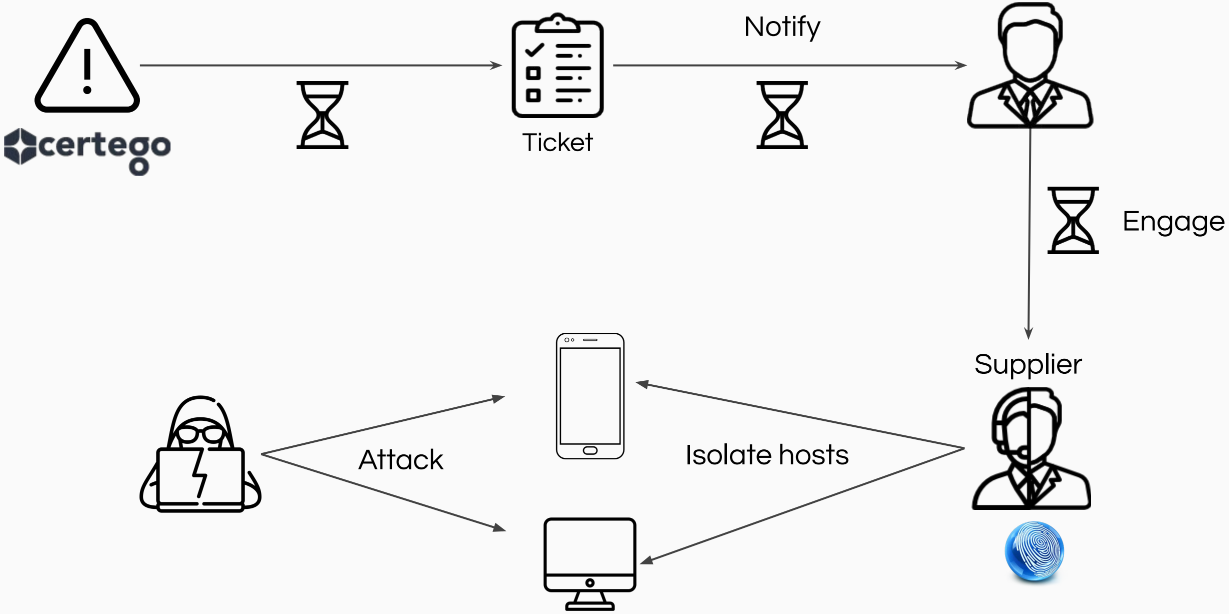
Tactical Response
Cisco ISE pxGrid Integration

Tactical Response

Tactical Response - Scenario

External managing of Cisco ISE could lead to a high MTTR (Mean Time To Respond). Even if the network is managed internally, there could be problems performing some actions (internal escalation, high workload, etc.)

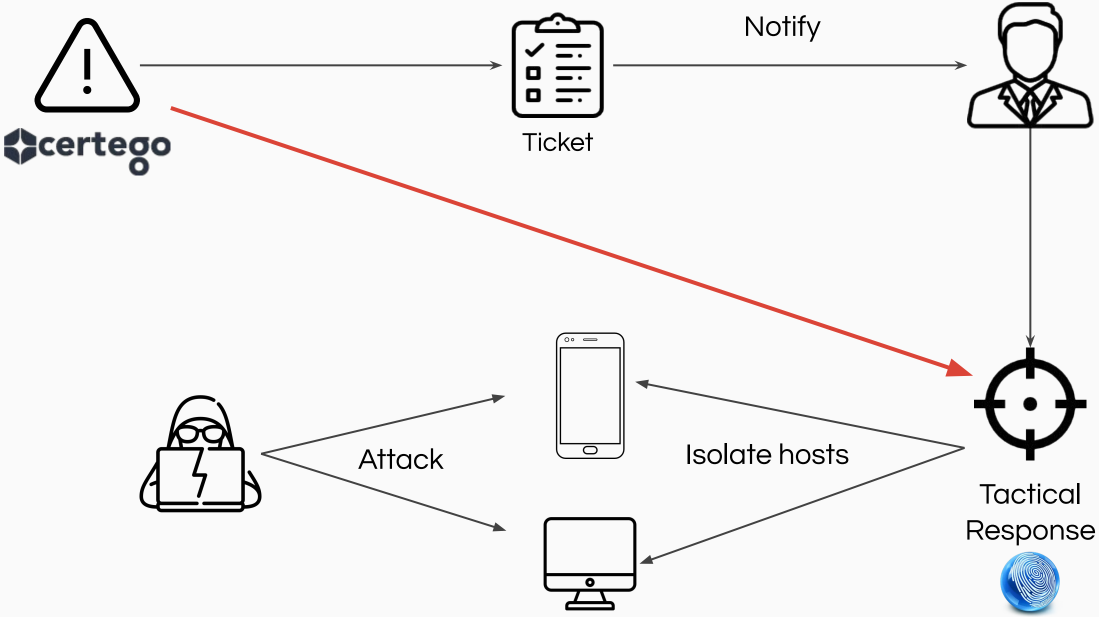


Tactical Response - Main goals

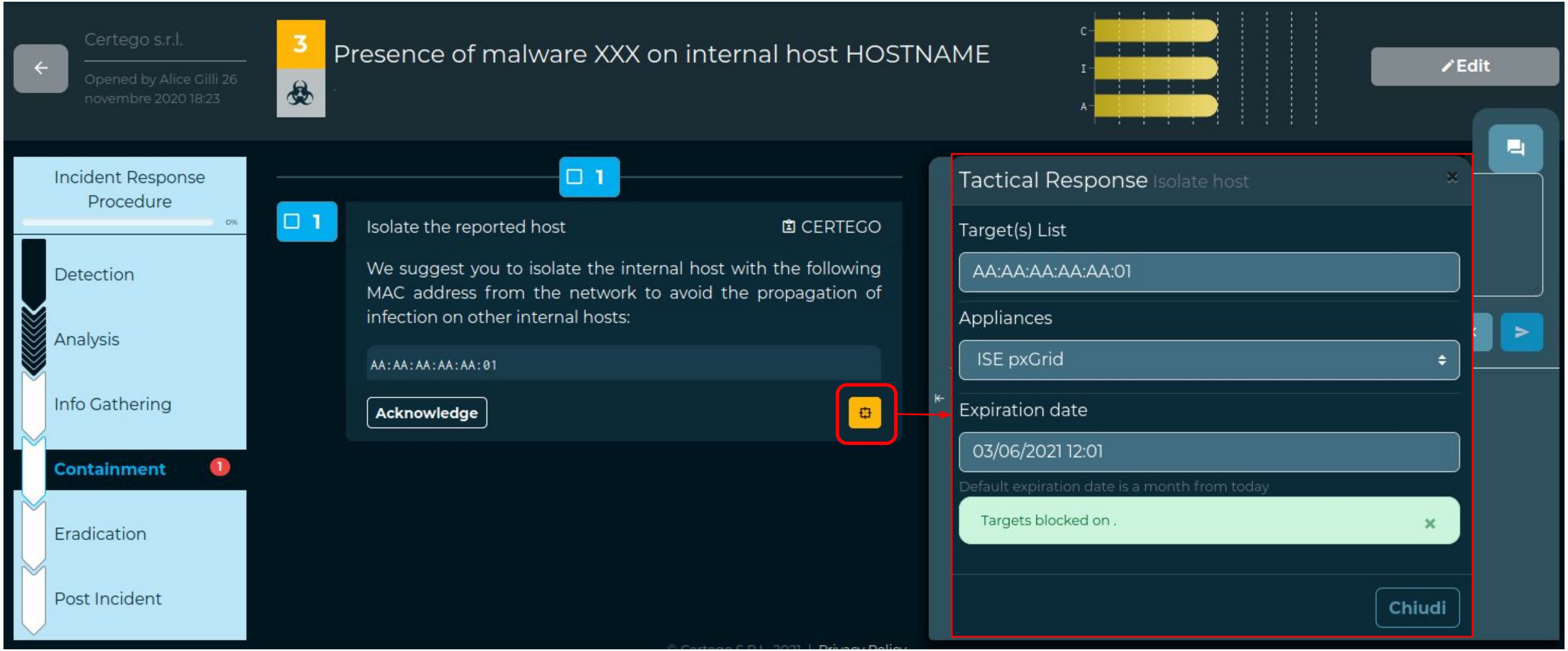
- Reduce the time needed to contain a Cyber Security Incident
- Prevent additional attacks or infections
- Lower the risk associated to ongoing incidents (e.g. by blocking resources related to further infection steps)
- Reduce workload of the Customer

Tactical Response - How it works

Tactical Response enables Certego IRT to contain attacks in less time, by isolating infected hosts via pxGrid API



Sample Ticket - Containment



Opened by Alice Gilli 26 novembre 2020 18:23

Presence of malware XXX on internal host HOSTNAME

Isolate the reported host — CERTEGO

We suggest you to isolate the internal host with the following MAC address from the network to avoid the propagation of infection on other internal hosts:

```
AA:AA:AA:AA:AA:01
```

Tactical Response Isolate host

Target(s) List: AA:AA:AA:AA:AA:01

Appliances: ISE pxGrid

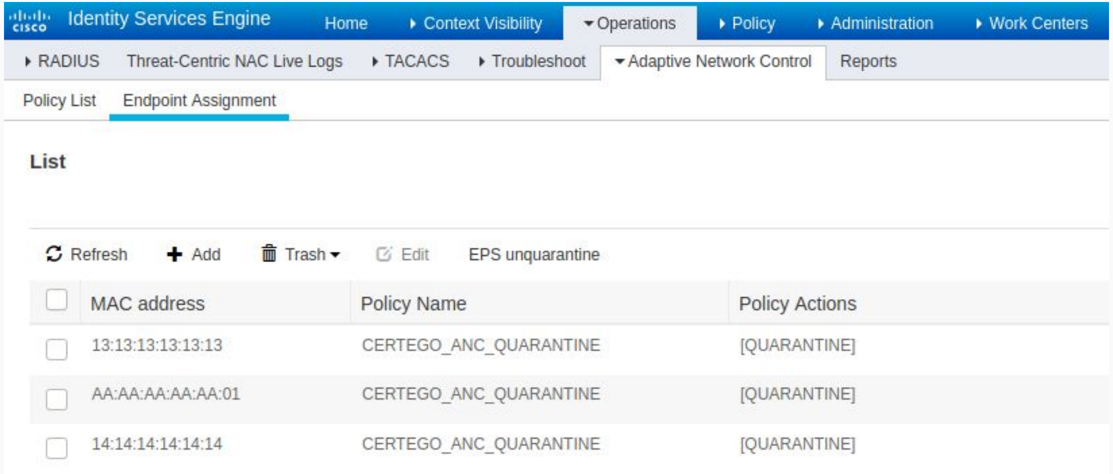
Expiration date: 03/06/2021 12:01

Default expiration date is a month from today

Targets blocked on .

Cisco ISE - ANC Policy

The MAC address AA:AA:AA:AA:AA:01 is now blocked on ISE, using pxGrid API.



□	MAC address	Policy Name	Policy Actions
□	13:13:13:13:13:13	CERTEGO_ANC_QUARANTINE	[QUARANTINE]
□	AA:AA:AA:AA:AA:01	CERTEGO_ANC_QUARANTINE	[QUARANTINE]
□	14:14:14:14:14:14	CERTEGO_ANC_QUARANTINE	[QUARANTINE]