Lifecycle of a security incident: from detection to response

Giovanni *merlos* Mellini

Codemotion Rome
23rd of March 2019

```
merlos@codemotion:~$ whoami
Giovanni merlos Mellini
Head of "Information, systems and network Security" at ENAV S.p.A.
Cyber Saiyan - Founder and President
RomHack Organizer
```


@merlos1977 giovannimellini scubarda.wordpress.com

Cyber Saiyan
www.cybersaiyan.it

ROMHACK
CYBERSECURITY CONVENTION
ROMA>28_SET_2019
Link Campus University

RomHack 2019
www.romhack.io

WHAT?

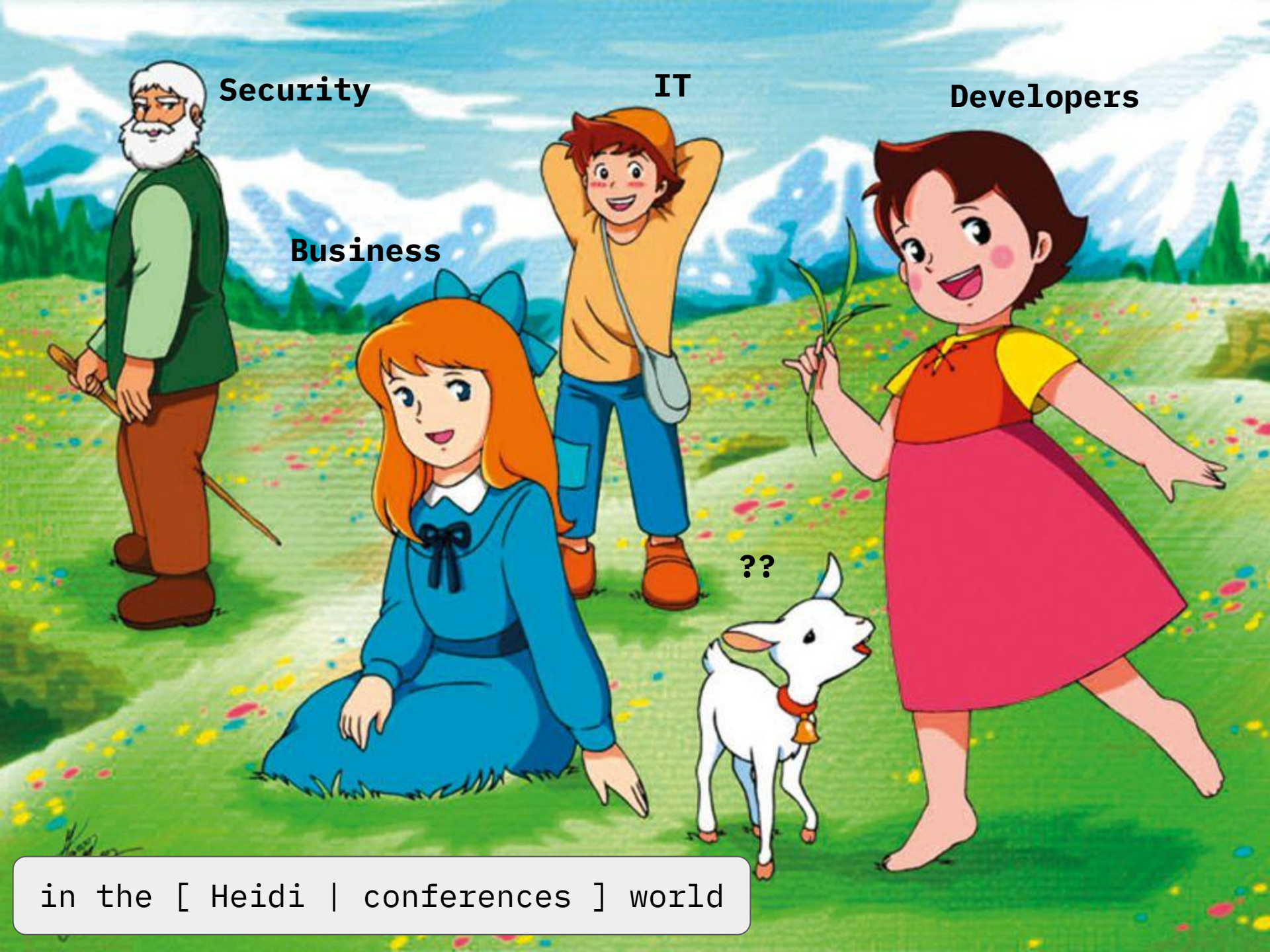
A real life experience

- started with a security check on a production system
- found a critical security problem
- what if exploited?
- how to detect it and mitigate risk?
- how to respond?

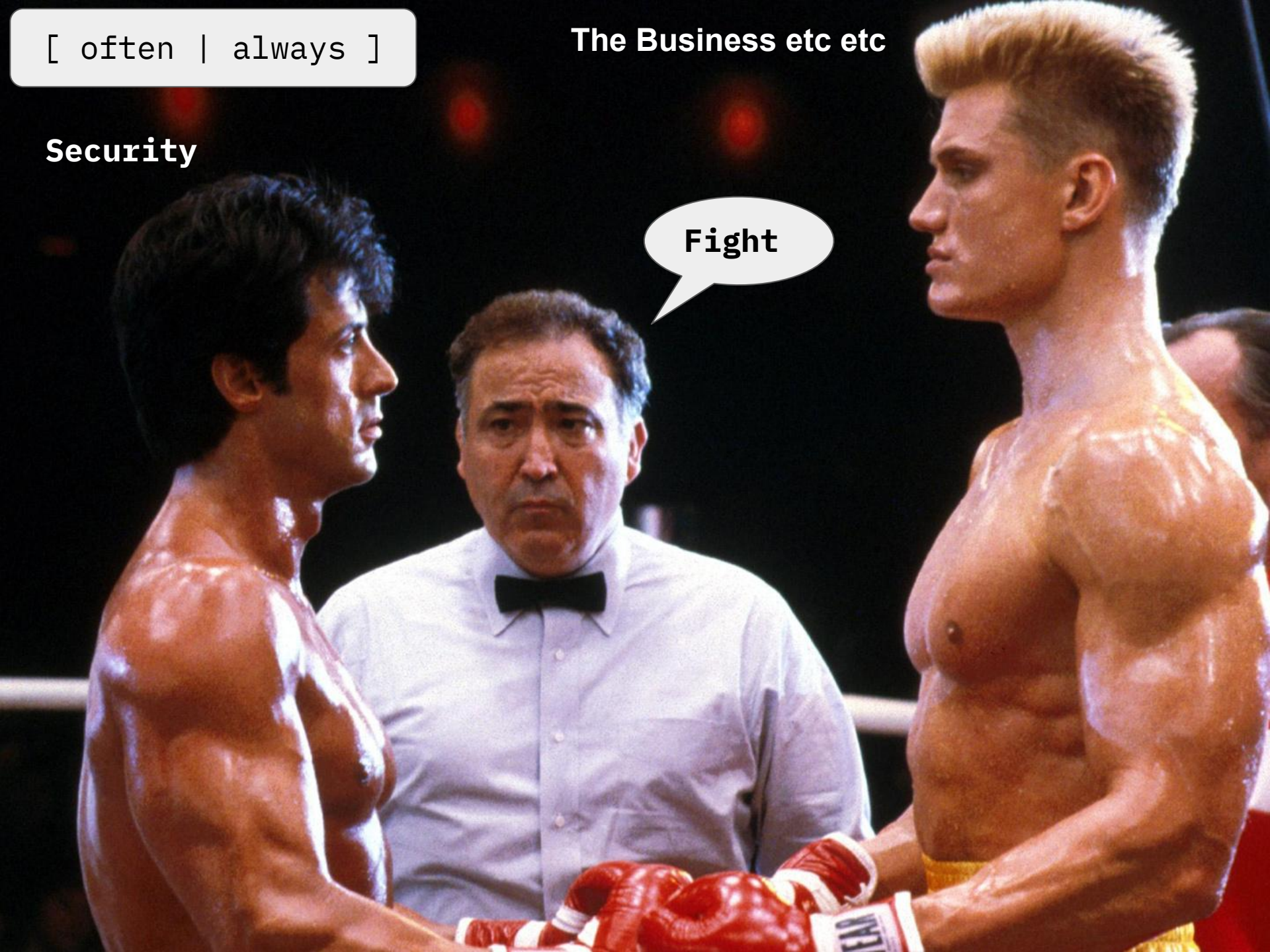
Lab lab lab

Murphy law? “Nun te temo”

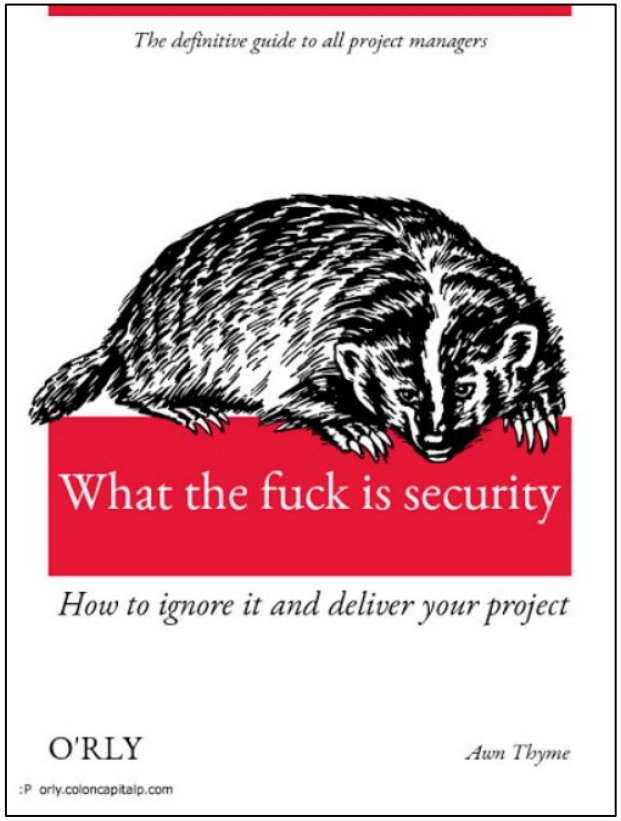
The root cause
or
how we deliver projects



in the [Heidi | conferences] world


[often | always]
The Business etc etc
Security
Fight

Vs



If you don’t have **security since the beginning** of your projects (ideal) probably you’ll have **security issues**

Security Checks

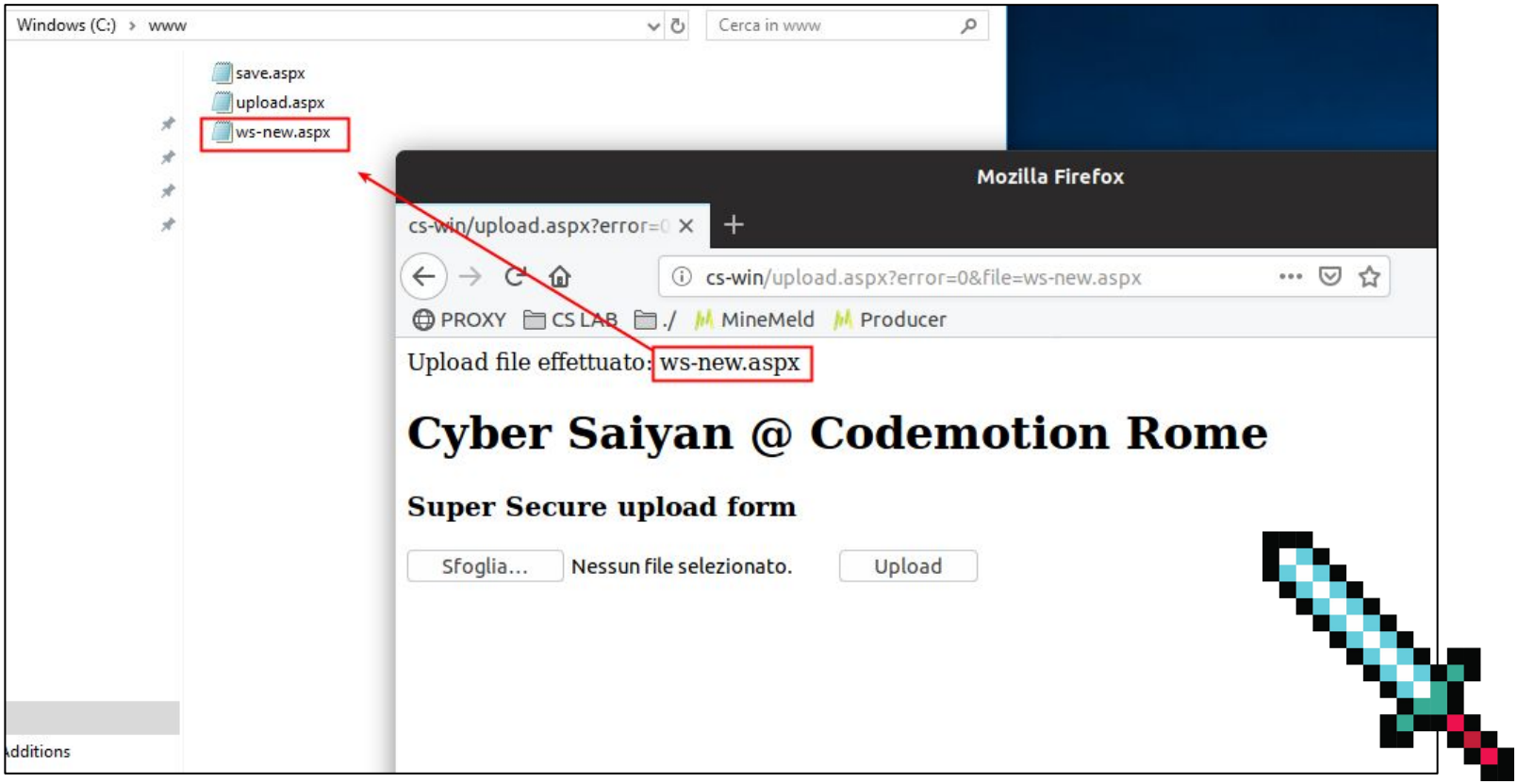
If you are lucky enough to have an **effective Security process** somewhere in your company there is a chance you intercept the project before goes live

THIS IS NOT OUR CASE

We knew about this system (web application) only after the IT dept. deployed it and **is actively used by the users**

Schedule a **Penetration Test** to check for vulnerabilities on the target system *hopefully in a test environment*

Demo time: exploit the RCE



RCE - **Remote Code Execution** -
is one of the worst vulnerabilities
- *High Critical* -
and needs to be fixed asap

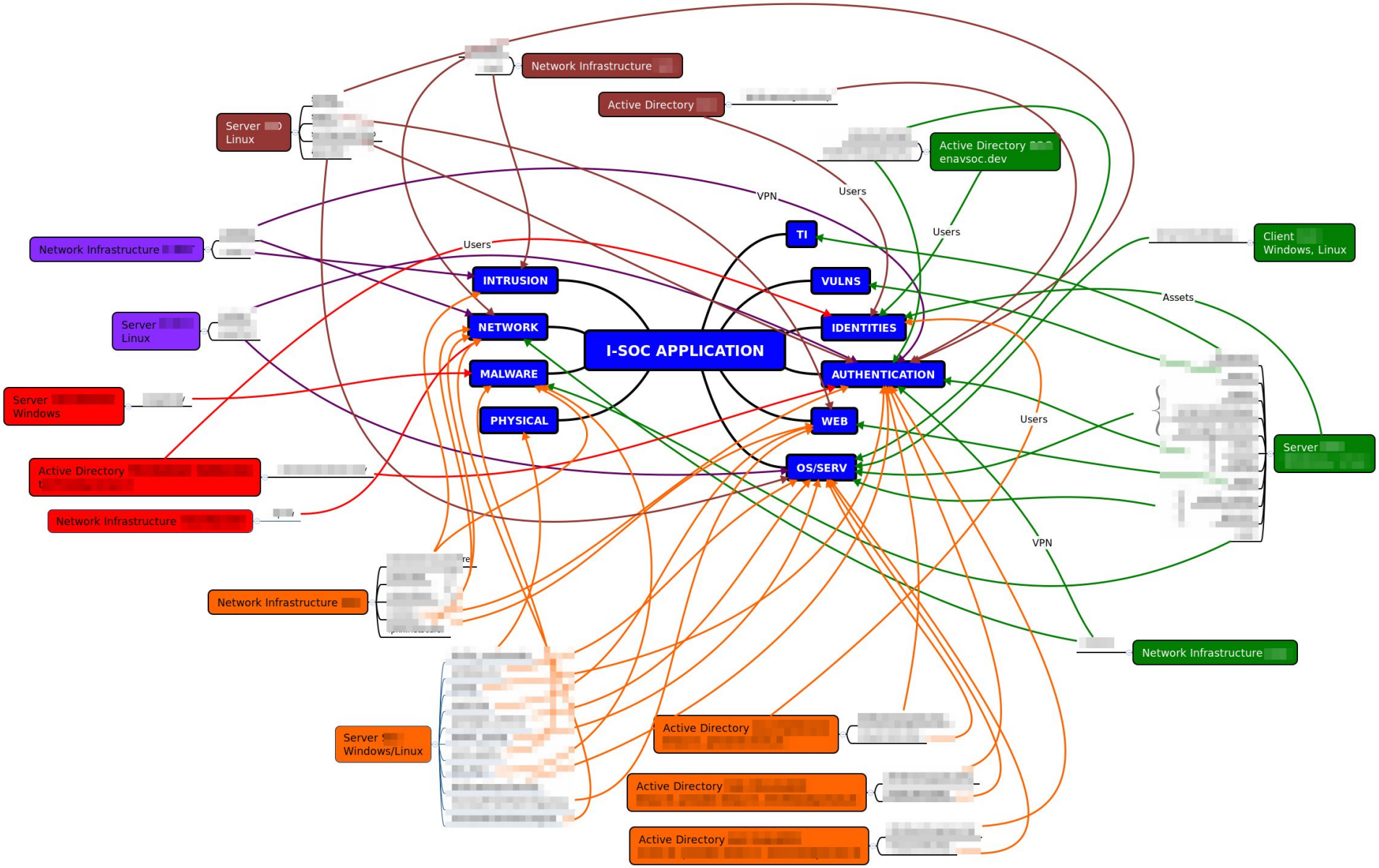
BUT PATCHING AND VALIDATION TAKES TIME

This means that until we fix the issue we are exposed to an **HIGH RISK** and we can

> shutdown the system until we fix
> **mitigate the risk and keep system online**

Mitigate the risk

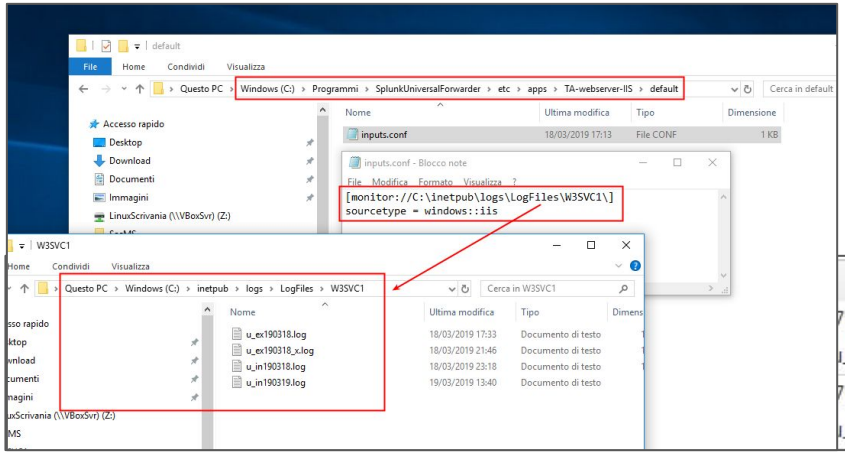
Understand your scenario and collect **relevant logs**

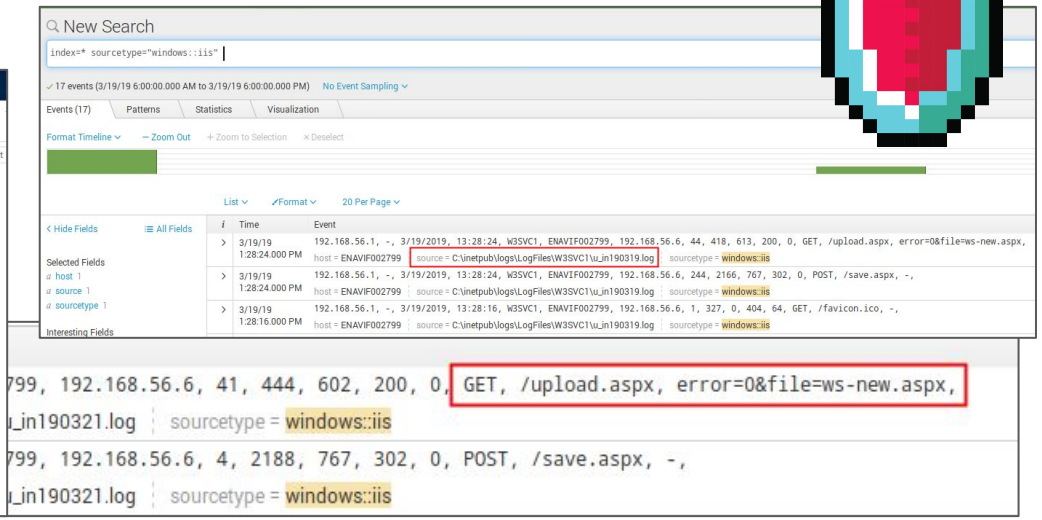


Context: IIS Web server + ASPX on Windows

- **collect** the logs
- send to a central **log collector**
- **analyze logs** while problem happens
- **find a pattern**

Demo time: collect relevant logs

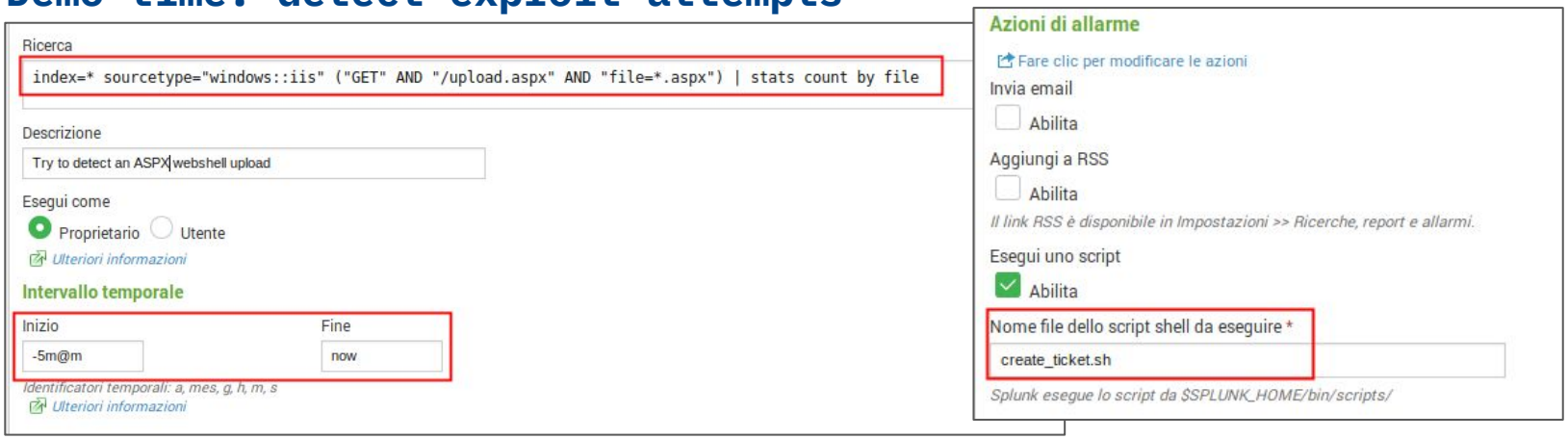


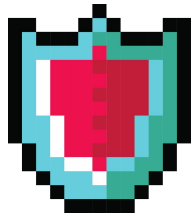


Write your own **detection rule**

- **identify** pattern unique fields
- few false **positive**
- **schedule** a search for the pattern
- create an **alert**
- **risk mitigation**

Demo time: detect exploit attempts





Respond to the incident

Catch it

- > **test the attack**
- > get **notified** on the service desk
- > show attack **details**
- > **react**

Demo time: test the attack

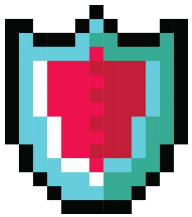
```
--------------
ven 22 mar 2019, 09.00.01, CET
arg[0]: /opt/splunk/etc/apps/CyberSaiyan/bin/scripts/create_ticket.sh
arg[1]: 1
arg[2]: index=* sourcetype="windows::iis" ("GET" AND "/upload.aspx" AND "file=*.aspx") | stats count by file

arg[3]: index=* sourcetype="windows::iis" ("GET" AND "/upload.aspx" AND "file=*.aspx") | stats count by file

arg[4]: CS webshell expolit
arg[5]: Saved Search [CS webshell expolit] number of events(1)
arg[6]: http://CS-SPLUNK:8000/app/CyberSaiyan/@go?sid=scheduler__admin__CyberSaiyan__RMD50499029d17e06047_at_1553241600_6
arg[7]:
arg[8]: /opt/splunk/var/run/splunk/dispatch/scheduler__adm
--------------
executing command /opt/CS/create_ticket.pl...
$VAR1 = {
          'ArticleID' => '51',
          'TicketNumber' => '2019032277000015',
          'TicketID' => '24'
        };
done
--------------
```

Dashboard

New Tickets

My locked tickets (0) | Tickets in My Queues (0) | **All tickets (1)**

		TICKET#	AGE	TITLE
		2019032277000015	1 m	Security event CS webshell expolit on 22/03/2019 09:



At the end

- security is an **enabler** not a blocker
- think secure since the **beginning**
- ask for security **requirements**
  OWASP TOP 10 for Web App
  https://bit.ly/2jdWbXH
- there is **not a magic potion**,
  often security problems are
  a **chain** of missing
  controls/configurations

ROMHACK

CYBERSECURITY CONVENTION

ROMA>28_SET_2019

Link Campus University

RomHack 2019
Call for Papers

www.romhack.io/cfp_en.html

@merlos1977 giovannimellini scubarda.wordpress.com