



Assemblea Nazionale 29.11.2018

LE PERSONE - I DATI - LE TECNOLOGIE

Mobility - Security, Government - Inclusion:
quali sono le sfide e gli scenari che ci attendono?

CYBERSECURITY

Antonio Lioy

Politecnico di Torino



Il Cluster SmartCommunitiesTech (SCT) è parte del sistema italiano Cluster Tecnologici Nazionali

Cybersecurity: rischi ed opportunità

Antonio Lioy

< antonio.lioy @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica



Ucraina, dic'15, 230.000 utenti, 6 ore



Germania, dic'14, attacco cyber ad altoforno



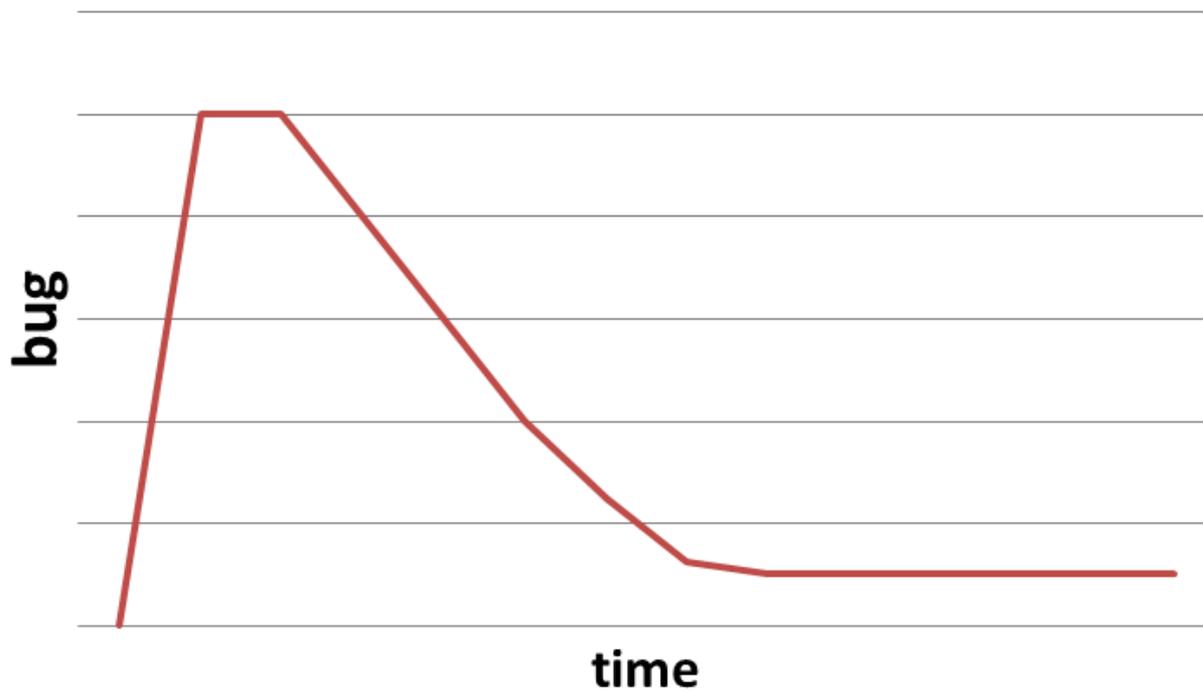
New York, 2013, attacco a diga (fallito per caso)

rapidamente

basso costo

PICK TWO

**alta qualità
(sicurezza)**



2.5-5 bug / function point

~125 bug per 50.000 LOC

3000 progetti, 40 anni, solo 2 con ZERO bug

Increasingly complex sw is being written by programmers who have no training in writing secure code.

*Roadmap for defeating DDOS attacks
(feb-2000, USA)*

- **addestramento degli sviluppatori**
- **analisi automatica del codice sorgente**
- **certificazione? QA?**
- **gestione dei rischi (visto che non possiamo evitarli)**

From: cattivik

To: Gianni Pautasso

Subject: paga!

**Abbiamo le foto di te davanti al PC, paga
10 bitcoin o le diffondiamo ai tuoi amici.**



mese	valore
gen	30.000
feb	34.678
mar	24.221
apr	20.000
mag	18.777

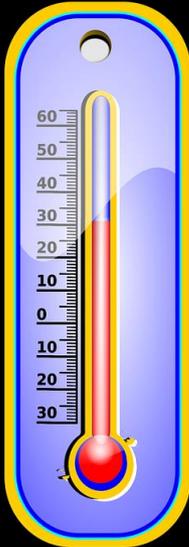
SOC (Security Operations Centre)

SIEM (Security Information & Event Management)



IF { evento-1 } THEN alarm-1
IF { evento-2 } THEN alarm-2
IF { eventi 1, 2, 3, 4 } THEN big-alarm
...

**SOC (Security Operations Centre)
SIEM (Security Information & Event
Management)**



da 0 a 30 in 2s

```
IF { evento-1 } THEN alarm-1  
IF { evento-2 } THEN alarm-2  
IF { eventi 1, 2, 3, 4 } THEN big-alarm  
...
```

**quantità ed eterogeneità dei dati
attacchi (anche fisici) per alterare i dati
... per fare prendere decisioni sbagliate
... per nascondere le tracce degli attacchi**



STUXNET



(BIG PLAYER) SIEM spariranno in pochi anni ...

rimpiazzati da **AI / ML ...**

non general-purpose ma **SECTOR/SYSTEM-SPECIFIC**

La cybersecurity è un problema
(ma anche una risorsa)
TRASVERSALE a tutti i settori

La cybersecurity NON è commodity
(non si compra un tanto al chilo)

Azioni: analisi + gestione dei rischi
DEFENSE-IN-DEPTH
TRUST-BUT-VERIFY

Intelligenza Artificiale + Machine Learning
SPECIFICHE per settore / sistema

The definitive guide for all project managers



What the fuck is security

How to ignore it and deliver your project

O'RELY

Awn Thyme