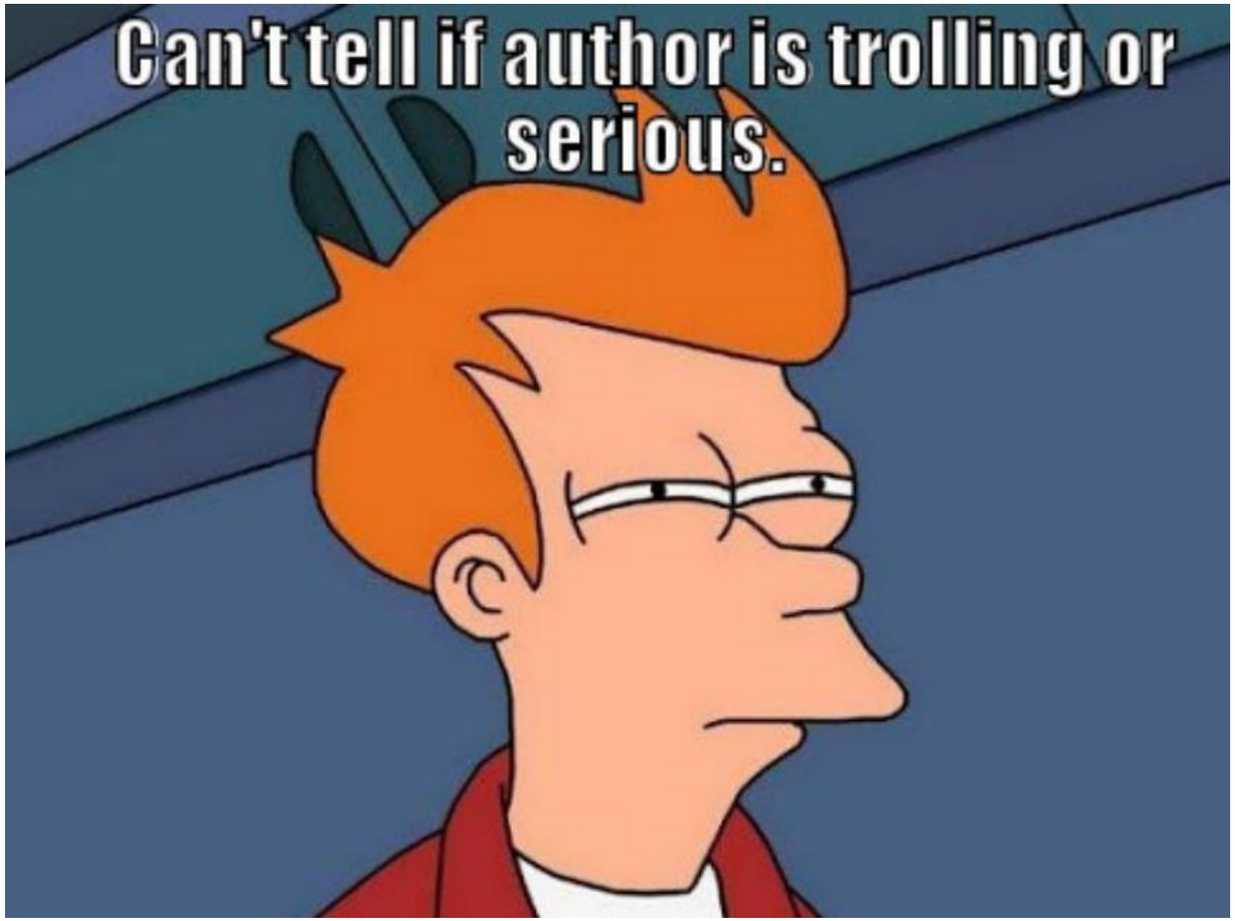
All you need to know to start Security Automation

Lech Lachowicz
Członek Zarządu ds. Profesjonalnego Rozwoju
ISSA Polska

Disclaimer



Who am I:
IT Security specialist with decent background in dev
Global Threat Defense lead responsible for detections, hunting, automation and breach simulation
Big fan of opensource and automation

Who I’m not:
NOT a full time Developer
NOT A DEVOPS

What is it going to be about:
Better and faster SECURITY

Current security operations challenges

Increasing volume and complexity of attacks

67%

of organizations say volume of attacks is increasing

Expanding compliance and obligations

72 hours

to comply with mandatory breach reporting for GPR

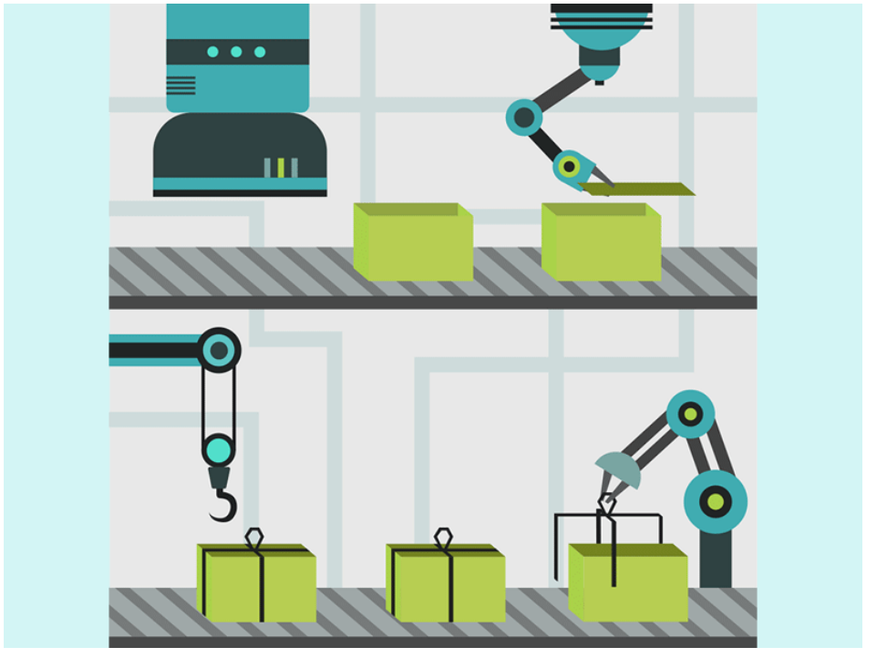
Challenging operational environments

26 or more

security products managed on average by organizations

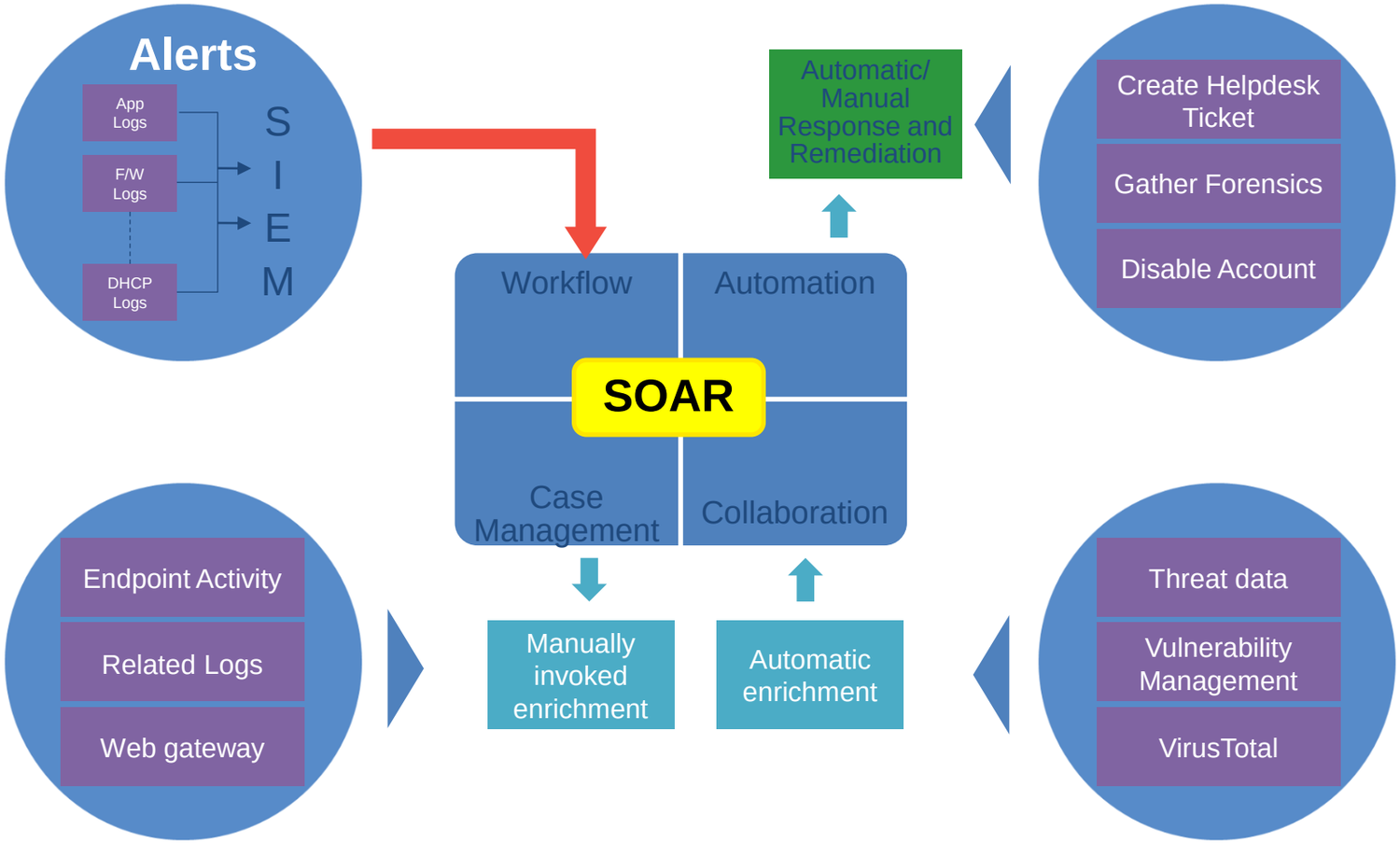
Security Operations need to

- **Minimize** duration and impact of cyber attacks
- **Optimize** SecOps and reduce staff burnout
- **Address** breach reporting requirements and show compliance
- **Maximize** security investments and scale insights across teams



So we automate

Step 0 – Pick the tool



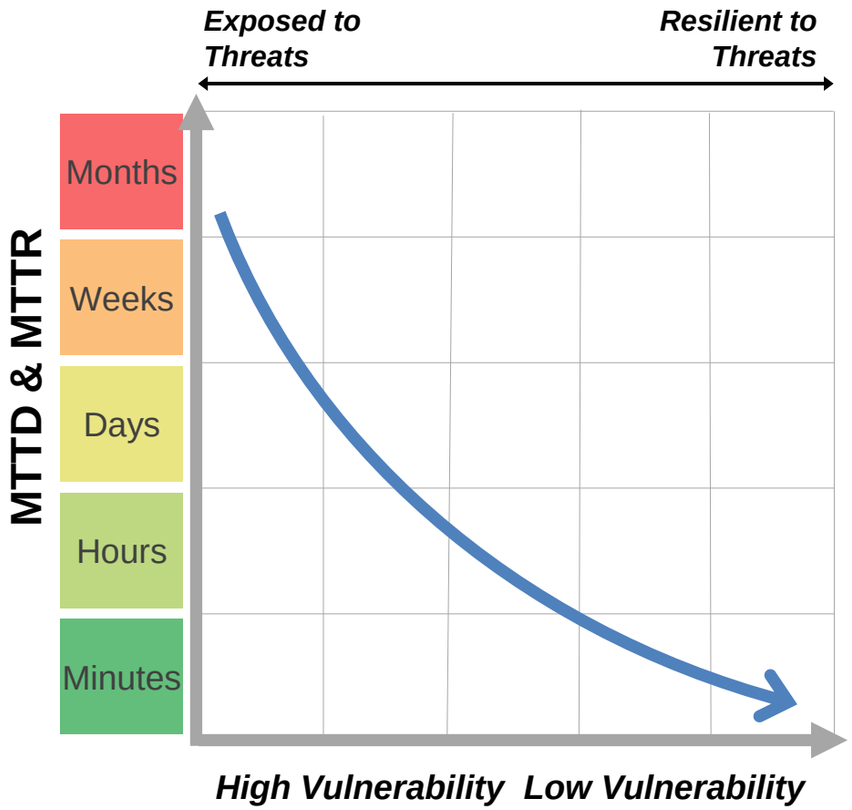
Use a tool thats closest to your ecosystem

If the tool can be part of your ticketing system – its the right one

Make sure you have the talent to maintain the tool – you'll need Python, Javascript, Ruby or something else

Be prepared to scale!

Step 1 – build the measure



MEAN-TIME-TO-DETECT (MTTD)
The average time it takes to recognize a threat requiring further analysis and response efforts

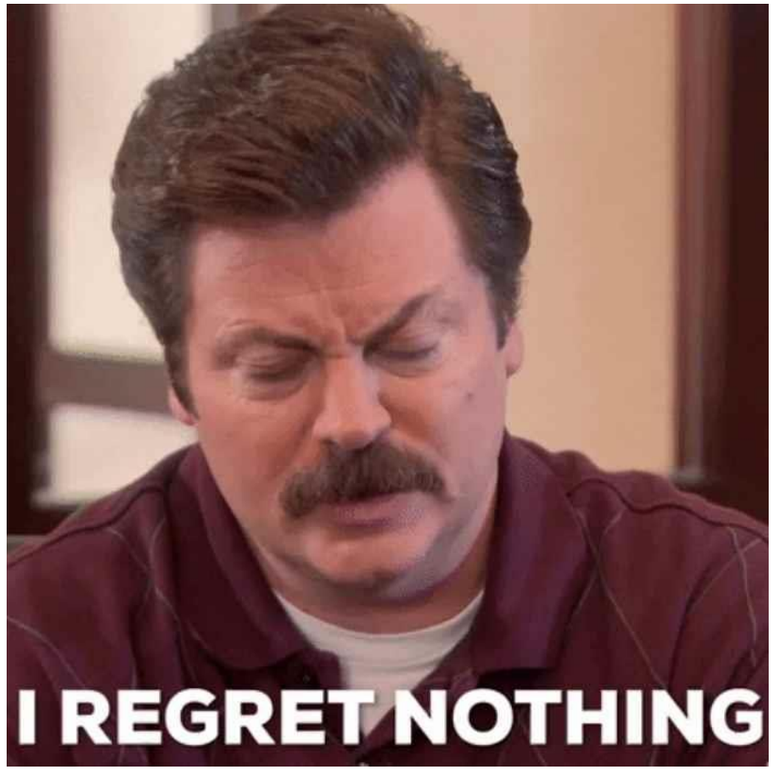
MEAN-TIME-TO-RESPOND (MTTR)
The average time it takes to respond and ultimately resolve the incident

As organizations improve their ability to quickly detect and respond to threats, the risk of experiencing a damaging breach is greatly reduced

Step 2 – Pick the process

#	Action	Current manual time spent (sec)	Current manual time spent - Explanation
A	Have a look at the email content	30	Need to download the email, open it and save a screenshot
B	Collect email header	60	Need to grab the email header then run it through a parsing script/tool and finally attach the data to the ticket
C	Check URL & determination	300	Need to manually check it against VT/OSINT, test it within SafeBrowser and determine if bad. Finally document it as IOC.
D	Check attachment & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident
E	Check downloaded malware & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident

Step 3 – Pick the strategy



Step 4 – Develop the playbook

Keep it simple

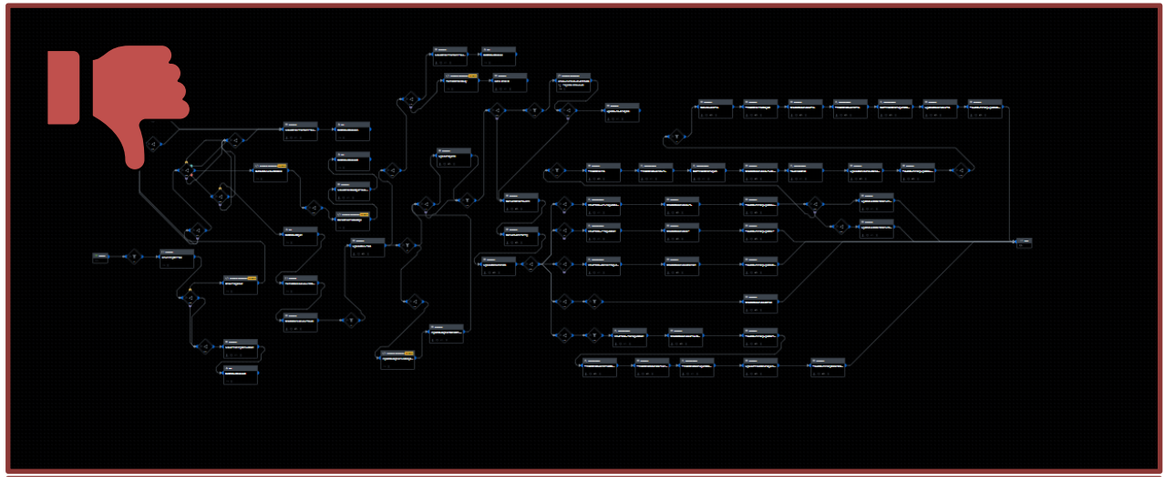
- Break into smaller pieces
- monster playbooks look cool but are hard to maintain

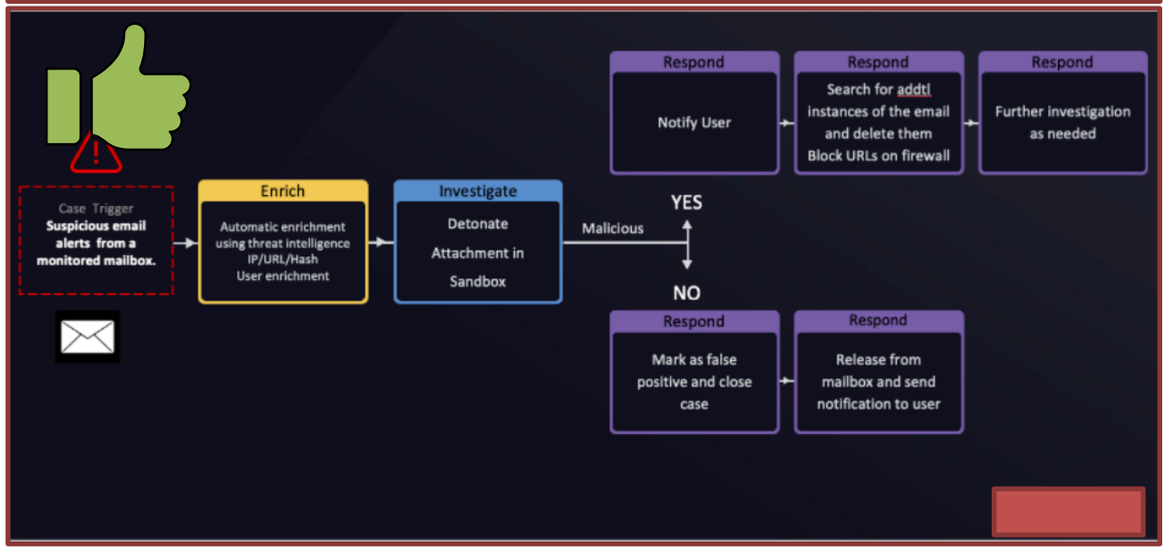
Reuse code

- Make the playbooks modular
- Do not modify built-in code… unless there’s no other choice

Build testing scenarios

- And test error handlers
- this is a MUST, period.





Step 5 – Measure the results

#	Action	Current manual time spent (sec)	Current manual time spent - Explanation	New manual time spent (sec)	New manual time spent - Explanation	Manual time saved (sec)
A	Have a look at the email content	30	Need to download the email, open it and save a screenshot	5	Screenshot already present in the Incident	**25**
B	Collect email header	60	Need to grab the email header then run it through a parsing script/tool and finally attach the data into the ticket	5	Header already displayed in the Incident, with quick spoof check for determination	**55**
C	Check URL & determination	300	Need to manually check it against VT/OSINT, test it within SafeBrowser and determine if bad. Finally document it as IOC.	120	OSINT is automatically gathered, and IOCs created. URL is detonated in Sandbox. Use Sandbox score and OSINT for determination.	**180**
D	Check attachment & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident	60	IOC already created with Sandbox report, for quick determination	**240**
E	Check downloaded malware & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident	60	IOC already created with Sandbox report, for quick determination	**240**

Thats 990sec vs 250sec = **~4 times better**

The benefits

Reliable

Operate 365 days a year!

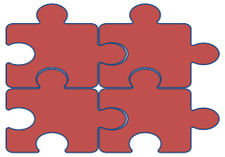
Retention

Freed up human resources for higher value-added tasks

Productivity

Accelerate detection and response

Consistent



Eliminating variations in processes

ROI

There are going to be savings

Fast

Automatically deploy security controls

Audit trail

Fully maintained logs for compliance

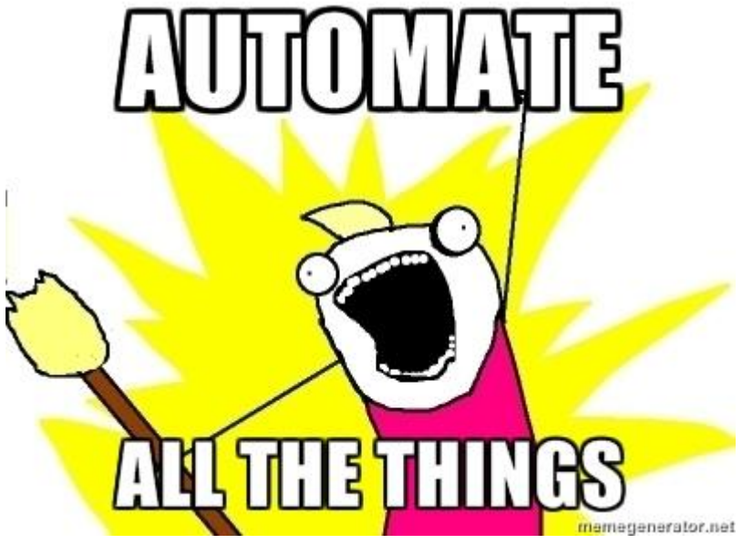
Scalable

Ramp up and down to match demand

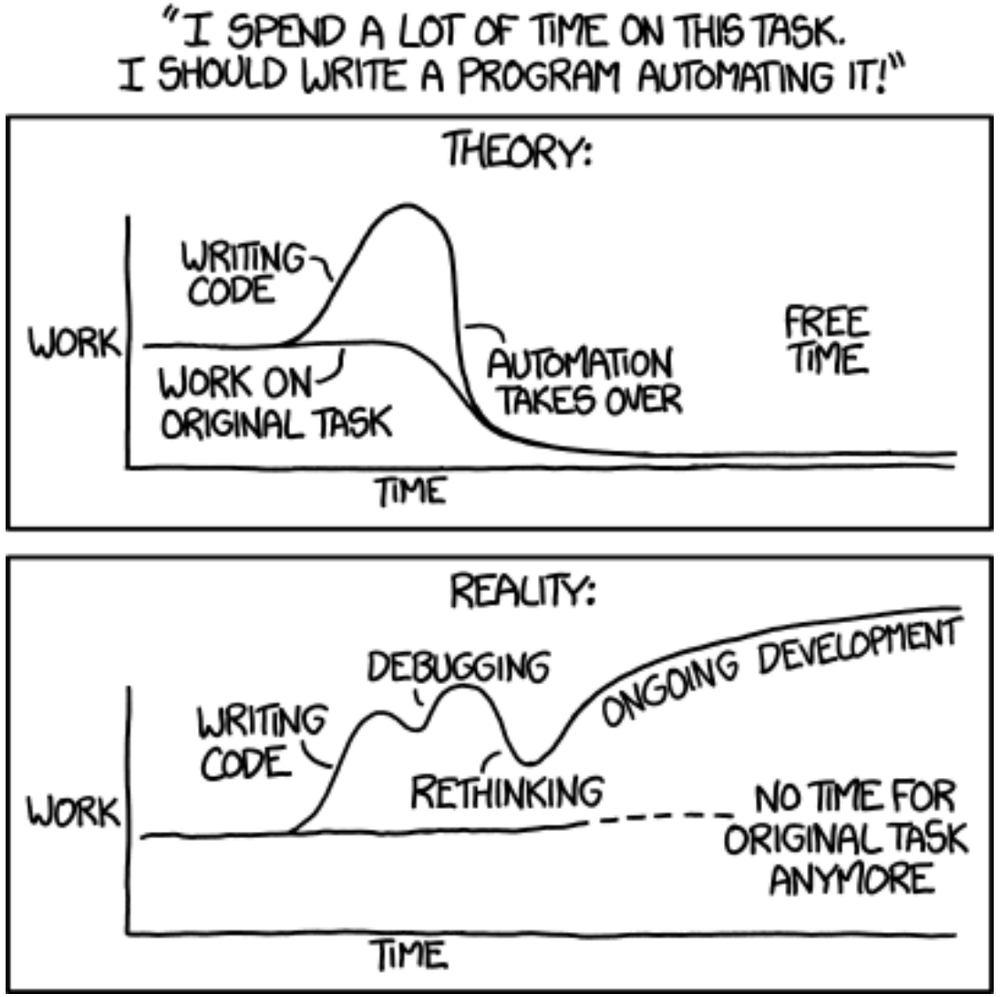
Visibility

Single pane of glass

Watch out!!!


AUTOMATE
ALL THE THINGS
memegenerator.net

?


"I SPEND A LOT OF TIME ON THIS TASK.
I SHOULD WRITE A PROGRAM AUTOMATING IT!"
THEORY:
WORK
WRITING CODE
WORK ON ORIGINAL TASK
AUTOMATION TAKES OVER
FREE TIME
TIME
REALITY:
WORK
WRITING CODE
DEBUGGING
RETHINKING
ONGOING DEVELOPMENT
NO TIME FOR ORIGINAL TASK ANYMORE
TIME

Questions

Thank you

Lech Lachowicz
Mail to: lech.Lachowicz@issa.com.pl