Automation SIG

L. Aaron Kaplan aaron@lo-res.org

David Durvaux David.durvaux@ec.Europa.eu

Benoit Roussille benoit.roussille@ec.Europa.eu

What's the Automation SIG?

- A discussion SIG on all topics Automation and IR/DFIR/CTI/… "*cyber*"
- Exchange Ideas on how to best automate IT security response
- Share successes and failure stories
- Working on a **best practice document on automation**

- Everyone talks about "info sharing". But what do you do with that? → You need automation.
- So let's share **how** we automate!

"[…] Teach a man to fish, and he'll eat for a lifetime"

History / Motivation

- @Workplace: looking at SOAR tools
- Wendy's keynote: CISO asks - "what should we re-use ? Buy? Build?" to automate?

- Questioning ourselves: what are others doing?

- Interesting finding in the SIG: lots of other teams are struggling with the same question
- Hard to wade through the sales-pitches
- → **Let's solve this problem together!**

Mission

- Provide a **forum** where members active in the field of Incidence Response (IR) automation can exchange best practices.
- **Document** our knowledge - in the SIG, write a common best practices document for automation in the the context of incidence response (IR)
- Compile a list of **tools for automation** in IR including their focus areas
- Disseminate **best practices** in term of CSIRT organisation to support automation needs;
- Identifying **ways to provide agile and effective automation**;
- **Cooperate** with other similar regional and global initiatives/groups – e.g. IHAP group, GÉANT TF-CSIRT, other FIRST SIGs…

Status-quo

- We have a confluence document on Automation
- Many chapters are still empty
- We are currently working on the chapters:
  - Use-cases / playbooks:
  - Tools
  - Standards (CACAO, …)
  - Open Source Tools
  - Closed source tools

https://amnesia.first.org/display/AUTO/IT+Security+Automation+Best+Common+Practices

Where we are heading / next steps

- We need more **playbooks** of the **most common use-cases**
- We want to show how these playbooks can be implemented with open source tools
- We will go to vendors and ask them to provide links / input on how to implement these playbooks in their tool

- We need your input

How to participate?

- Sign up to the SIG at portal.first.org
- Or ask the SIG chairs
- You don’t need to be a FIRST member to participate in the SIG.