

HOW WE SIMPLIFY INCIDENT RESPONSE

Ferruccio Vitale, SOC Manager
bw digitronik/Cybertech Group

AGENDA

- Meet our SOC
- Why IR is so complex
- How we made life easier



MEET OUR SOC

Cybertech Group



CYBERSECURITY EXPERTS *of the* ENGINEERING GROUP

Cybertech Group is one of the most important European Managed Security Services Providers.

With **more than 30 security specialists**, analysts and incident responders, we offer a **24/7 SOC** and **Incident Response Retainer** program, enabling organizations to a faster and more effective response to cyber incidents.



3

FEDERATED
COUNTRIES

+30

SECURITY
ANALYSTS

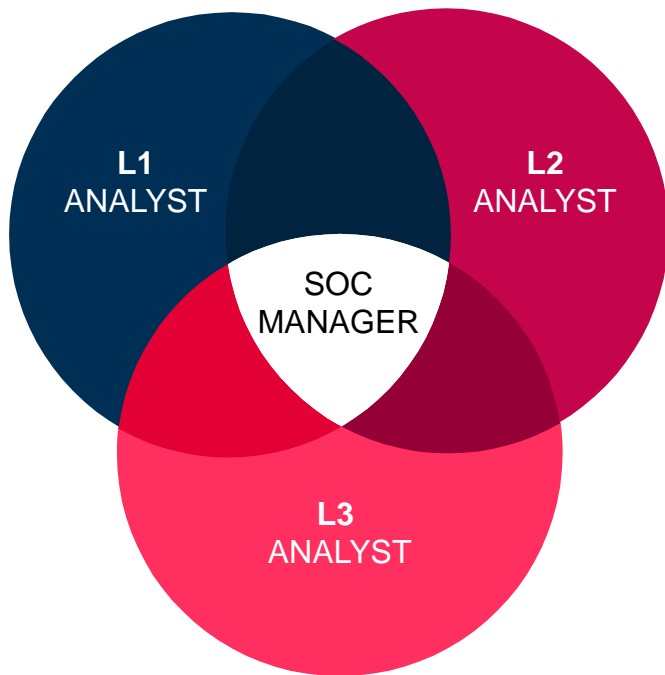
+150

ALERTS
PER DAY



CYBERTECH
ENGINEERING GROUP

Strongly organized and skilled



L1

Real Time Monitoring
Initial Triage
Information Collection
Change Management

L2

Incident Analysis
Incident Coordination
Mitigation
Remediation

L3

Threat Intelligence
Threat Hunting
Adversary Intelligence
Forensic Analysis
Malware Analysis
Reverse Engineering
Incident Response

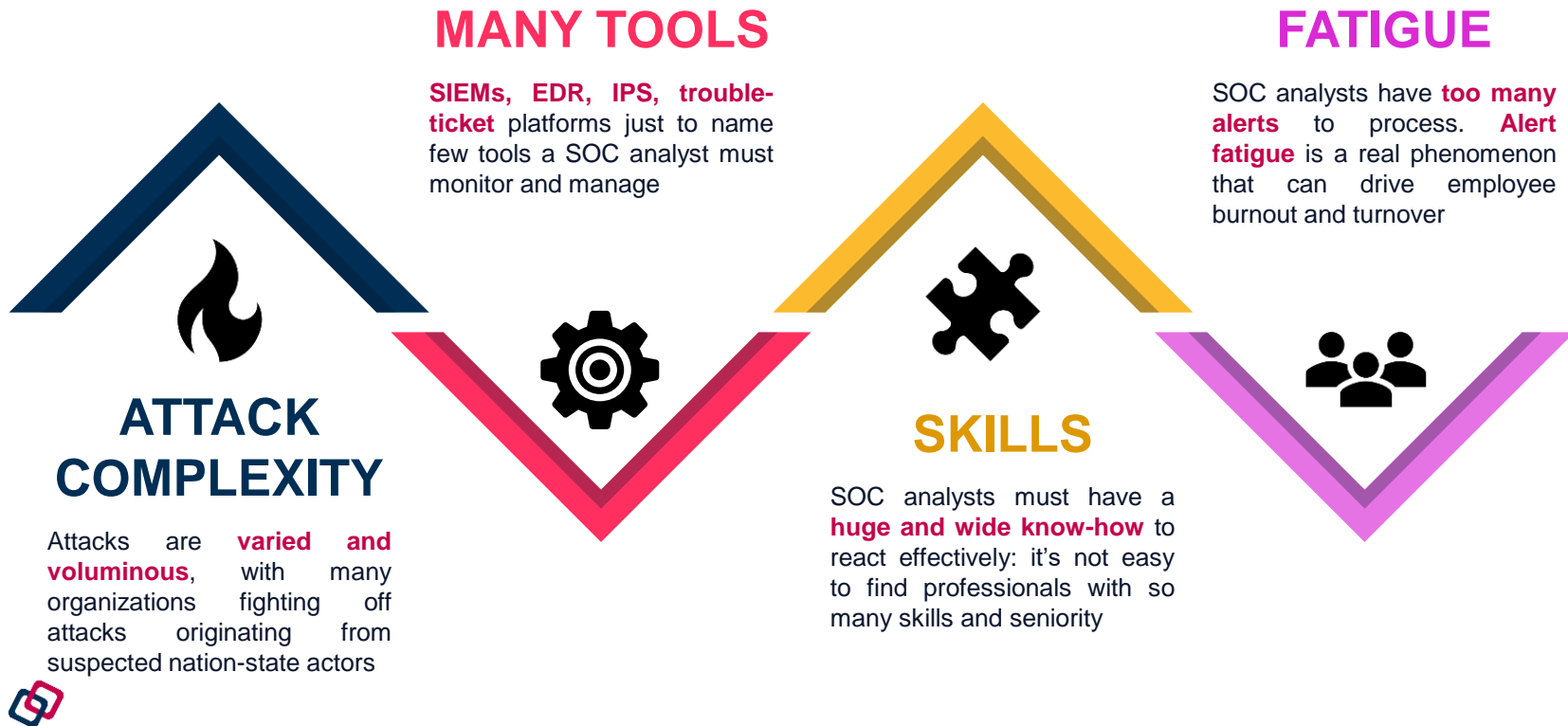


WHY IR IS SO COMPLEX

Technical and human aspects



Scenario



Still some issues



- Alerts Priority
- Time To Respond
- Quality Of Analysis
- Compliance to Laws
- Metrics
- Reusability
- Client procedures



WORK FROM HOME, TECHNICAL AND HUMAN IMPACTS

- Lower level of security
- Fragile connectivity
- Need for more communication and collaboration
- People are even more targeted



THE NEEDS *AND* THE ANSWERS

How we made life easier



What analysts want?

AUTOMATION

More automation to speed up IR and reduce the stress of manual operations

INTEGRATION

Integration of SOC tools with third-party systems so they can easily connect with other departments and IR processes

THREAT INTEL

Threat intelligence integrated with SOC tools to cut down on the challenge of monitoring too many threat intel feeds



Incident triage steps

- Enrich data via threat intelligence lookups
 - Attackers' source IP reputation
 - Phishing domain reputation
 - Indicator of Compromise
- Lookup client's CMDB
- Geographical data mapping
- Collect further data from EDR, IPS
- Evaluate known vulnerabilities of the targets

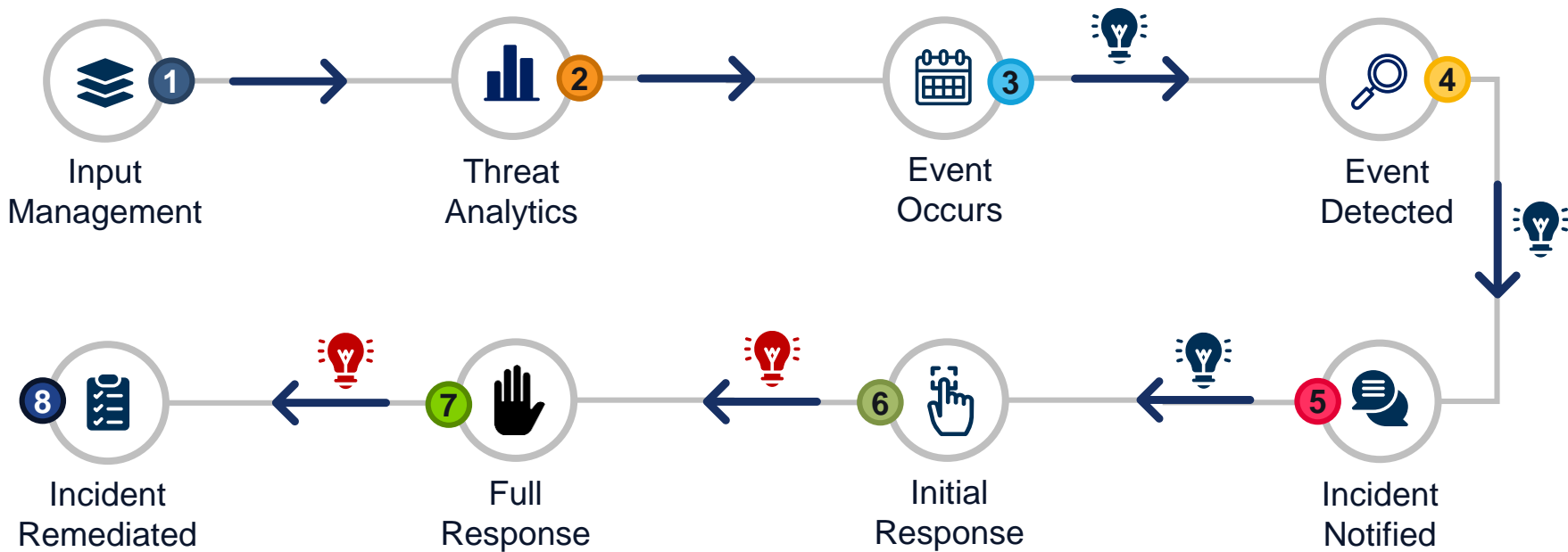


During an attack,
every second counts



What if we are able
to automate all
these steps?

Introducing the SOAR



Data Enrichment



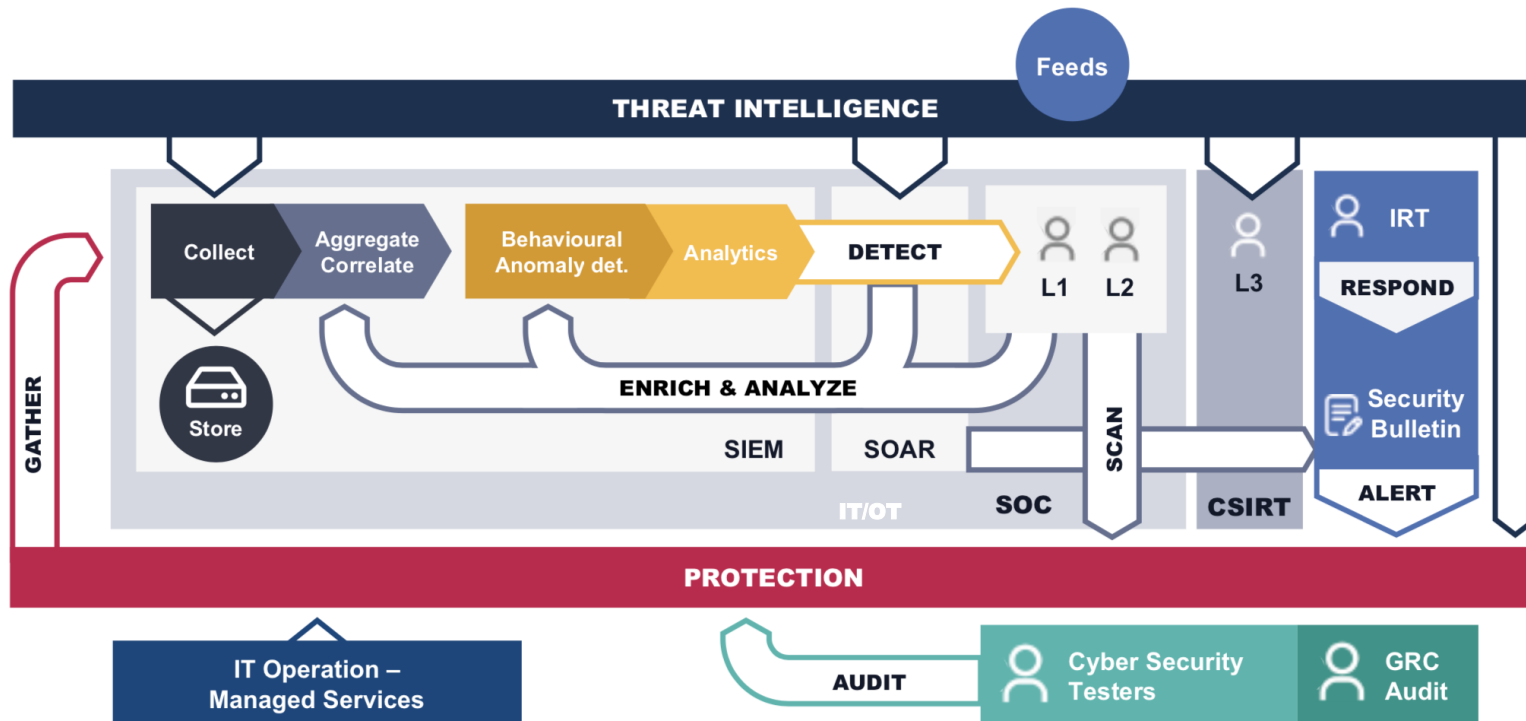
Security Control Automation

A single tool for every challenge

- All alerts converge into a **single dashboard**
- Automated **prioritization** of alerts
- Ability to **track** incident, indicator, and analyst-level metrics
- Remediations are **mediated** by the platform
- **Better communication** with teams outside of security operations

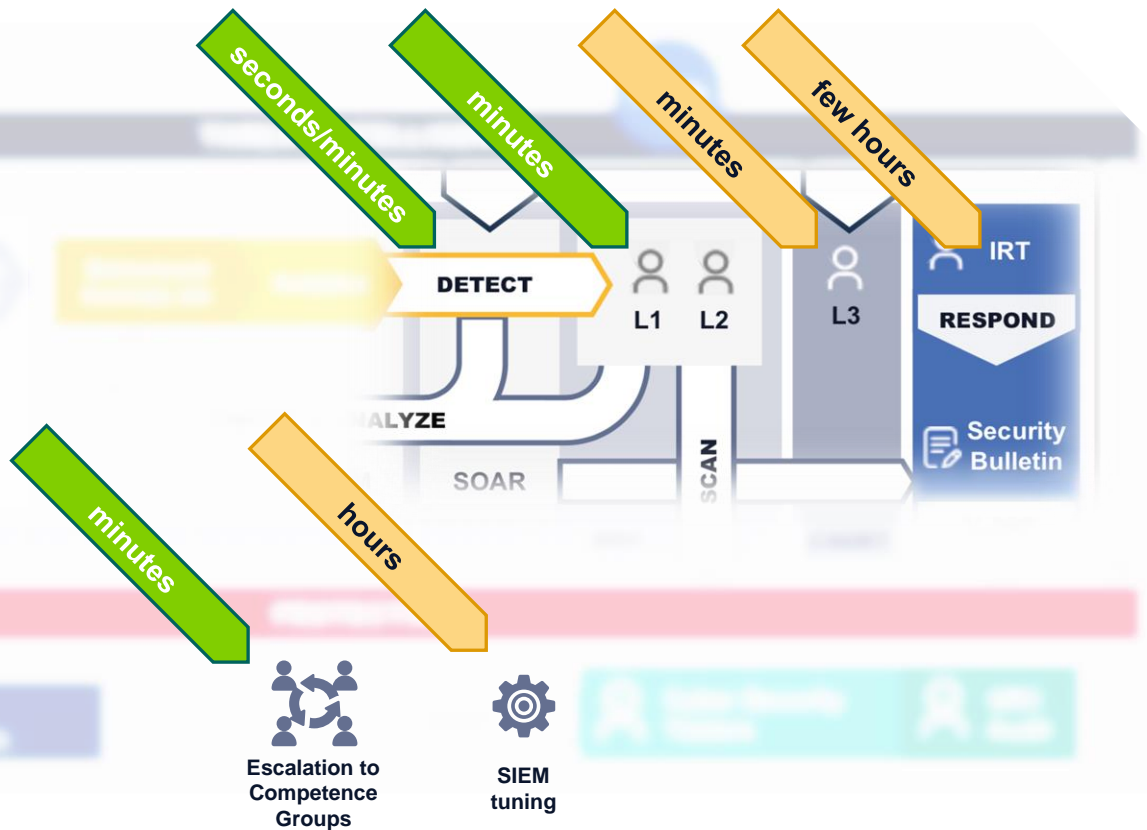


The heart of our framework



















Elapsed

How quickly
the SOC acts
and reacts



Automation in Phishing Analysis

15 minutes
without
SOAR

| | | |
|---|---|---|
|  | Open the trouble ticket platform, accept the ticket |  |
|  | Download the original mail(s) |  |
|  | Analyze mail headers |  |
|  | Lookup Threat Intel sources |  |
|  | Analyst consideration |  |
|  | Notify the client it's phishing |  |
|  | Block the sender on mail servers |  |
|  | Block links on DNS protection service |  |

3-5 minutes
with SOAR

**MTTR decreased
by 75%**



 Manual operation

 Automatic operation

Benefits

| NEEDS | SOLUTIONS | RESULTS |
|--------------|--|--|
| Threat intel | Respond to incidents with confidence and proper priority | Lower MTTD |
| Automation | 30% of our use cases are fully automated | Lower workload |
| Integration | Developed 40 automations to interact with third-party platforms | Lower error rate, higher security |
| Playbooks | Standard playbooks can easily customized on client needs Complaint to privacy regulations of all European countries | Higher compliance, satisfaction |



Thanks for your attention



Ferruccio Vitale

SOC Manager

 www.cybertech.eu

 [@Cybertech_eu](https://twitter.com/Cybertech_eu)

 [Cybertech.eu](https://www.linkedin.com/company/Cybertech.eu)

 [gruppo.engineering](https://www.facebook.com/gruppo.engineering)

ferruccio.vitale@cybertech.eu

