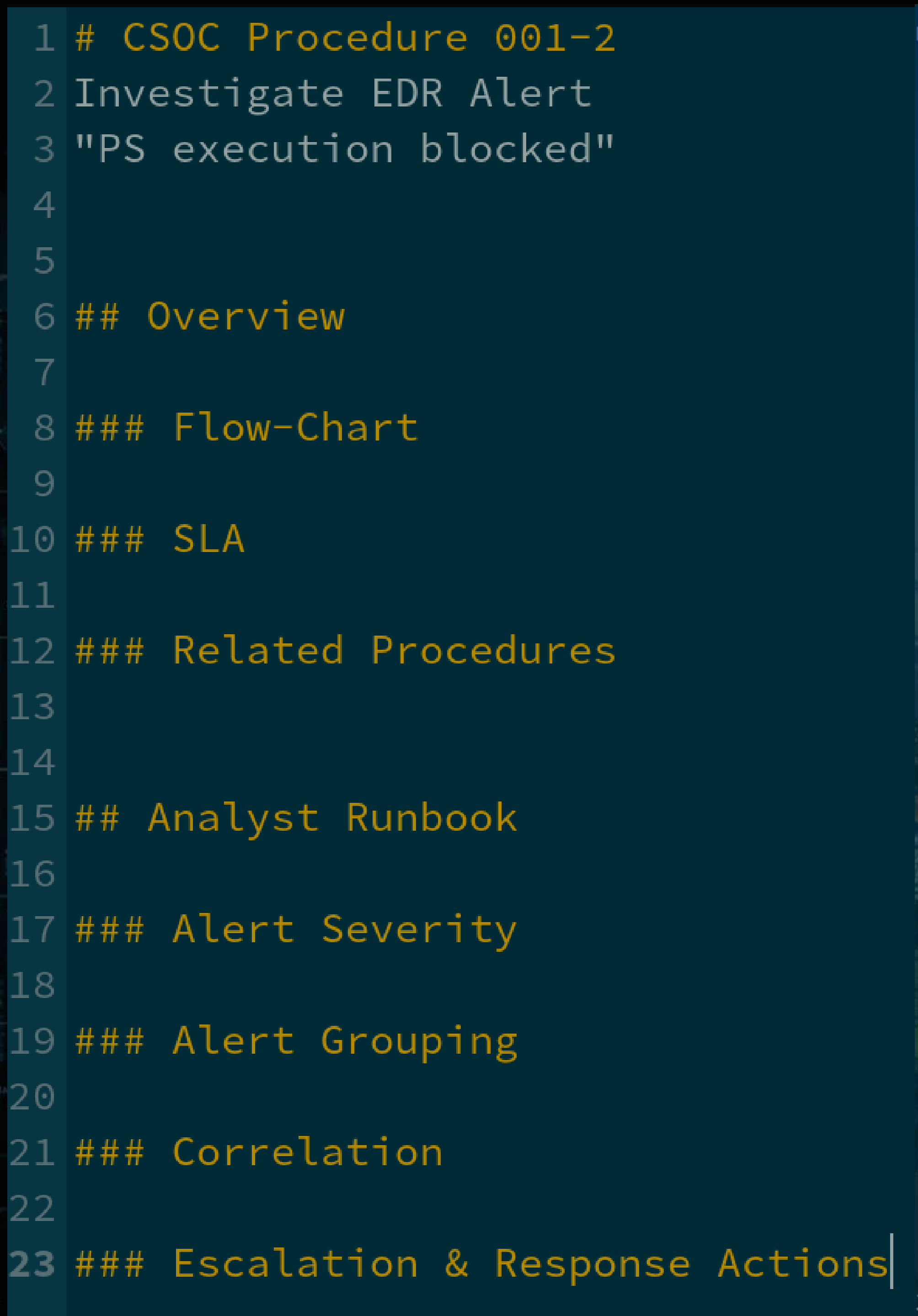


The authority of all SOC team members must be clearly defined!

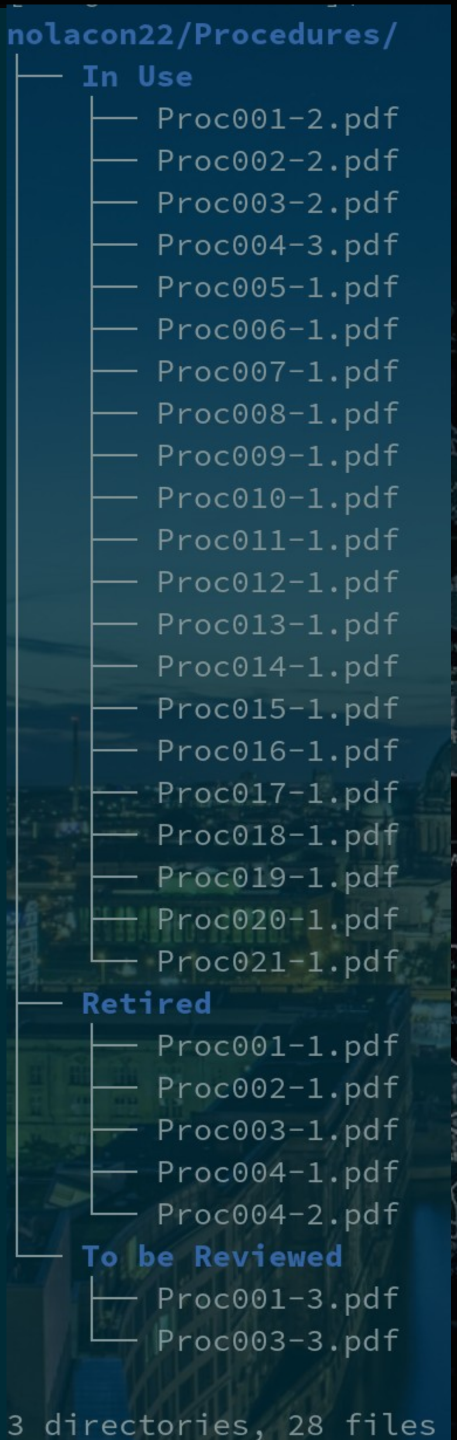
If approval for certain log data access is needed, move that procedure out of the SOC.

DO NOT create SOC Response procedures that include any kind of approval flow!

All Response Actions the SOC is supposed to take, need to be fully authorized.



```
# CSOC Procedure 001-2
Investigate EDR Alert
"PS execution blocked"


## Overview

### Flow-Chart

### SLA

### Related Procedures


## Analyst Runbook

### Alert Severity

### Alert Grouping

### Correlation

### Escalation & Response Actions
```



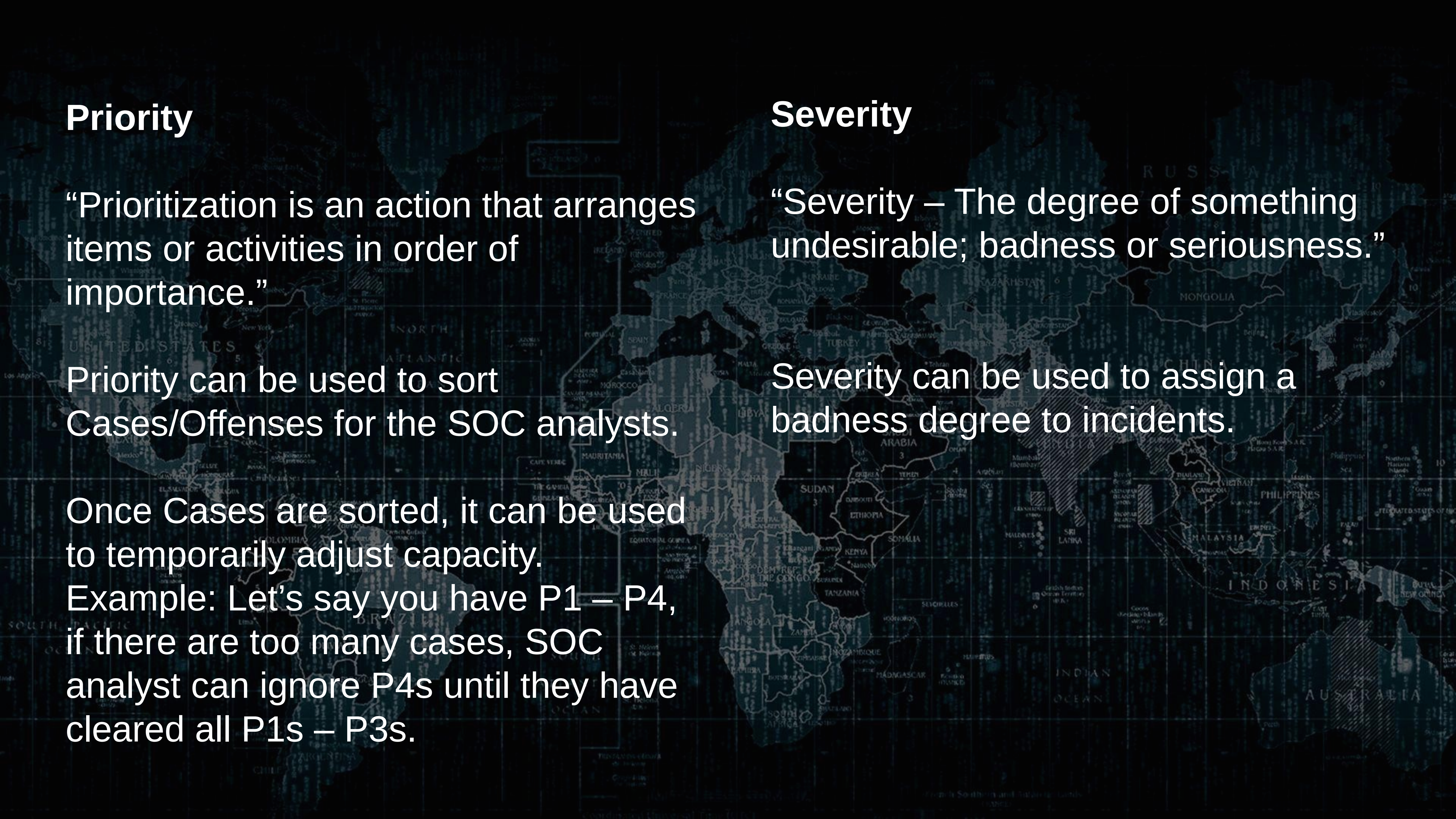
```
nolacon22/Procedures/
├── In Use
│   ├── Proc001-2.pdf
│   ├── Proc002-2.pdf
│   ├── Proc003-2.pdf
│   ├── Proc004-3.pdf
│   ├── Proc005-1.pdf
│   ├── Proc006-1.pdf
│   ├── Proc007-1.pdf
│   ├── Proc008-1.pdf
│   ├── Proc009-1.pdf
│   ├── Proc010-1.pdf
│   ├── Proc011-1.pdf
│   ├── Proc012-1.pdf
│   ├── Proc013-1.pdf
│   ├── Proc014-1.pdf
│   ├── Proc015-1.pdf
│   ├── Proc016-1.pdf
│   ├── Proc017-1.pdf
│   ├── Proc018-1.pdf
│   ├── Proc019-1.pdf
│   ├── Proc020-1.pdf
│   └── Proc021-1.pdf
├── Retired
│   ├── Proc001-1.pdf
│   ├── Proc002-1.pdf
│   ├── Proc003-1.pdf
│   ├── Proc004-1.pdf
│   └── Proc004-2.pdf
└── To be Reviewed
    ├── Proc001-3.pdf
    └── Proc003-3.pdf

3 directories, 28 files
```

USE CASE MANAGEMENT

Procedures should all have the same structure, so they are easy to digest/navigate.

There needs to be an Approval process that puts procedures into production or retires them.

A matrix (large spreadsheet) is recommended to organize all procedures. Procedures could be organized by Business Problem, Detection Tool, Response Tool, MITRE Att@ck...



Priority

“Prioritization is an action that arranges items or activities in order of importance.”

Priority can be used to sort Cases/Offenses for the SOC analysts.

Once Cases are sorted, it can be used to temporarily adjust capacity.
Example: Let’s say you have P1 – P4, if there are too many cases, SOC analyst can ignore P4s until they have cleared all P1s – P3s.

Severity

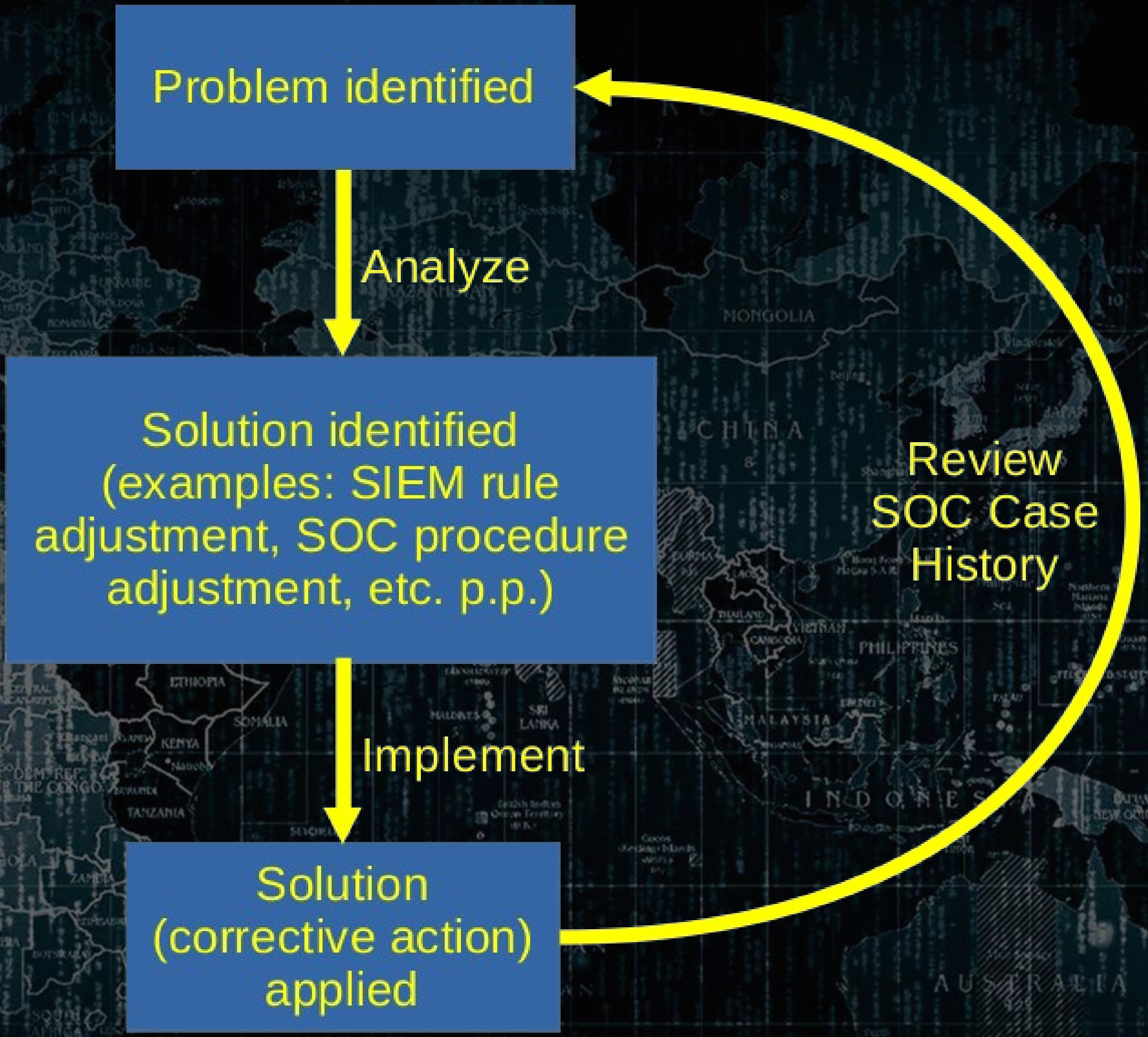
“Severity – The degree of something undesirable; badness or seriousness.”

Severity can be used to assign a badness degree to incidents.

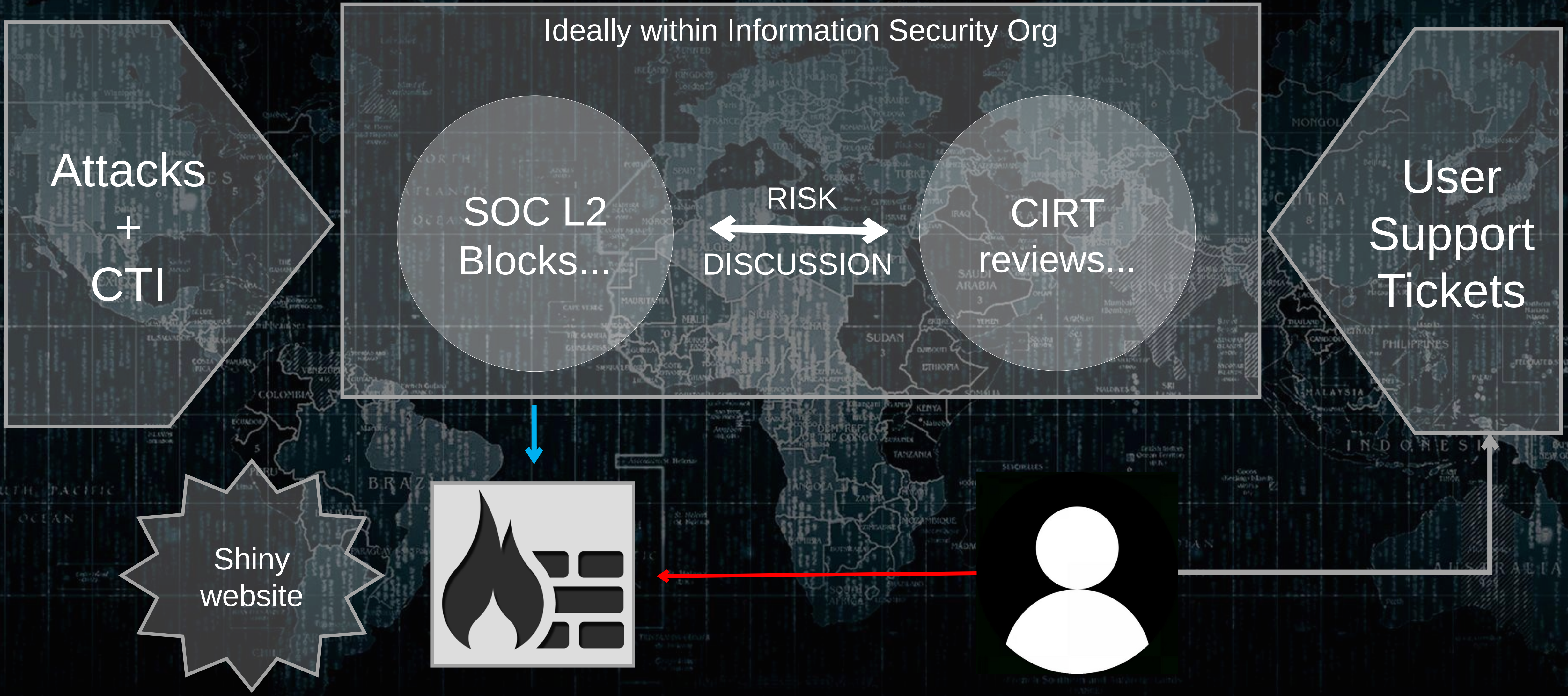
Quality Control (QC)
Continuous Improvement Process

Things go wrong sometimes, so you need a process to ensure that the SOC does not repeat mistakes.

False Negatives are an example for a thing that went wrong – Once the Root Cause Analysis succeeded, the QC process produces corrective actions that eliminate the root cause for the foreseeable future.


Problem identified
Analyze
Solution identified (examples: SIEM rule adjustment, SOC procedure adjustment, etc. p.p.)
Implement
Solution (corrective action) applied
Review SOC Case History

Block Dispute Resolution



Attacks + CTI

Ideally within Information Security Org

SOC L2 Blocks...

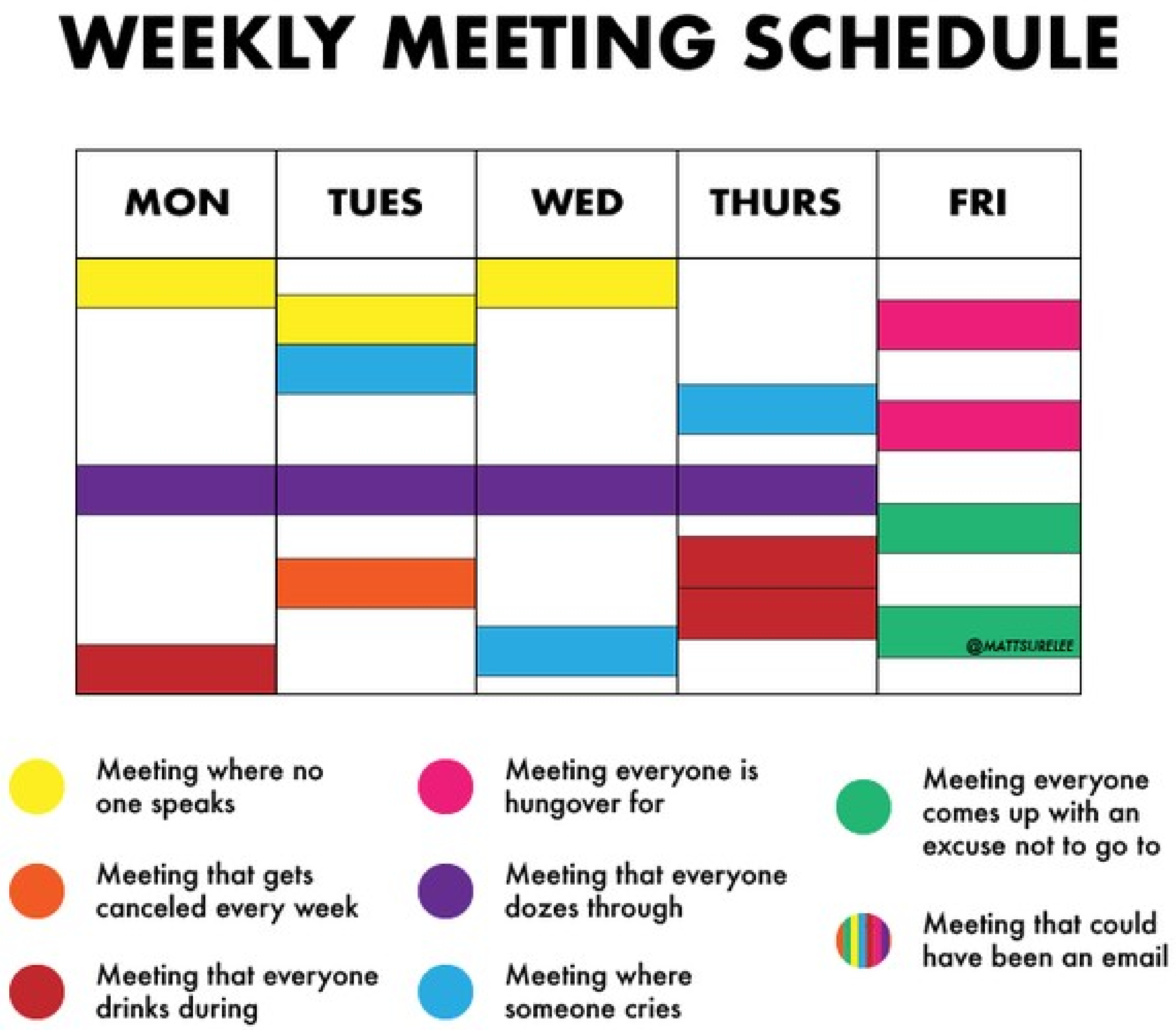
RISK

DISCUSSION

CIRT reviews...

User Support Tickets

Shiny website


WEEKLY MEETING SCHEDULE
MON
TUES
WED
THURS
FRI
@MATTSURELEE
Meeting where no one speaks
Meeting that gets canceled every week
Meeting that everyone drinks during
Meeting everyone is hungover for
Meeting that everyone dozes through
Meeting where someone cries
Meeting everyone comes up with an excuse not to go to
Meeting that could have been an email

Standing Meetings

Weekly CSOC meetings are great to discuss recent escalations and false positive rates. Add engineers to the meeting for conversations about visibility.

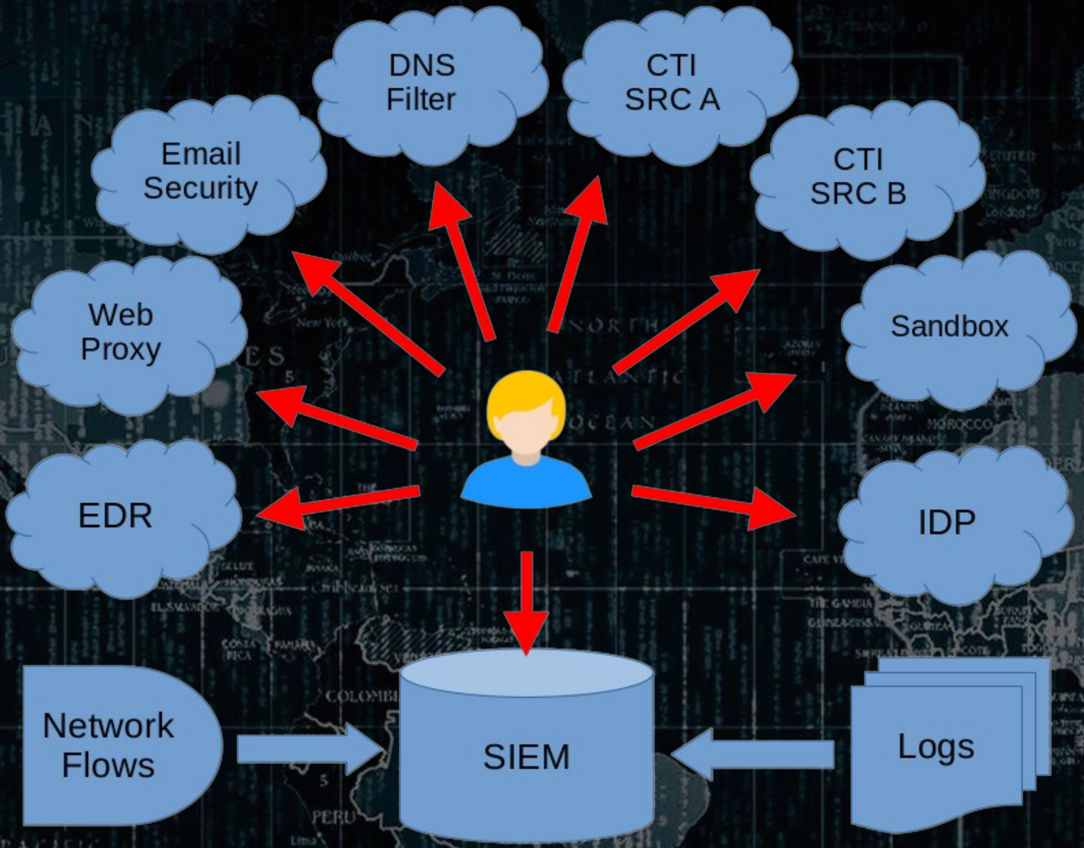
Reporting

Weekly Reports for capacity tracking and immediate threat levels.

Monthly Reports for risk and improvement tracking.

NSOC watch floor circa 1985

SOC Technologies

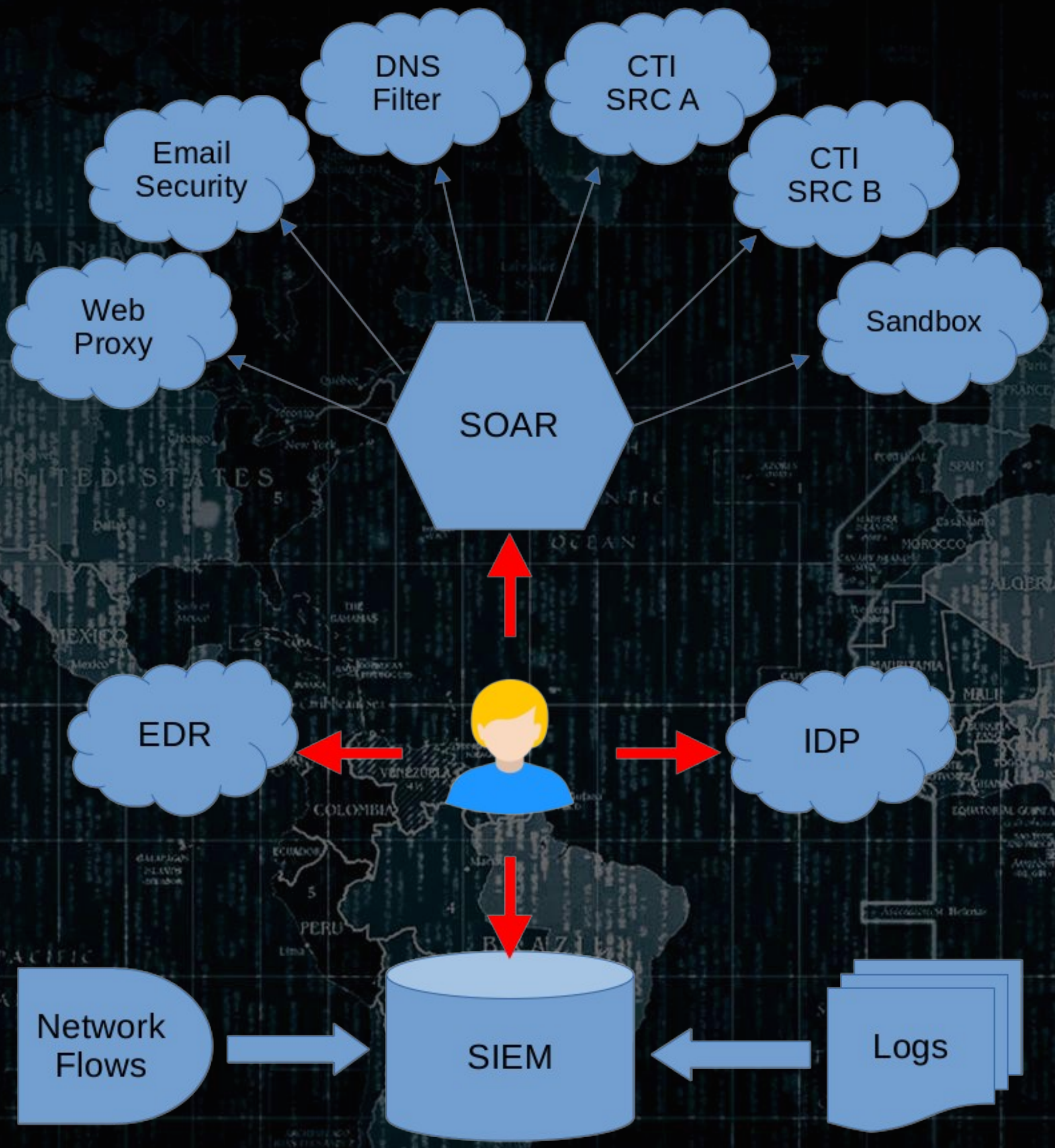


Traditional SIEM based Architecture

SIEM

- Log Aggregation/Correlation
- Data Enrichment
- Alerting
- Incident Management
- Threat Hunting

SOC Analyst quickly get overloaded with interfaces for too many tools.

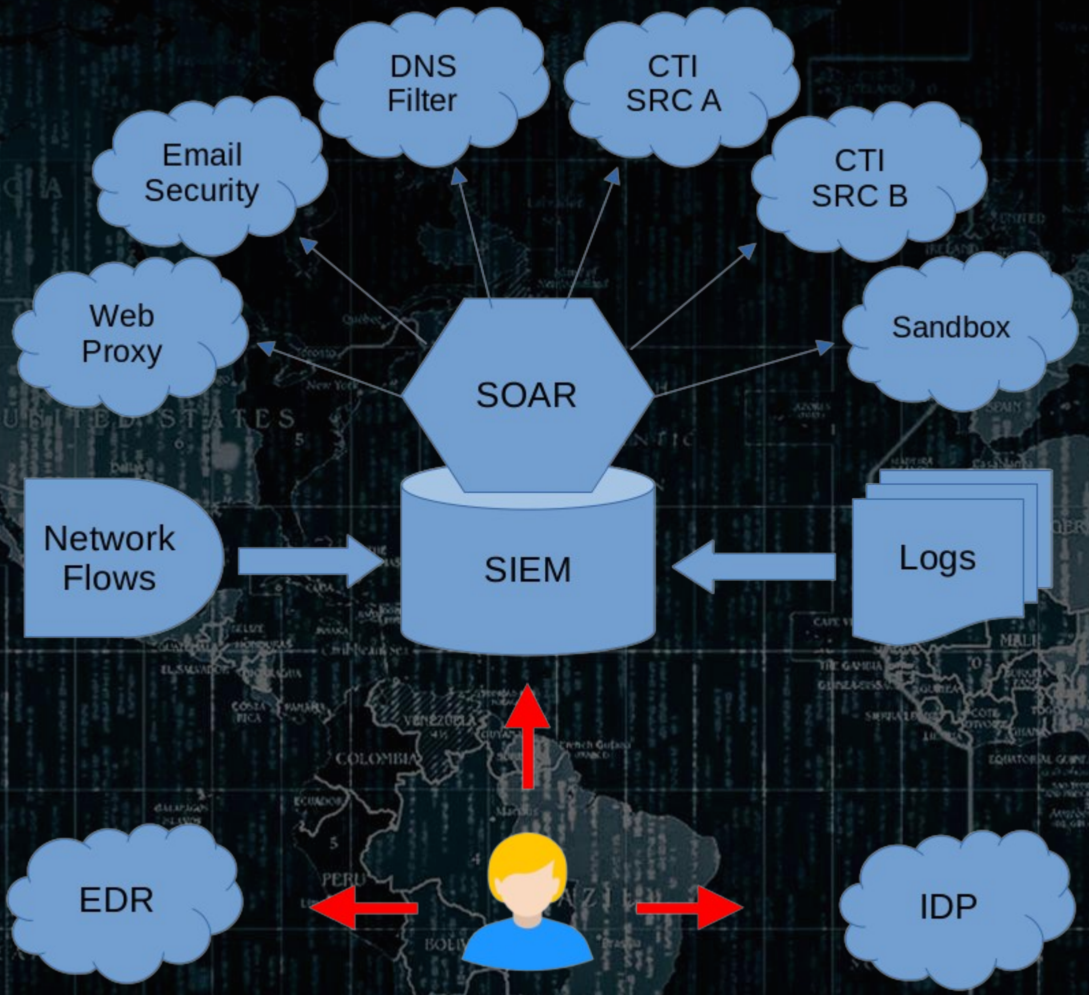


SOAR based Architecture

SOAR
- Incident Management
- Data Enrichment
- Response Automation

SIEM
- Log Aggregation/Correlation
- Alerting
- Threat Hunting

Cyber Tools geared towards specific SOC activities (i.e. EDR) cannot be hidden behind a SOAR.



FUTURE Architecture

SOAR integrated into SIEM
- Incident Management
- Data Enrichment
- Response Automation
- Log Aggregation/Correlation
- Alerting
- Threat Hunting

Multiple vendors are working towards this – Examples are:
- Microsoft Sentinel
- Google Chronicle + Siemplify

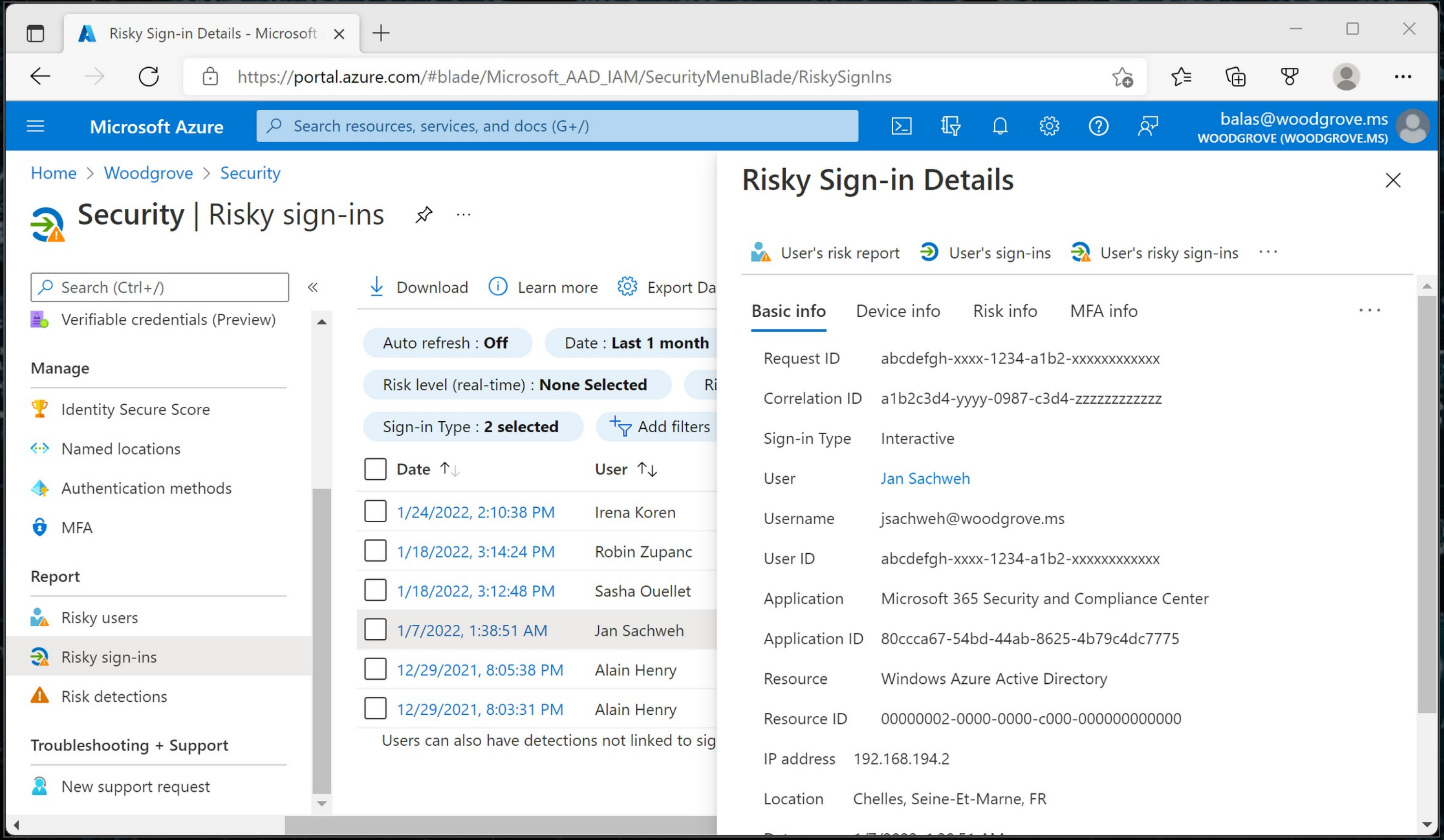
LOG Types – Not all Logs are equally useful!

Consider prioritizing the on-boarding...

Cost: Event vs Netflow

Prio by ROI:

1. IDP (SSO/MFA) Logs
2. Auth Logs in general
3. Email Security Alerts/Logs
4. EDR/EPP Alerts
5. DNS Logs
6. IDS/IPS Logs
7. Host Process Logs
8. WAF Logs
9. ...



Date	User
1/24/2022, 2:10:38 PM	Irena Koren
1/18/2022, 3:14:24 PM	Robin Zupanc
1/18/2022, 3:12:48 PM	Sasha Ouellet
1/7/2022, 1:38:51 AM	Jan Sachweh
12/29/2021, 8:05:38 PM	Alain Henry
12/29/2021, 8:03:31 PM	Alain Henry

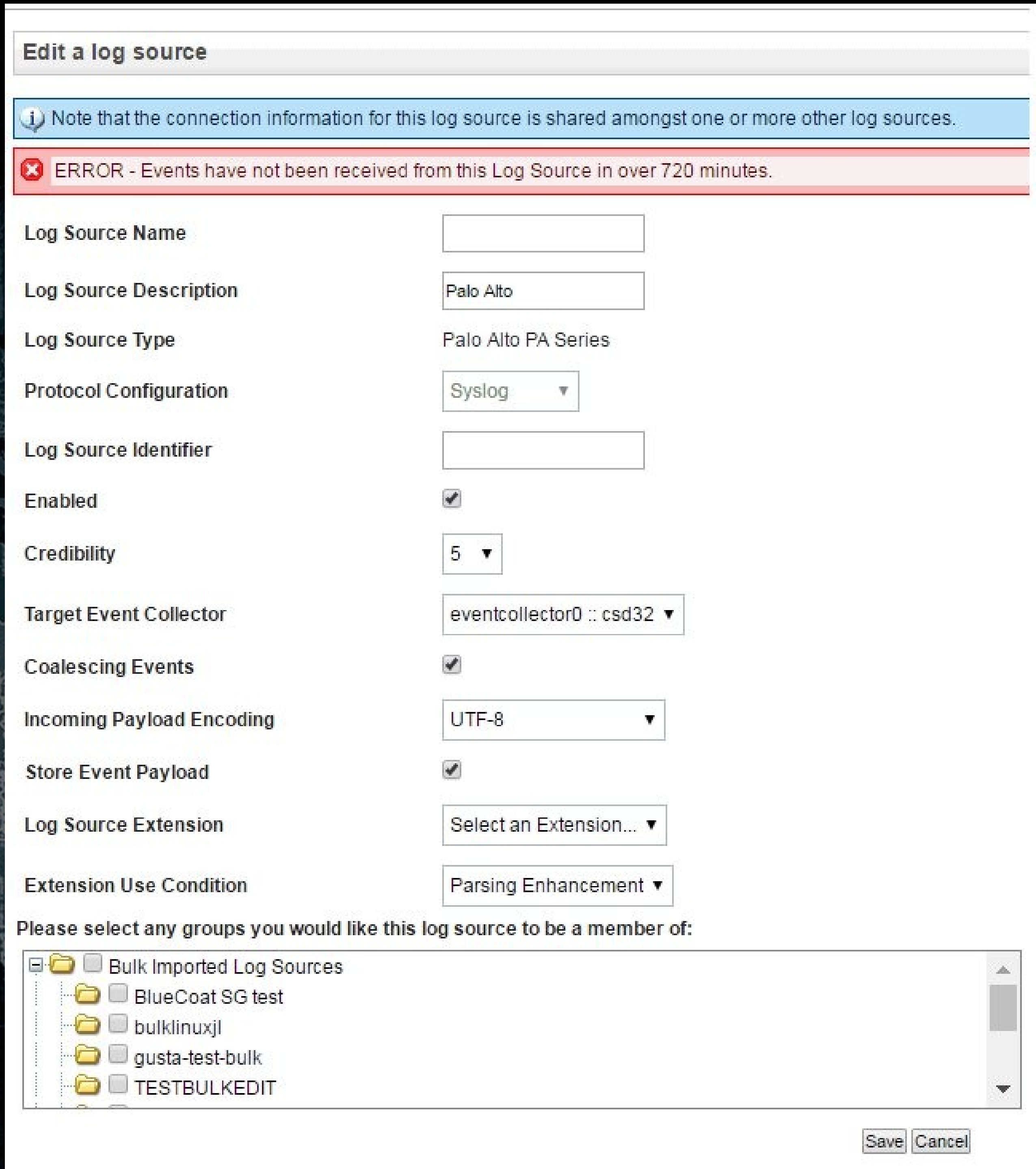
Users can also have detections not linked to sig

Request ID	abcdefgh-xxxx-1234-a1b2-xxxxxxxxxxxx
Correlation ID	a1b2c3d4-yyyy-0987-c3d4-zzzzzzzzzzzz
Sign-in Type	Interactive
User	Jan Sachweh
Username	jsachweh@woodgrove.ms
User ID	abcdefgh-xxxx-1234-a1b2-xxxxxxxxxxxx
Application	Microsoft 365 Security and Compliance Center
Application ID	80ccca67-54bd-44ab-8625-4b79c4dc7775
Resource	Windows Azure Active Directory
Resource ID	00000002-0000-0000-c000-000000000000
IP address	192.168.194.2
Location	Chelles, Seine-Et-Marne, FR

Don’t let your SOC go blind – Monitor your Logs!

> Keep a good inventory of all Log Sources
> Provide Log Source reports to System Owners on a regular basis

A missing Log Source is a high priority engineering event that needs immediate attention!



Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources.

ERROR - Events have not been received from this Log Source in over 720 minutes.

Log Source Name	
Log Source Description	Palo Alto
Log Source Type	Palo Alto PA Series
Protocol Configuration	Syslog ▼
Log Source Identifier	
Enabled	☑
Credibility	5 ▼
Target Event Collector	eventcollector0 :: csd32 ▼
Coalescing Events	☑
Incoming Payload Encoding	UTF-8 ▼
Store Event Payload	☑
Log Source Extension	Select an Extension... ▼
Extension Use Condition	Parsing Enhancement ▼

Please select any groups you would like this log source to be a member of:

- □ Bulk Imported Log Sources
  - □ BlueCoat SG test
  - □ bulklinuxjl
  - □ gusta-test-bulk
  - □ TESTBULKEDIT

User & Entity Behavior Analytics

Uses ML to profile users’ normal behavior, which allows alerting on abnormal behavior. Examples:
> Seb suddenly logs in on a Saturday
> Seb suddenly logs in from Russia
> Seb suddenly downloads many files
> ServerA suddenly interacts with 100 other systems

UEBA is very useful for forensics. UEBA’s usefulness for Real-time Alerting is limited.

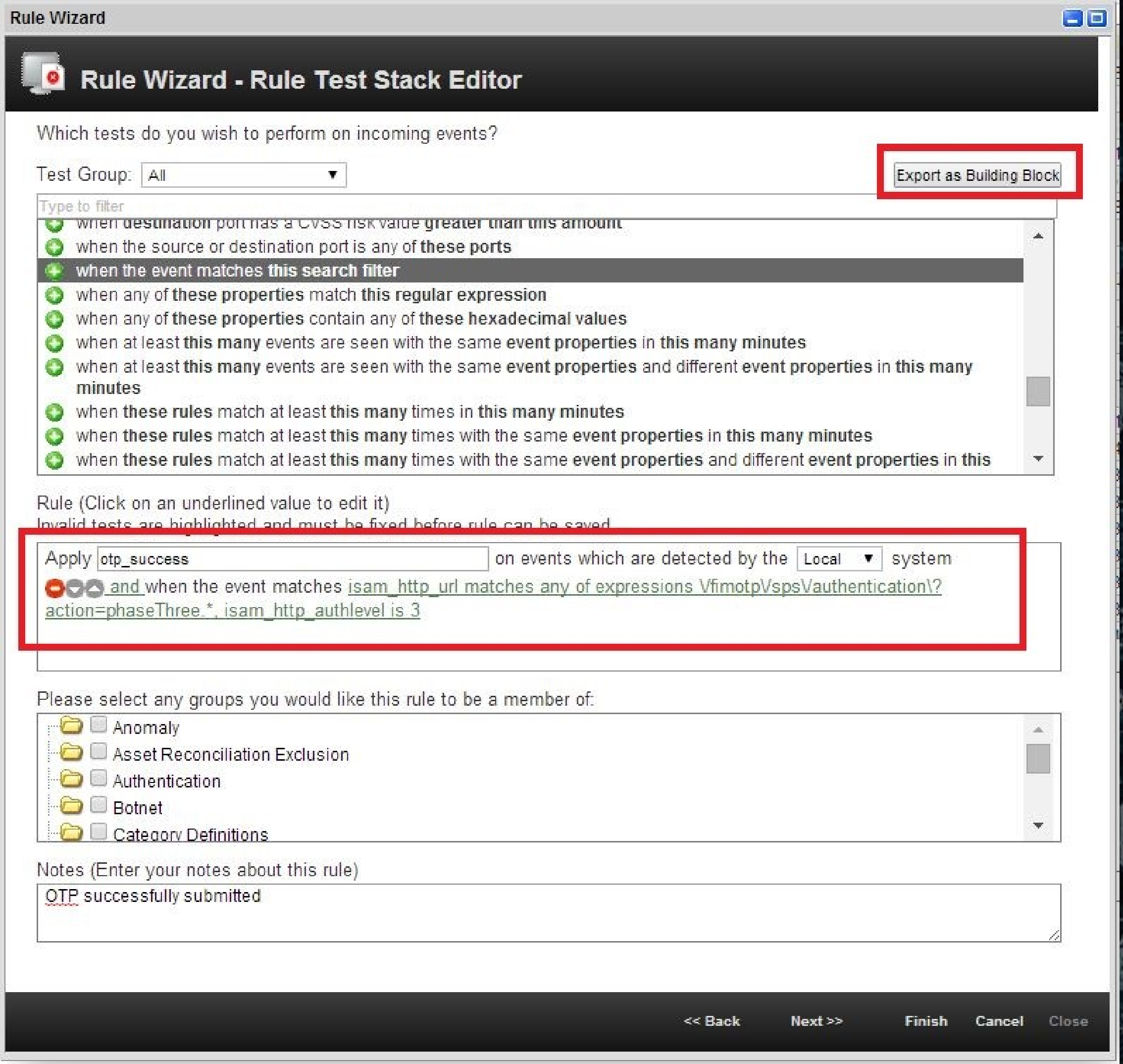
Best Use: Insider Threat Monitoring

New Log Source >> New Alert Rules

SOC analysts will have to analyze and play with new log sources for a while before use cases can be created in a meaningful way.

SIEM might come with pre-defined alert rules, which in most cases still have to be adjusted to the environment.

Many Log Sources produce most value through combination with other Log Sources >> Multi-Log-Source Alert Rules.



Rule Wizard

Rule Wizard - Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group: All ▼ Export as Building Block

Type to filter

- when destination port has a CVSS risk value greater than this amount
- when the source or destination port is any of these ports
- when the event matches this search filter
- when any of these properties match this regular expression
- when any of these properties contain any of these hexadecimal values
- when at least this many events are seen with the same event properties in this many minutes
- when at least this many events are seen with the same event properties and different event properties in this many minutes
- when these rules match at least this many times in this many minutes
- when these rules match at least this many times with the same event properties in this many minutes
- when these rules match at least this many times with the same event properties and different event properties in this

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply otp_success on events which are detected by the Local ▼ system
and when the event matches isam_http_url matches any of expressions VfimotpVspsVauthentication\?action=phaseThree.*, isam_http_authlevel is 3

Please select any groups you would like this rule to be a member of:

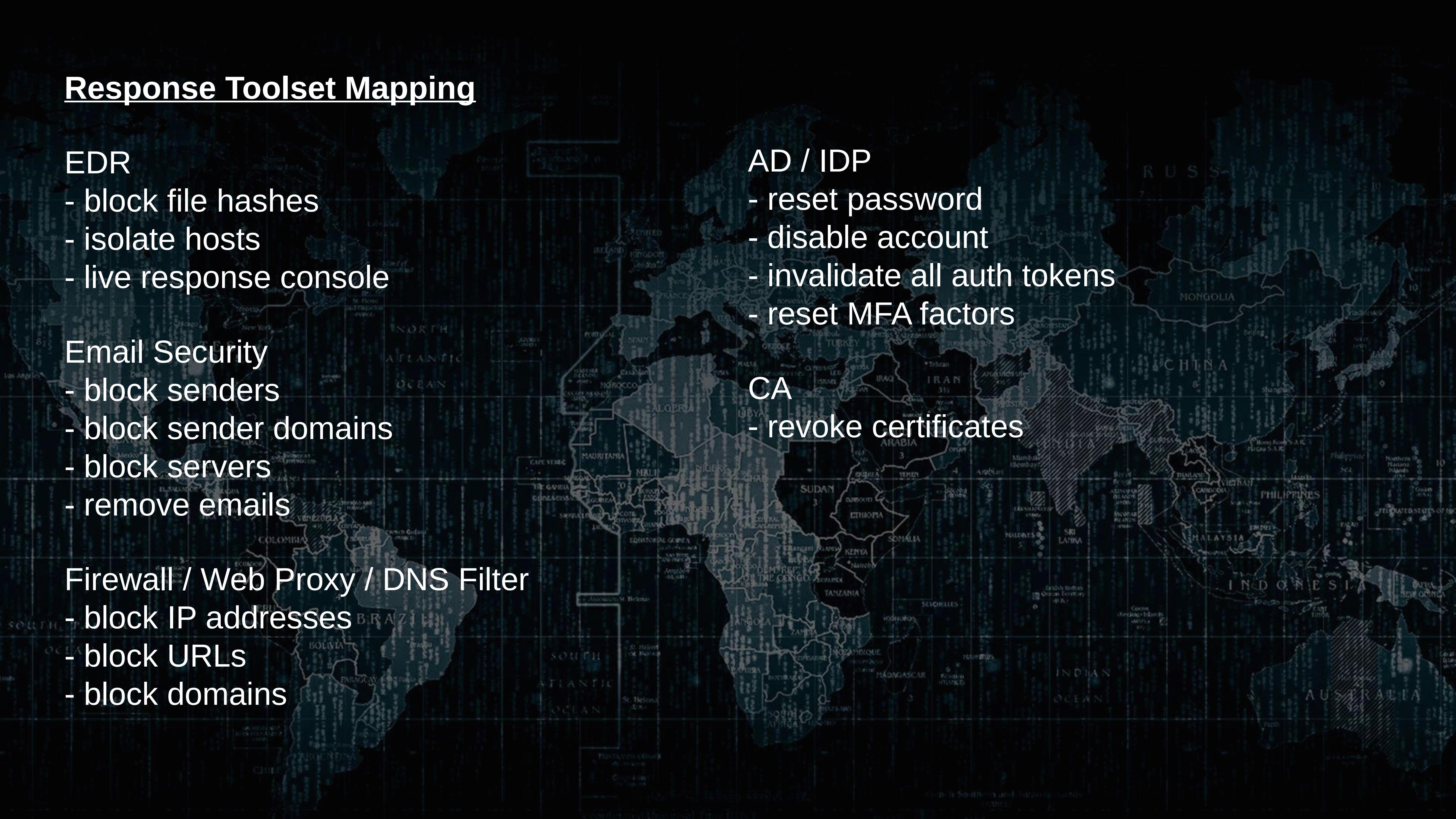
- □ Anomaly
- □ Asset Reconciliation Exclusion
- □ Authentication
- □ Botnet
- □ Category Definitions

Notes (Enter your notes about this rule)
OTP successfully submitted

Wrap up

0. Do you need a SOC? Do you need EYES ON GLASS?
1. MDR vs SOC (SOCaaS vs Hybrid SOC vs Inhouse SOC)
2. SOC Roles & Responsibilities
3. Define Escalation (SOC >> CIRT >> BRT >> Exec)
4. Define Use Cases & Procedures
5. Define Prioritization
6. Plan Technologies >> Detection & Response Architecture
7. Start Detecting >> Investigating
8. Start Responding...

Add-on slides



Response Toolset Mapping

EDR
- block file hashes
- isolate hosts
- live response console

Email Security
- block senders
- block sender domains
- block servers
- remove emails

Firewall / Web Proxy / DNS Filter
- block IP addresses
- block URLs
- block domains

AD / IDP
- reset password
- disable account
- invalidate all auth tokens
- reset MFA factors

CA
- revoke certificates

SOC Manager’s Recipe for 1st SOC

1. Identify immediate Use Cases
   (Where do you need help?)
2. Choose Level of Outsourcing
3. Work with vendors (and/or HR) to calculate budget
4. Convince Leadership and acquire budget
5. On-board Analysts
6. Analyze Detection coverage and produce Detection Road-map
7. Plan Response Action on-boarding
8. Define first set of daily/weekly/monthly metrics
9. Enter Continuous Improvement Cycle
   - Month 1 - 3   Meet with Analysts at least twice a week for 2h
   - Month 4 - 6   Meet with Analysts at least twice a week for 1h
   - Month 7+   Meet with Analysts at least once a week for 1h
   - Review daily metrics for first 6 months
   - Review weekly metrics for first 12 months
   - Review monthly metrics
   - Have Quarterly Business Review Meetings to align with overall Cyber Program

CANADA
UNITED STATES
MEXICO
NORTH ATLANTIC OCEAN
COLOMBIA
VENEZUELA
PERU
BOLIVIA
BRAZIL
PARAGUAY
ARGENTINA
CHILE
SOUTH PACIFIC OCEAN
SOUTH ATLANTIC OCEAN
IRELAND
UNITED KINGDOM
MOROCCO
ALGERIA
MAURITANIA
MALI
GREECE
IRAQ
IRAN
SAUDI ARABIA
YEMEN
SUDAN
ETHIOPIA
SOMALIA
KENYA
TANZANIA
ANGOLA
ZAMBIA
MOZAMBIQUE
MADAGASCAR
SOUTH AFRICA
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
INDIA
SRI LANKA
THAILAND
VIETNAM
CAMBODIA
PHILIPPINES
MALAYSIA
INDONESIA
JAPAN
INDIAN OCEAN
AUSTRALIA

?