Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

# CSIRT Evoluzione

**Gianluca Peco**

**Mini WS CCR sulla Sicurezza Informatica**
**13-15/2/2023 - Padova**

Public

# CSIRT evoluzione

- **infrastruttura**
  - basata su infrastruttura di virtualizzazione ridondata dei SSNN, richiede aggiornamento:
    - sistema di ticket tracking (da agganciare a strumenti OSINT – open source intelligence);
    - server di posta sicuro (ora basato su BSD, di difficile gestione – collaborazione in corso con Gruppo Mailing);
- **processi**
  - gestione automatizzata segnalazioni servizi esposti da shadowserver (creazione db consultabile, …);
  - adozione ulteriori strumenti/fonti OSINT (shodan, spiderfoot, …);

27

- **Creazione canali di comunicazione alternativi** (telegram? signal?)
  - per gestire eventuali emergenze per il gruppo in assenza di strumenti ufficiali
  - per veicolare comunicazioni importanti e asincrone verso responsabili sicurezza locali.

34

# Premessa ( lo so che non andrebbero mai fatte….)

Molti degli argomenti trattati nelle presentazioni relative ai wg non ancora strutturati e di R&D:

- CSIRT evoluzione
- SOC Fondazione
- CTI & OSINT

saranno elenchi di:

- desiderata (nella speranza di riuscire ad esaudirle)
- spunti di riflessione (nella speranza di approfondire le conoscenze)
- domande (nella speranza di trovare risposte)
- elenchi di tool provati (nella speranza possano essere utili)
- elenchi di tool ancora da provare (idem)
- spazio per la discussione (nella speranza si trovino convergenze)
- piano operativo di azione (motivo ultimo di questo workshop)

# Premessa (lo so che non andrebbero fatte…)

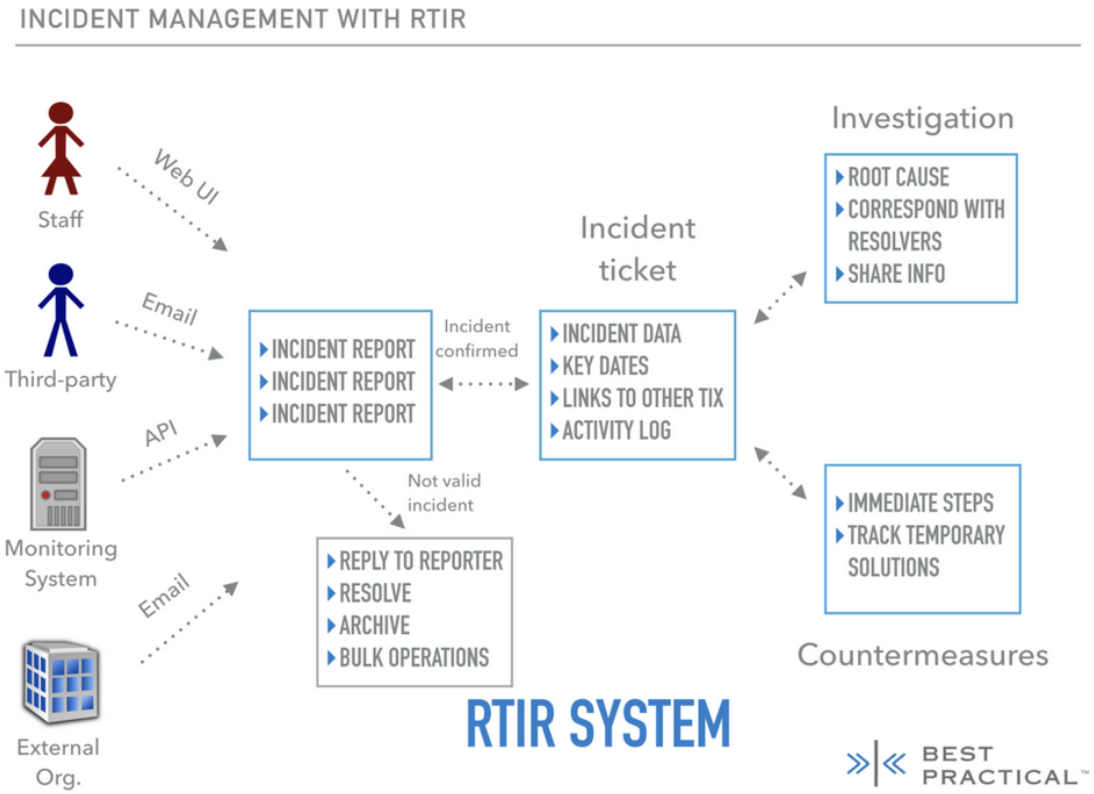
Soprattutto saranno cut&paste selezionati di alcuni documenti di riferimento che mi sono stati di aiuto per inquadrare le problematiche relative all'organizzazione e gestione di CSIRT & SOC

Non inserirò le citazioni in ogni slide, ma tutto il materiale si trova in:

- 11 strategies of a world class cybersecurity operations center (MITRE.org)
- FIRST_CSIRT_Services_Framework_v2.1.0.pdf (FIRST.org)
- How to set up csirt and soc (ENISA)

# RTIR Incident Management Workflow

- Incident handling workflow for security teams developed with the Janet CSIRT and Terena (now GÉANT) as described here.
- Separate queues for incident report triage, incident handling, investigation, and countermeasures.
- Keep communication clear with individual and bulk reply actions. Customize using RT's flexible email templating system.
- Constituencies configuration that allows parallel workflows but with different staff. Keeps ticket data segregated for staff serving multiple different customers.
- Tickets log all activity, store custom information in custom fields, track key dates to meet SLAs.



# RTIR

## Key Features & Functionality

- Dedicated incident dashboard with pre-built listings of most due tickets. Can be edited to show most important tickets at a glance.
- Preset with useful custom fields. Can add as many additional custom fields as needed to track incident data.
- Search tickets on any metadata attributes including status, dates, linked users, and custom fields.
- Generate activity reports in HTML, text, or spreadsheet format.
- Convenient linking of tickets related to an incident:
  - Box on IR creation to add an existing Incident ID
  - Link and New links next to Incident field in IR basics
  - Portlet for each linked queue that provides Create and Link links at top for key queues
- Incident page shows all linked incident reports, investigations, countermeasures tickets along with current status of each.
- Automatic parsing and population of IP custom fields for network-related reports.
- Cascading status change that allows actions like resolve to apply to linked tickets.
- Reply to a single correspondent or reply to all interested parties connected to all tickets for an incident.
- Merge/Split for incidents for flexible handling as an incident plays out.
- Bulk operations like Bulk Abandon and Bulk Reject to handle large batches of tickets at once.
- RT API can accept automatic data feeds from external systems such as Splunk, ArcSight, Nagios, Squil, and Qualys.
- Create multiple incident report queues to segregate incoming reports.
- RTIR also builds on Extensions that are compatible with Request Tracker.
- And, of course, all the other great features of RT.

# https://github.com/bestpractical/rtir-extension-misp

Integrazione RTIR con MISP. Realizzata e supportata dalla comunità di riferimento di RT

Alcune interessanti integrazioni permettono lo scambio di incidenti e l'enrichment degli eventi in MISP

```
DETAILS
    This integration adds several different ways to work between the MISP
    and RTIR systems as described below.

  Consume Feed from MISP
    After adding the MISP configuration described above, the Feeds page in
    RTIR at RTIR > Tools > External Feeds will have a new MISP option
    listed. This feed pulls in events for the past X number of days based on
    the DaysToFetch configuration. From the feed display page, you can click
    the "Create new ticket" button to create a ticket with information from
    the MISP event.

  MISP Portlet on Incident Display
    On the Incident Display page, if the custom field MISP Event ID has a
    value, a portlet MISP Event Details will be displayed, showing details
    pulled in from the event via the MISP REST API.

  Update MISP Event
    On an incident with a MISP Event ID, the Actions menu will have an
    option "Update MISP Event". If you select this action, RTIR will update
    the existing MISP event with an RTIR object, including data from the
    incident ticket.

  Create MISP Event
    If MISP Event ID has no value, the Actions menu on incidents shows an
    option to "Create MISP Event". Select this to create an event in MISP
    with details from the incident ticket.
```

# Case Management

**Case Management**

- Every SOC needs a way to track incidents. Generally, the more mature the SOC, the more sophisticated and customized that incident tracking capability needs to be. Case and workflow management, perhaps more than any other SOC tool, is intimately involved in SOC operations. Consequently, there is no one size fits all.
- This section covers requirements, architectural options, and success factors for incident tracking. It also discusses areas in which an incident tracking system (by itself) is insufficient, indicating the SOC should seek out additional forms of knowledge management.

# More than ticketing system

- Allows consistent and complete information capture across incidents for each state of the incident life cycle alert triage, in-depth analysis, response, closure, and reporting
- Can record both structured information from analysts (incident category, time reported), semi-structured data (impacted users, impacted systems) and unstructured information (analyst narrative), along with time-stamped notes
- Has necessary interfaces with constituents, usually including one or more of the following:
  - Direct mediated access to cases a constituent or constituent's service/systems are involved in
  - Communication with one or more constituency ticketing and case management systems
  - Email messaging and interface with constituents, such as notifying constituents on case updates, automated escalation, tasking, and email replies that will update the case
- Is insulated from adversary access, particularly in the case of a large-scale breach

# More than ticketing system

- Supports trending, metrics, and feedback: Including mean/median time to acknowledge, respond, eradicate, and close
- As a feedback loop to inform detections and analytics tuning, and for advanced SOCs, labeling for supervised ML models
- The SOC should expect to routinely gather and report on metrics and workflow
- Can incorporate artifacts or pointers to artifacts, such as events or malware samples.
- Allows analysts to capture information about specific entities (particularly users and hosts) that can be referenced and correlated with other cases, thereby providing continuity across disparate analysts and cases, and potentially avoiding redundant work
- Allows linking and parent/child relationship between cases, including the ability to spawn child cases and tasks to other parties, such as request malware analysis or follow up by another analyst
- Some ticketing systems will overlap with related product segments, in particular: Information collection, data enrichment, and response automation(SOAR)
- Cyber threat integration and enrichment, such as threat indicator matching

# Case management and case tracking pros and cons

| Approach | Pros | Cons |
|---|---|---|
| **Existing IT case management system used by the constituency IT operations organization** | • Usually comes with polished feature set, documented setup, and central administration.<br>• Economy of scale; acquisition and O&M free or less expensive.<br>• Larger pool of case management system experts.<br>• Robust reporting and metrics.<br>• Seamless integration with IT help desk and IT operations | • Less likely to be flexible to SOC needs.<br>• SOC may need to adjudicate customizations through other groups and approval boards.<br>• Sensitive data is comingled with general IT help tickets.<br>• Admins can see SOC's cases which increased the likelihood of compromise of internal threat cases.<br>• If general constituency systems are compromised, adversary may be able to see or manipulate SOC cases.<br>• Customization may be lengthy or expensive, especially if vendor does not provide "out of the box" SOC extensions, use cases, templates, and workflows.<br>• Depending on customization options, may feel equivalent to a "walled garden." |
| **SOC instance of COTS IT case management system** | • Comes with polished feature set, documented setup, and central administration.<br>• Usually has out of the box customization specific to SOC use cases<br>• Robust reporting and metrics.<br>• Case details available only to parties designated by the SOC.<br>• Usually, the most flexible and powerful approach amongst all ticketing options. | • Can be very expensive.<br>• Customization may be lengthy or expensive, especially if vendor does not provide "out of the box" SOC extensions, use cases, templates, and workflows.<br>• Depending on customization options, may feel equivalent to a "walled garden." |
| **SOC instance of FOSS security case management system** | • Depending on tool chosen, may come with polished feature set, documented setup, and central administration.<br>• Many (such as TheHive , SCOT and RTIR ) are designed specifically for use by SOCs or have incident handling modules or plug-ins.<br>• Free to acquire.<br>• Reporting and metrics possible.<br>• Case details available only to parties designated by SOC. | • Unless there is a commercial vendor that offers professional services, setup and sustainment may be a challenge with community-only support.<br>• O&M & customization may require staff with experience in scripting, programming, or databases. |

# Case management and case tracking pros and cons

| Approach | Pros | Cons |
|---|---|---|
| **SIEM or SOAR case tracking system** | • "Free" and usually easy to leverage if SOC owns a SIEM or SOAR.<br>• Likely very strong if part of a SOAR<br>• Specifically built for tracking security incidents.<br>• Leverages user groups, permissions, and escalation paths shared with other SIEM/SOAR tasks and functions.<br>• Users can attach events and some artifacts to tickets. | • Not appropriate if SOC workflow is not focused on the SIEM.<br>• Typically, more limited flexibility, depending on SIEM product.<br>• Usually less robust than purpose-built case management (especially with some legacy SIEM products)<br>• If SIEM/SOAR goes down, nearly all aspects of SOC operations (triage, analysis, case tracking) are also down.<br>• Optimized for alert handling from SIEM, usually less-so for other platforms (e.g., email or EDR). |
| **Custom-built ticketing system** | • Extremely flexible<br>• Reporting and metrics possible<br>• Case details available only to parties designated by SOC | • Expensive to build and maintain.<br>• SOC must build system from scratch, requiring staff with extensive experience with programming and databases.<br>• Development of system may take a while, since SOC must start from nothing.<br>• Less and less justified due to availability of robust COTS and FOSS SOC ticketing capabilities. |
| **Cloud-based SaaS ticketing system** | • Has pros associated with SOC tools and data in the cloud (See Section 8.7)<br>• Turnkey capability which can be up in a matter of hours or days.<br>• Usually no upfront costs.<br>• Sustainment, O&M, upgrades very simple.<br>• Generally, will require less staff to support. | • Has cons associated with SOC tools and data in the cloud (See Section 8.7).<br>• Heavily dependent upon security features and internal protections of the vendor.<br>• Could be compromised if vendor or underlying cloud is breached.<br>• Single errors in configuration and management can easily open system to outside exposure or compromise.<br>• Not appropriate for air gapped SOCs and enclaves.<br>• Depending on customization options, may feel equivalent to a "walled garden." |

# THE HIVE – Cortex – Cortex Neuron

Soluzione XSOAR opensource molto promettente – R&D candidato

Case Management ( Ticket ?? )

Observable Analysis

Repository per analyzer & responder - no shadowserver OOB

https://thehive-project.github.io/Cortex-Analyzers/

## TheHive 4 #

TheHive is a scalable, open source and free Security Incident Response Platform designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.

license AGPL-3.0 release v4.1.24

- Sources: https://github.com/TheHive-Project/TheHive
- Documentation: https://docs.thehive-project.org/docs/thehive/

## Cortex

Cortex is a powerful observable analysis and active response engine.

license AGPL-3.0 release v3.1.7

- Sources: https://github.com/TheHive-Project/Cortex
- Documentation: https://github.com/TheHive-Project/CortexDocs

## Cortex Neurons

Cortex neurons is the repository of the reviewed Analyzers and Responders, contributed by the community.

tag v3.2.3

- Sources: https://github.com/TheHive-Project/Cortex-Analyzers/
- Documentation: https://thehive-project.github.io/Cortex-Analyzers/

# SCOT?


## What is SCOT?

SCOT is an Incident Response collaboration and knowledge capture tool focused on flexibility and ease of use. Our goal is to add value to the incident response process without burdening the user.SCOT was developed at Sandia National Laboratories by and for the Incident Response team over a period of several years. We're making SCOT open source to try and help out the rest of the computer security community.

## Why use SCOT?

SCOT was developed by incident responders for incident responders to make our jobs easier.

- Free text HTML (no hunting for the right field)
- Designed for Cyber Security data
- Instant updates keep the team in sync
- Automated detection/correlation of IPs, Email addresses, Domains and Hashes
- Integrated offline GeoIP databases
- Alert collection and standardization
- Plugin infrastructure for automation
- And much more

SCOT is now available on GitHub at the link below. Please see our documentation on ReadTheDocs for Install and usage instructions.

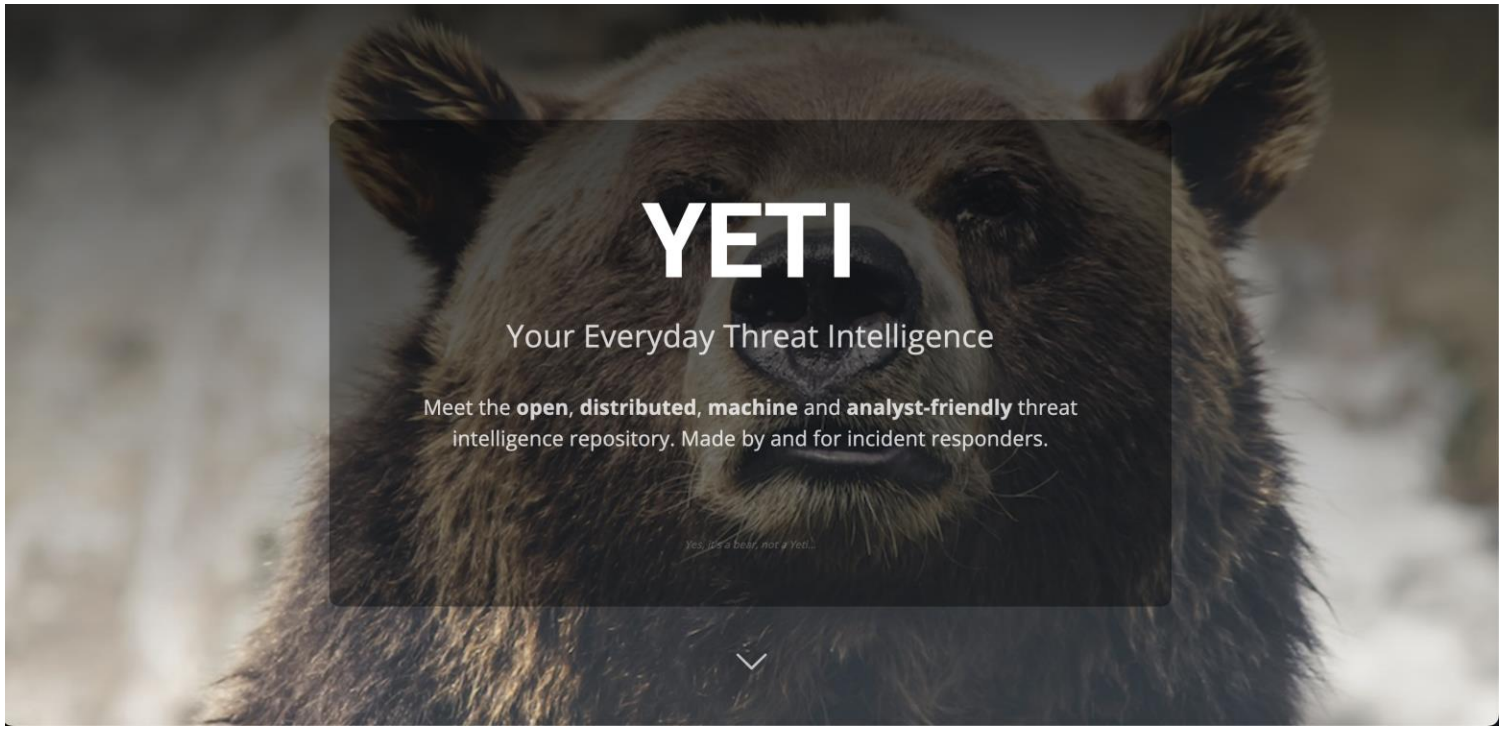
# YETI

In a nutshell, Yeti allows you to:

- Submit observables and get a pretty good guess on the nature of the threat.
- Inversely, focus on a threat and quickly list all TTPs, Observables, and associated malware.
- Let responders skip the “Google the artifact” stage of incident response.
- Let analysts focus on adding intelligence rather than worrying about machine-readable export formats.
- Visualize relationship graphs between different threats.

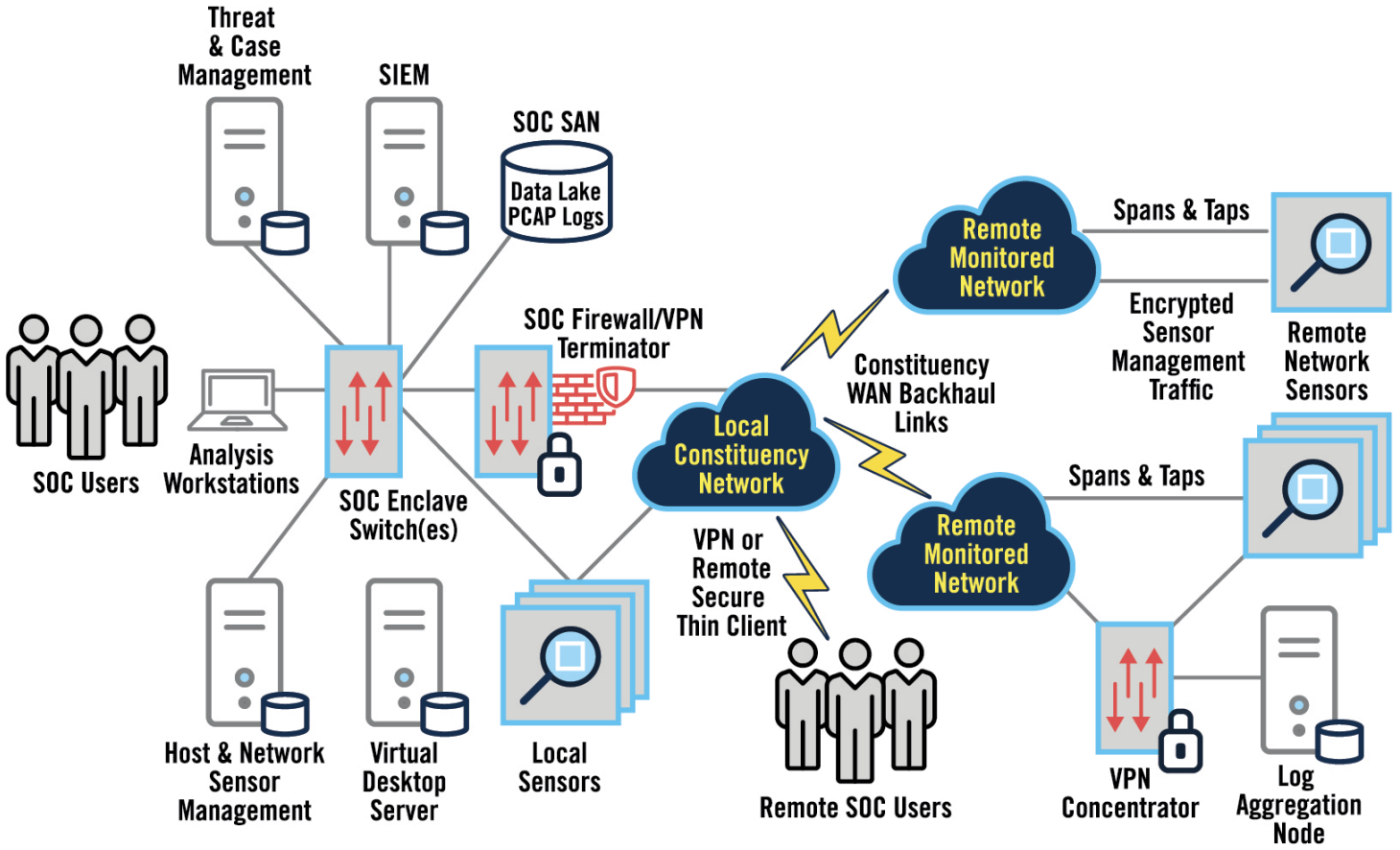
This is done by:

- Collecting and processing observables from a wide array of different sources (MISP instances, malware trackers, XML feeds, JSON feeds…)
- Providing a web API to automate queries (think incident management platform) and enrichment (think malware sandbox).
- Export the data in user-defined formats so that they can be ingested by third-party applications (think blocklists, SIEM).



# Protecting SOC Tools and Data

- The SOC is a source of tremendous insights and situational awareness across the constituency, not to mention the raw data it collects.
- The SOC also has the responsibility to protect these tools and data from misuse. For example, even the best SOCs have gaps in their visibility, which is useful to an adversary.
- Knowledge of what monitoring tools are in use might allow the adversary to mount direct attacks against them or, more often, shape its attacks to avoid detection. Yet, sharing insights with others in the constituency is also important for defense.
- This causes a natural tension, and every SOC must decide the mix of protections and sharing it should put in place.



# Communication suite ??

Comunicazione in senso esteso non solo canali asincroni ma anche sincroni out of band ???

Telegram
Signal
Jitsi
BigBlueButton
??

# Proposte

- Ticketing system RTIR : già operativo, orientato all'incident response, da integrare con MISP
  - Semplificazione dei due sistemi in uso
- TheHive/Cortex/CortexNeutron da affiancare in produzione ad integrazione degli strumenti CSIRT
- *Integrazione fonti OSINT – vediamo anche una prossima presentazione*
- YETI test di funzionalità per verificarne l'utilità (fase 2 ??)
- Infrastruttura da consolidare e semplificare per facilitare la fruizione senza diminuire la sicurezza
  - Apertura sul perimetro interno via VPN per l'accesso alle console di MISP TheHive RTIR
  - Apertura sul perimetro interno diretta da reti fidate (analisti distribuiti)
- Integrazione con Incident response dell' EDR