On the Importance of Cyber-Defense Line Automation

You don’t need a better car, you need to learn how to drive

Enrico Lovat, Florian Hartmann, Philipp Lowack
Who are we?
You don’t need a better car, you need to learn how to drive

What this talk is about

• What we did
• What we learn in the process

What this talk is NOT about

• Cars
• Step-by-step tutorial on how to fix things
• Code
• Vendor bashing

A tool can make you faster. But you need many tools

The “glue” in-between tools is as important as the tools themselves.
Example
Example use case: Malware via email

- How can the user report a suspicious email?
- How do you analyze it?
- Is it a targeted attack or mass malware?
- Did the user click on the attachment?
- Who is the Infosec responsible for the user?
- How do you prevent the attached malware from exfiltrating data from infected machines?
- How can you make sure similar infections are detected?
- How can you prevent other clients from being infected by the same malware?
- …
The old way

- Inbox
  - Reports mails
  - Analyze attachments
- Sandbox
  - Extract potential C&C URLs
- Vetting
  - Virus Total
- SIEM (ProxyLogs)
  - Search for Indicators/URLs
  - Proxy Solution 1
- Ticket Tracker
  - Issue Tickets
  - Analyze Results
- Corporate Employee Directory
- Active Directory
- Investigation
  - Analyze Results
Evolution 1 - Scripts
Scripts: pros and cons

• Scripts allow analysts to perform their tasks faster

• Script written by an analyst can be reused by the other analysts

• Scripting requires good understanding of the tools/service used → only few can edit the scripts

• Each analyst has a different favorite scripting language → hard to script against others’ scripts
Evolution 2 - API
**API: documentation**

**CISO ARE get CISO by GID**

Searches for the given CISO GID.

**URL**

```
GET https://api.cert siemens.com/api/ciso-are/v1.0/ciso-by-gid/<ciso-gid>
```

**GET Parameter**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>required</td>
<td>ciso-gid</td>
<td>string</td>
</tr>
</tbody>
</table>

**Result**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Returns a CISO object or null if no CISO was found.</td>
</tr>
</tbody>
</table>

**Example**

```json
{
  "email": "<email>",
  "gid": "<gid>",
  "jobtitle": "",
  "name": "<name>",
  "orgunit": {
    "are": "",
    "company": "GS IT ISEC CCS",
    "costlocation": "<costlocation>",
    "department": "Corporate Core / Corporate Architectures",
    "CF": "Core BI",
    "location": "MCH P",
    "unit": "GS"
  },
  "scd_link": "<url to scd>",
  "surname": "<surname>"
}
```
API: pros

- **Simplicity**: while not everybody can script against an LDAP server, any developer knows how to query a REST API.

- **Flexibility**: once one REST API for a tool has been developed by an analyst, everybody can script against it using his/her language of preference.

- **Abstraction**: Coding against a REST API allows to easily exchange the “backend”, e.g. replacing a commercial tool with an open source one, as long as it implements the same interface.

- **Authentication**: wrapping the original interface into a custom API allows for better identity management (e.g. handle different authentications).
Global Search

URL: 13d.pp.ru
Tag: Malware
Source: Daily Malware
Type: blacklist
Active?: active
Processed: manual

File/Url: shipping_docs0583945.scr
MD5: 5540fb8490c8491112a01ae577a524
SHA256: 536c0c5a83c9db082a0784dd197af1801dc9f53365c8cebc4e470a2e3a8507
go to CMAP

Value: 13d.pp.ru
Category: Network activity
Type: hostname
Timestamp: 2017-05-19T02:08:24
IDS: True
Comment: 
Event ID: 113273
go to MISP
Details

IP Tools

History
13d.pp.ru
API: Extra pros - Maltego integration
## API: Extra pros - Vetting interface

### Threat Intelligence - Vetting Interface

**Event Name:** Analysis report for email with subject: FedEx parcel #0000287729 delivery problem  
**Event ID:** 630  
**Timestamp:** March 9, 2017, 10:12 p.m.

**Event Tags:**

<table>
<thead>
<tr>
<th>AID</th>
<th>Type</th>
<th>Attributes</th>
<th>Proposed Tags</th>
<th>Data Enrichment</th>
</tr>
</thead>
<tbody>
<tr>
<td>148325</td>
<td>fn</td>
<td>Ground-Label-0000287729.doc.wsf</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148326</td>
<td>fn</td>
<td>a93e7b65a980f646b39271e219674438b8304a275cc12872299e3c92587fe86~</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148327</td>
<td>fn</td>
<td>Ground-Label-0000287729.zip</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148328</td>
<td>md5</td>
<td>0ac33f21c0c27393dc70b80e461d16</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148329</td>
<td>md5</td>
<td>9a90c3cadc85665284a8d4feac5277f</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148330</td>
<td>md5</td>
<td>4f59c0c968717838b9193bad53b47</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148331</td>
<td>sha256</td>
<td>t52b763d3005ba217690c4b72c3a6d5620b10d7e8be6421a5d0174d87ac590</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148332</td>
<td>sha256</td>
<td>7cc7f6eb32645620c8213f568d3ebac50664a1f58a55073d3034da8e68d296247</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>148333</td>
<td>sha256</td>
<td>86e7b6fa9b80f66868cb917e2196744388b8304a275cc12872299e3c92587fe86~</td>
<td>+</td>
<td></td>
</tr>
</tbody>
</table>

**Options:**  
*Add Tag*
Example - revisited
Example: How do we handle it today

Mail reported as spam

Report as SPAM/Malware

In-house developed Outlook plugin.

Selected email is sent (as attachment) to a particular mailbox.
Example: How do we handle it today

Mail reported as spam

MALST (MALware mailingLiST)

Analysis of the email
Example: How do we handle it today

Mail reported as spam

MALST (MALware mailingLiST)

In-house developed tool to monitor inbox and analyze received emails

Set of scripts + WebGUI
Example: How do we handle it today

Mail reported as spam

↓

Analysis of the email

↓

Analysis of email attachment

**CMAP**

View File Information

- **Filename**: Shipment Details_PDF.scr
- **Upload Date**: May 23, 2017, 2:04 p.m.
- **Modified Date**: May 23, 2017, 2:04 p.m.
- **Threat Index**: 2
- **First Uploader**: cert-malwareemailing.bit (Script, CCRT Malware:Mailings)

Quick Links:
- latest analyses (dynamic)
- iSDEEP similarity to other files

Files compiled same year and month:

OpCode Distribution Graph
Example: How do we handle it today

Mail reported as spam

\[\text{Analysis of the email} \rightarrow \text{Analysis of email attachment}\]

### CMAP

- **View File Information**
  - SHA256: f26ba390c0d87f7b0156650363b3b7e9b0cd848163620b79acede4b40f78b6
  - Filename: Shipment Details_PDF.scr
  - Upload Date: May 23, 2017, 2:04 p.m.
  - Modified Date: May 23, 2017, 2:04 p.m.
  - Threat: TLP
  - First Uploader: cert-malware.malwarelist (Script, CERT MalwareList)
  - Quick Links: MALICIOUS (dynamic)

- **Analytics**
  - SISEEP similarity to other files:
    - (Last check: May 24, 2017, 3:22 a.m.)
  - Files compiled same year and month:
  - OpCode Distribution Graph

**Cuckoo sandbox + In-house developed GUI and additional analyses**
Example: How do we handle it today

Mail reported as spam → Analysis of the email → Analysis of email attachment → Manual vetting of analysis results

Threat Intelligence Vetting Interface

Threat Intelligence processing
- Historic search in proxy logs
- Issuing of remediation tickets
- Tracking of remediation status

Threat Intelligence Vetting Interface

Mail reported as spam → Analysis of the email → Analysis of email attachment → Manual vetting of analysis results
Example: How do we handle it today

- Mail reported as spam
- Analysis of the email
- Analysis of email attachment
- Manual vetting of analysis results

**Threat Intelligence Vetting Interface**

It retrieves indicators from sandbox analysis, filters and enriches them, applies tags and push back the changes to TI database.
Example: How do we handle it today

Mail reported as spam
  ↓
Analysis of the email
  ↓
Analysis of email attachment
  ↓
Manual vetting of analysis results
  ↓
Threat intelligence processing

**MANTIS → MISP**

In-house developed tool, supporting STIX/TAXII

New MISP-centric architecture
Example: How do we handle it today

Mail reported as spam
↓
Analysis of the email
↓
Analysis of email attachment
↓
Manual vetting of analysis results
↓
Threat intelligence processing

MANTIS → MISP

Mail reported as spam
↓
Analysis of the email
↓
Analysis of email attachment
↓
Manual vetting of analysis results
↓
Threat intelligence processing
Example: How do we handle it today

Mail reported as spam
  ↓
Analysis of the email
  ↓
Analysis of email attachment
  ↓
Manual vetting of analysis results
  ↓
Threat intelligence processing
  ↓
Historic search in proxy logs
Example: How do we handle it today

Mail reported as spam
Analysis of the email
Analysis of email attachment
Manual vetting of analysis results
Threat intelligence processing
Historic search in proxy logs
Issuing of remediation tickets

Remediation tickets
In-house developed tool to easily handle creation of remediation tickets

1. Create single Ticket or multiple tickets (CSV)
2. Validate import job and selected tickets
3. Import selected tickets to RT
Example: How do we handle it today

Mail reported as spam
→
Analysis of the email
→
Analysis of email attachment
→
Manual vetting of analysis results
→
Threat intelligence processing
→
Historic search in proxy logs
→
Issuing of remediation tickets
→
Tracking of remediation status

Request Tracker
Opens source ticketing system + many customizations
Evolution 3 – What’s next?
What's next?

- Mail DB
  - Reports mails
  - Analyze attachments

- Sandbox
  - Extract potential C&C URLs

- Vetting Tool
  - Reputation Services
  - Virus Total
  - Store and cross-ref. Indicators/URLs
  - Central blacklist
  - Proxy Solution 1
  - Proxy Solution 2

- Ticket Tracker
  - Issue Tickets
  - Search for Indicators/URLs

- Remediation Ticket Tool
  - Analyze Results

- TI Platform
  - Active Directory
  - (C)ISO List
  - Anti Virus

- SIEM
  - Proxy Solution (ProxyLogs)
What’s next?

Manual step
Automated step

TLP:GREEN
What's next?

Central Workflow Engine

- Mail DB
- Ticket Tracker
- Remediation Ticket Tool
- Vetting Tool
- Sandbox
- TI Platform
- SIEM (ProxyLogs)
- Proxy Solution 1
- Proxy Solution 2
- Central blacklist
- Sinkhole
- Corporate Employee Directory
- Active Directory
- (C)ISO List
- Anti Virus
- Virus Total
- Reputation Services

Employees

InfoSec Officers

Analysts
What’s next?

INCIDENT HANDLING PLAYBOOK

In case of “Suspicious email reported”
   Step 1: Analyze email and extract URLs
   Step 2: Analyze sample in Sandbox
   Step 3: If Threat Index > 10 then …
   …
   …
Make it easy!

Use the same interface to access your internal and external services/data sources.
Works for us ≠ Works for you

Every company/institution is different
Lessons learned

More than twice? Script it!

Optimization accumulates over time!
Lessons learned

Containerize your tools!

Lowers setup overhead in the long run and provides well-documented setup instructions for free.
Standardize your infrastructure!

Try to stick to the same tool stack (programming language, frameworks, libraries).
Manage your user centrally!

Easily offer other stakeholders in your company access to (some of) your tools.
Compromise (sometimes)!

Find a tradeoff between adapting your tools to your processes and vice versa.
DIY but don’t DIY!

Don't (always) implement your own tools, but rather use fitting open-source tools.
Lessons learned

**Make it easy!** Use the same interface to access your internal and external services/data sources.

**Works for us ≠ Works for you!** Every company/institution is different.

**If you have to do it more than twice, script it!** Optimization accumulates over time!

**Containerize your tools!** Lowers setup overhead in the long run and provides well-documented setup instructions for free.

**Standardize your infrastructure!** Try to stick to the same tool stack (programming language, frameworks, libraries).

**Manage your user centrally!** Easily offer other stakeholders in your company access to (some of) your tools.

**Compromise (sometimes)!** Find a tradeoff between adapting your tools to your processes and vice versa.

**Do it yourself but don’t do it yourself!** Don’t (always) implement your own tools, but rather use open-source tools.
Enrico Lovat
Florian Hartmann
Philipp Lowack

Siemens CERT
CT RDA ITS CER-DE
Otto-Hahn-Ring 6
81739 München

enrico.lovat@siemens.com
hartmann.florian@siemens.com
philipp.lowack@siemens.com

cert@siemens.com
https://www.cert.siemens.com