



SIEMENS

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?

SIEMENS

TLP:GREEN

A photograph of a Siemens building facade. The building features a prominent dark blue section with the word "SIEMENS" in large, white, three-dimensional letters. Below this section is a reddish-brown band, and at the bottom is a light blue section with a series of windows. The sky is a clear, bright blue.

SIEMENS

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

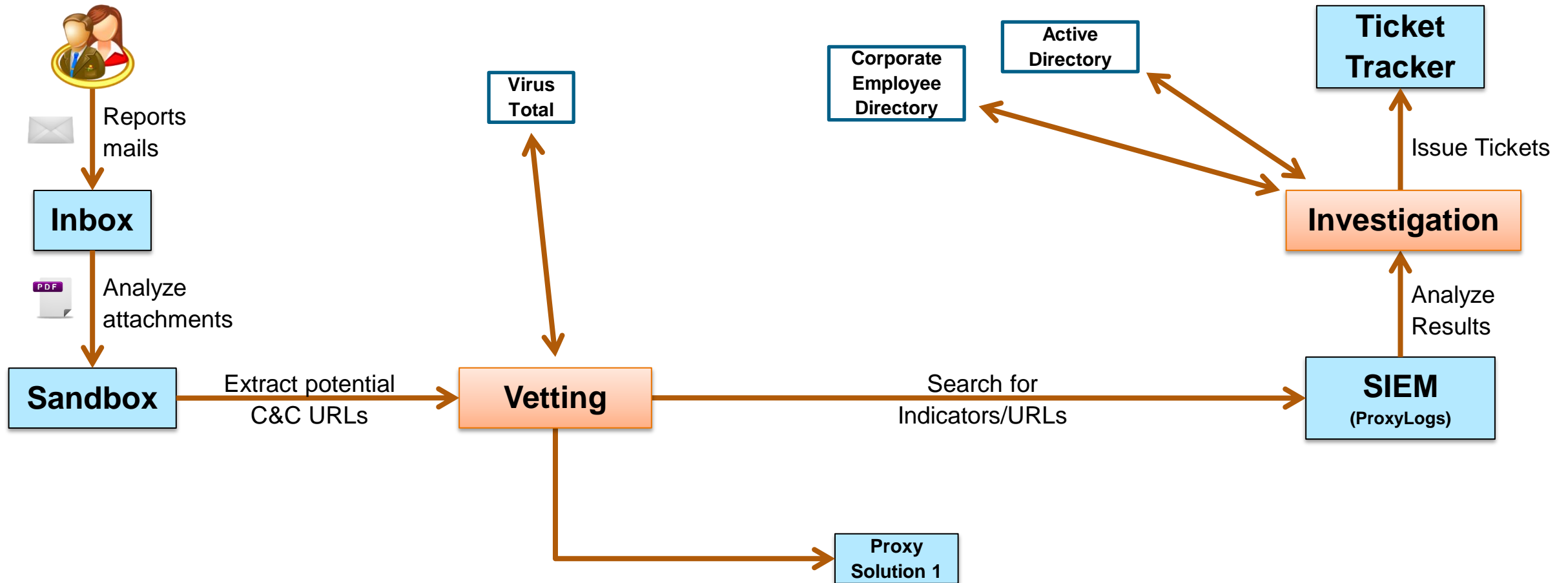
## Example use case: Malware via email

TLP:GREEN



- 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



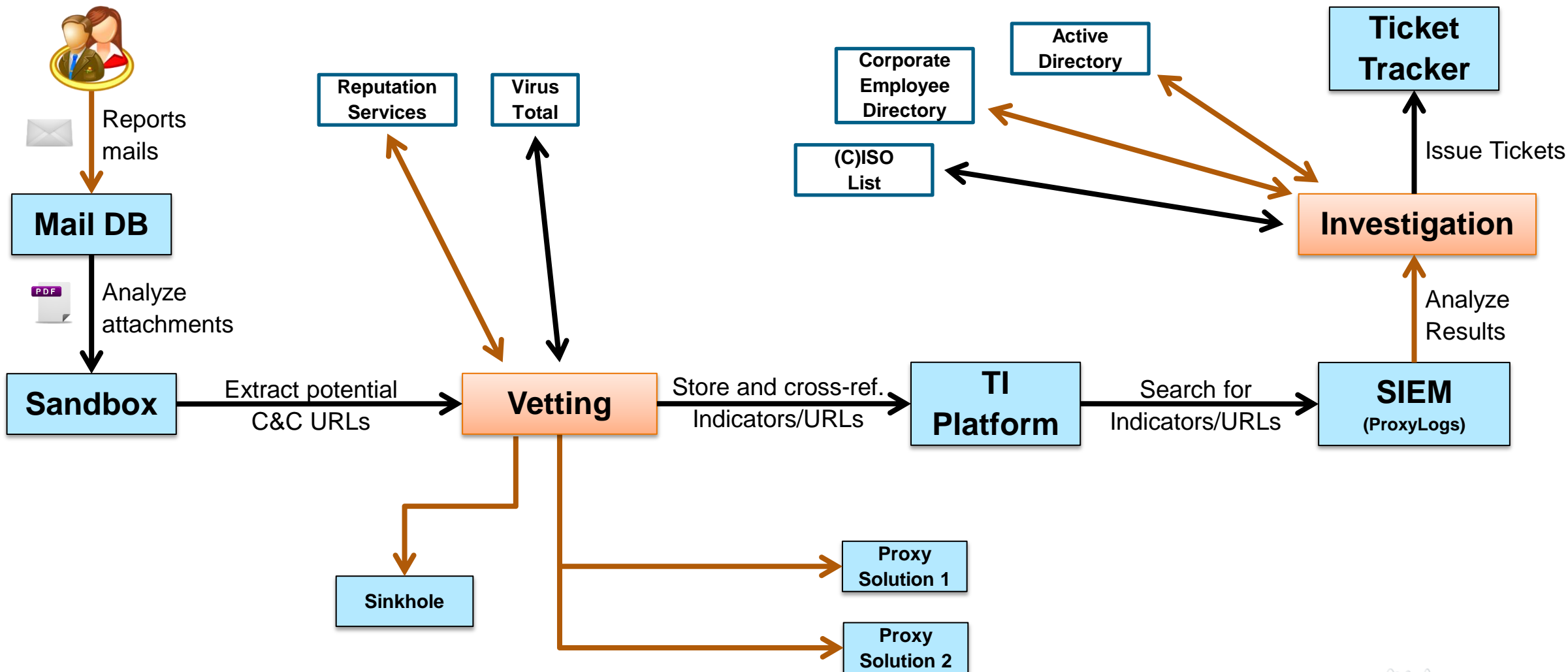
## Evolution 1 - Scripts

# Evolution 1 - Scripts

Manual step →  
Automated step →

SIEMENS

TLP:GREEN






## Scripts: pros and cons

- Scripts allow analysts to perform their tasks **faster**
- Script written by an analyst can be **reused** by the other analysts

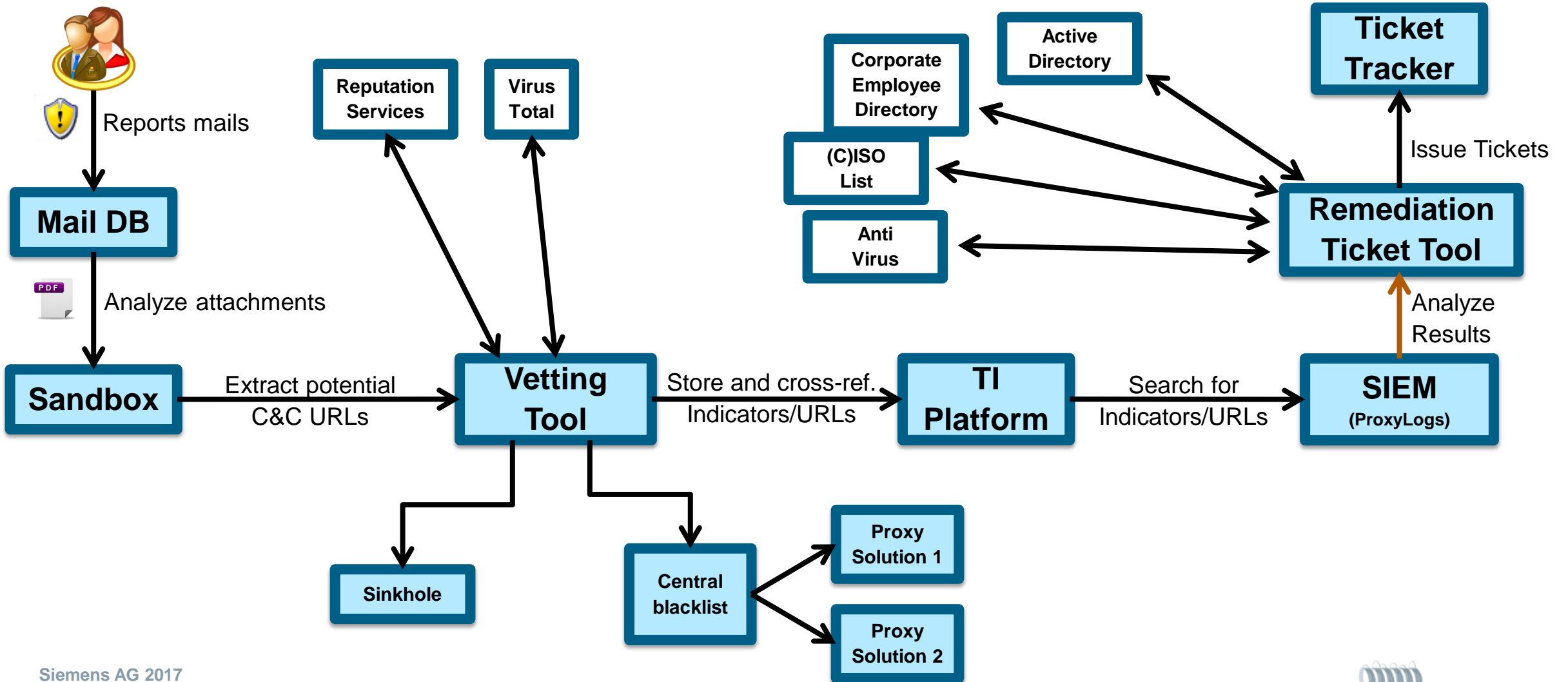


- 
- Scripting requires good understanding of the **tools/service** used → only few can edit the scripts
  - Each analyst has a different favorite scripting **language** → hard to script against others' scripts

## Evolution 2 - API

# Evolution 2 - API

Manual step →  
Automated step →



## API: documentation

Active Directory

AV Portal

Circl

CISO ARE

- get all AREs
- get ARE by ARE
- get AREs by CISO GID
- get all CISOs
- get CISO by GID

CISO NIC

CMAP

DGA Archive

Global Search

Ikarus

IP Tools

MANTIS

NIC

passive DNS

Proxy Blacklist/Whitelist

Request Tracker

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

Name	Type	Description
<b>required</b> ciso-gid	string	The CISO GID to search for, e.g. <input type="text"/>

Result

Status	Description	Example
<b>200</b>	Returns a CISO object or null if no CISO was found.	<a href="#">show example response</a> <pre>{   "email": "&lt;email&gt;",   "gid": "&lt;gid&gt;",   "jobtitle": "",   "name": "&lt;name&gt;",   "orgaunit": {     "are": "",     "company": "GS IT ISEC CCS",     "costlocation": "&lt;costlocation&gt;",     "department": "Corporate Core / Corpora CF, CoE BI",     "location": "MCH P",     "unit": "GS"   },   "scd_link": "&lt;url to scd&gt;",   "surname": "&lt;surname&gt;" }</pre>

## 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

- Inbox  DGA Archive  Circl pDNS  nslookup

### History

l3d.pp.ru

### Proxy Blacklist / Whitelist

1

URL	Tag	Source	Type	Active?	Processed	
<input type="text" value="l3d.pp.ru"/>	Malware	Daily Malware	blacklist	active	manual	<input type="button" value="Details"/>

### CMAP

1

File / Url	MD5	SHA256	
shipping_docs0583945.scr	<input type="text" value="9540ffb849dc8491112a01ae757aa524"/>	<input type="text" value="536c0c5a83c9db08d82a0784dd197af1801dc8f53365c8cebc4e470a2e3a8607"/>	<input type="button" value="go to CMAP"/>

### MISP

1

Value	Category	Type	Timestamp	IDS	Comment	Event ID	
l3d.pp.ru	Network activity	hostname	2017-05-19T02:08:24	True		113273	<input type="button" value="go to MISP"/> <input type="button" value="Details"/>

### IP Tools

## API: Extra pros - Maltego integration

TLP:GREEN

The screenshot displays the Maltego Chlorine 3.6.1 interface. The main window shows a network graph with nodes of various colors (red, orange, blue, green, yellow, pink, brown) connected by lines. The interface includes a top menu bar with options like Investigate, Manage, View, Organize, Machines, and Collaboration. Below the menu is a toolbar with various icons for actions like Copy, Paste, Delete, and Selection. The main graph area has tabs for Main View, Bubble View, and Entity List. On the right side, there are panels for Detail View and Property View, both showing '<No Selection>' and '<No Properties>' respectively. At the bottom, there is an Output panel.

Legend:

Scanhosts	Host	Sinkhole
Incident	IPv4 Address	CMAP File
Employee	Domain	NIC Information
siemens.AVE vent		

## API: Extra pros - Vetting interface

## Threat Intelligence - Vetting Interface

Search: 

▼ 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:

<input type="checkbox"/>	AID	Type	Attributes	Proposed Tags	Data Enrichment
<input checked="" type="checkbox"/>	148325	filename	Ground-Label-0000287729.doc.wsf	+	
<input type="checkbox"/>	148326	filename	aa5e7b6fa98b0f9646bc9271e219674438b8304a275cc12872299e3c92587fe6~	+	
<input type="checkbox"/>	148327	filename	Ground-Label-0000287729.zip	+	
<input type="checkbox"/>	148328	md5	0ac33f21c8c2793dc704b880eb461d18	+	
<input type="checkbox"/>	148329	md5	9a90c3adc8fc686f284a9d4feac52f3f	+	
<input type="checkbox"/>	148330	md5	4f9d9cc0c968717838b9193bad5a3b47	+	
<input type="checkbox"/>	148331	sha256	f96763d3005ba2176f0c4b72c3ad7d6520b1f0d7e5be6421a5d0174d877ac590	+	
<input type="checkbox"/>	148332	sha256	7ec7fceb3264620c82134fd58d0eabac40604a1f98a58073d034da6e8d298247	+	
<input type="checkbox"/>	148333	sha256	aa5e7b6fa98b0f9646bc9271e219674438b8304a275cc12872299e3c92587fe6	+	

MISP

IPinfo.io

VT

Others

## Details

ID	630
Info	Analysis report for email with subject: FedEx parcel #0000287729 delivery problem
Orgc	ORNAME
Org	MISP
Related Events	[]
Sharing Group ID	0
Threat Level ID	2
Event-Tags	test.vet,
Distribution	2
Galaxy	[]
UUID	58c1c559-8b58-48a9-bcb0-08caac110003

## Options:

[Add Tag..](#)



Example - revisited

## Example: How do we handle it today

TLP:GREEN

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



Analysis of the email

### ***MALST (MALware mailingliST)***

Malware Mailinglist		Home	Browse	Browse by Attachment	Search	About	Contact
<b>eMail Details: 1945458</b>							
<b>Meta Information</b>							<a href="#">download this email</a>
AddedOn	2017-05-24 10:08:18						
ReceivedOn	2017-05-17 09:37:14						
Subject	Fw:5/17/2017 9:37:14 AM						
From	manuela.walther (chopin-chopin@goo.jp)						
To	(wjar1916@gmail.com)						
Mail MD5	26a1edeb341ae67846b00ba0b0fa639c						
Mail SHA256	d5f3192840747223bbe12923769f95de1d94b6f8da4735097e741bc1059c8062						
Text Charset	us-ascii						
Text Size	77						
Text MD5	2725fb232d94b66e23cdf581fc2de809						
Text SHA256	7993c595f905408e198a5a49ceea3a58c622fe11bfd81865fe5607abc625d72						
HTML Charset	us-ascii						
HTML Size	679						
<b>Hyperlink Information</b>							
<a href="http://selfcatering-kerry.com/move.php">http://selfcatering-kerry.com/move.php</a>							
<b>Content Information</b>							
Text Part	<a href="http://selfcatering-kerry.com/move.php">http://selfcatering-kerry.com/move.php</a>						

## Example: How do we handle it today

Mail reported as spam



Analysis of the email

### ***MALST (MALware mailingliST)***

The screenshot shows the MALST web interface. At the top, there is a navigation bar with links: Malware Mailinglist, Home, Browse, Browse by Attachment, Search, About, and Contact. Below the navigation bar, the main content area is titled "Most recent emails". It contains a table with the following columns: AddedOn, ReceivedOn, Details, Subject, From (email), and From (name). The table lists several email entries with their respective dates, subjects, and senders.

AddedOn	ReceivedOn	Details	Subject	From (email)	From (name)
2017-05-24 10:08:19	2017-05-24 09:56:54	<a href="#">details</a>	TfL in High Court dispute with Heathrow over Crossrail fees	railtechnologymagazine@cognitivepublishing.co.uk	Rail Technology Magazine Online
2017-05-24 10:08:19	2017-05-17 09:03:52	<a href="#">details</a>	Copy Of Offer Accepted and Sales Memo - (All Parties - 3 pages)	team@klcsolicitors.co.uk	Conveyancing team
2017-05-24 10:08:18	2017-05-17 09:37:14	<a href="#">details</a>	Fw:5/17/2017 9:37:14 AM	chopin-chopin@goo.jp	manuela.walther
2017-05-24 10:08:18	2017-05-17 09:37:14	<a href="#">details</a>	Fw:5/17/2017 9:37:14 AM	chopin-chopin@goo.jp	davidlamont924
2017-05-24	2017-05-24	<a href="#">details</a>	Re:re:Order	info@vinivee.com	Jessica Mark

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

SHA256 f26ba3905cd8279f76bf1566556361b8b27ebcddb4813629bfaaceab4b9873b8

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 24 TLP amber

First Uploader cert-malwaremailinglist (Script, CERT MalwareMailinglist)

Quick Links [latest analysis \(dynamic\)](#) [latest json report](#) [STIX report](#) [Delete File](#)

Analysis PE Details File Details **Additional Information** Virustotal BFK Tags More

MD5 8a4ad68d7852da209ad073bfa48112a6

SHA1 66a702d28dacfb934bf1b5304aa68664f7e354bb

SHA256 f26ba3905cd8279f76bf1566556361b8b27ebcddb4813629bfaaceab4b9873b8

CRC32 87539AB8

SSDeep 1536:uhuf38qBKfQRTJR0fQDG45vUtv5/wQMz+nNiox94aJ7IEKmgikSwlUUxlvz/6Xe:uYx4QRf0vrt5AQqUNio8all2EAT7

Filename(s) Shipment Details\_PDF.scr

File size 184320 bytes

File type PE32 executable (GUI) Intel 80386, for MS Windows

### Analytics

SSDEEP similarity to other files:  
(Last check: May 24, 2017, 3:22 a.m.)

Files compiled same year and month:

#### OpCode Distribution Graph

OpCode Distribution of Sections

## Example: How do we handle it today

Mail reported as spam



Analysis of the email



Analysis of email attachment

### CMAP

The screenshot displays the CMAP web interface. The top navigation bar includes 'CMAP', 'Home', 'Upload', 'Browse', 'Groups', 'Search', and 'Preferences'. A search bar is present with the placeholder text 'search hash or filename'. The main content area is titled 'View File Information' and contains the following details:

- SHA256:** f26ba3905cd8279f76bf1566556361b8b27ebcddb4813629bfaaceab4b9873b8
- 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:** 24
- TLP:** amber
- First Uploader:** cert-malwaremailinglist (Script, CERT MalwareMailinglist)
- Quick Links:** latest analysis (dynamic), latest json report, STIX report, Delete File

On the right side, there is an 'Analytics' section with two expandable items:

- SSDEEP 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

Siemens CERT Utilities Home Login

### Threat Intelligence - Vetting Interface

Search:

▼ 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:

<input type="checkbox"/>	AID	Type	Attributes	Proposed Tags	Data Enrichment
<input checked="" type="checkbox"/>	148325	filename	Ground-Label-0000287729.doc.wsf	+	
<input type="checkbox"/>	148326	filename	aa5e7b6fa98b0f9646bc9271e219674438b8304a275cc12872299e3c92587fe6~	+	
<input type="checkbox"/>	148327	filename	Ground-Label-0000287729.zip	+	
<input type="checkbox"/>	148328	md5	0ac33f21c8c2793dc704b880eb461d18	+	
<input type="checkbox"/>	148329	md5	9a90c3adc8fc686f284a9d4feac52f3f	+	
<input type="checkbox"/>	148330	md5	4f9d9cc0c968717838b9193bad5a3b47	+	
<input type="checkbox"/>	148331	sha256	f96763d3005ba2176f0c4b72c3ad7d6520b1f0d7e5be6421a5d0174d877ac590	+	
<input type="checkbox"/>	148332	sha256	7ec7fceb3264620c82134fd58d0eabac40604a1f98a58073d034da6e8d298247	+	
<input type="checkbox"/>	148333	sha256	aa5e7b6fa98b0f9646bc9271e219674438b8304a275cc12872299e3c92587fe6	+	
<input type="checkbox"/>	148334	email-dst	service.spe@siemens.com	+	

MISP | IPInfo.io | VT | Others

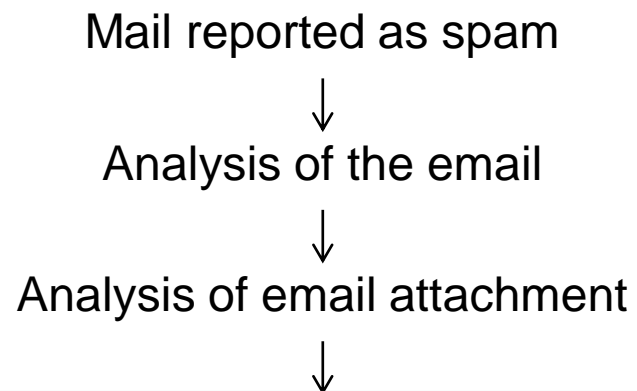
#### Details

ID	630
Info	Analysis report for email with subject: FedEx parcel #0000287729 delivery problem
Orgc	ORGNAME
Org	MISP
Related Events	[]
Sharing Group ID	0
Threat Level ID	2
Event-Tags	test:vet,
Distribution	2
Galaxy	[]
UUID	58c1c559-8b58-48a9-bcb0-08caac110003

Options:  
[Add Tag..](#)

After actions:

## Example: How do we handle it today



Manual vetting of analysis results

### Threat Intelligence Vetting Interface

The screenshot shows the 'Threat Intelligence - Vetting Interface' with a search bar containing 'counter/?a='. Below the search bar, there are two event summaries. The first event is 'Analysis report for email with subject: FedEx parcel #0000287729 delivery problem' (filtered from 13 total entries). The second event is 'Analysis report for email with subject: Fwd: CONFIRM TO INQUIRY AS ATTACHED' (filtered from 9 total entries). Each event summary includes a table with columns for AID, Type, Attributes, Proposed Tags, and Data Enrichment. The first table has one row with AID 148522, Type 'url', and Attributes containing a URL. The second table has one row with AID 148523, Type 'url', and Attributes containing a URL. On the right side, there is a 'Details' panel with tabs for 'MISP', 'IPInfo.io', 'VT', and 'Others'. The 'Details' panel includes fields for ID, Info, Orgc, Org, Related Events, Sharing Group ID, Threat Level ID, Event-Tags, Distribution, and Galaxy.

It retrieves indicators from sandbox analysis, filters and enriches them, applies tags and push back the changes to TI database.



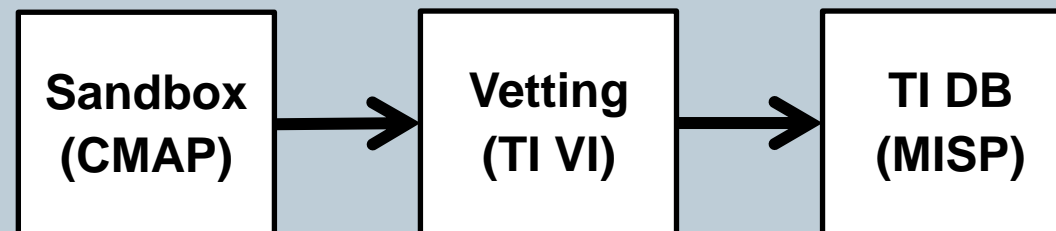
## Example: How do we handle it today



### ***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

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit MISP Enrich

List Events  
Add Event  
Import From MISP Export  
List Attributes  
Search Attributes  
View Proposals  
Events with proposals  
Export  
Automation

#### Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

My Events Org Events Filter

Published	Org	Owner Org	Id	Clusters	Tags	#Attr.	Email
✓		Siemens CERT			tlp:white MALWARE kill-chain:Weaponization kill-chain:Delivery kill-chain:Installation kill-chain:Command and Control	45	
✓		Siemens CERT			tlp:green	6	
✓		Siemens CERT			APT tlp:white diamond-mode:Adversary diamond-mode:Infrastructure	70	
✓		Siemens CERT			tlp:green	1	
✓		Siemens CERT			osint:source-type="blog-post" malware_classification:malware-category="Ransomware"	77	

## Example: How do we handle it today



### Historic log search

CDC Alert & Analysis Interface

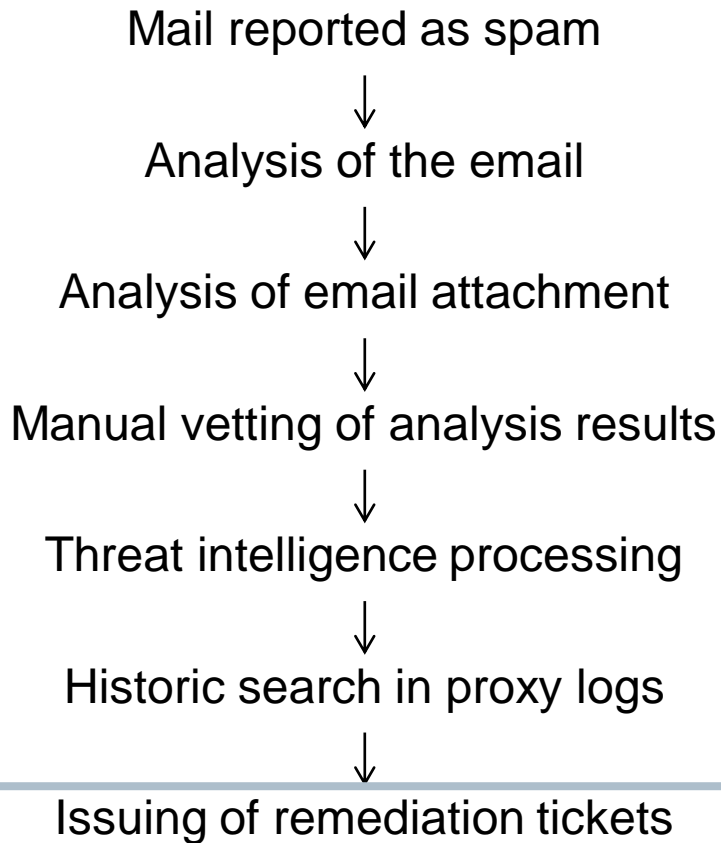
proxy.src\_address = "[REDACTED]"

Proxy Logs  
Got 1000 rows in 261.6738s [259.4995s querying GreenplumEU]

Show 50 entries

start_time	src_address	src_user_name	request_meth
2017-01-24T11:05:17	[REDACTED]	noauth-protocol\$	connect
2017-01-24T11:05:17	[REDACTED]	noauth-protocol\$	connect
2017-01-24T11:05:17	[REDACTED]	noauth-protocol\$	connect
2017-01-24T11:07:19	[REDACTED]	noauth-useragent\$	get
2017-01-24T11:07:19	[REDACTED]	noauth-useragent\$	get

## Example: How do we handle it today



### Remediation tickets

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

1. Create single Ticket or multiple tickets (CSV)

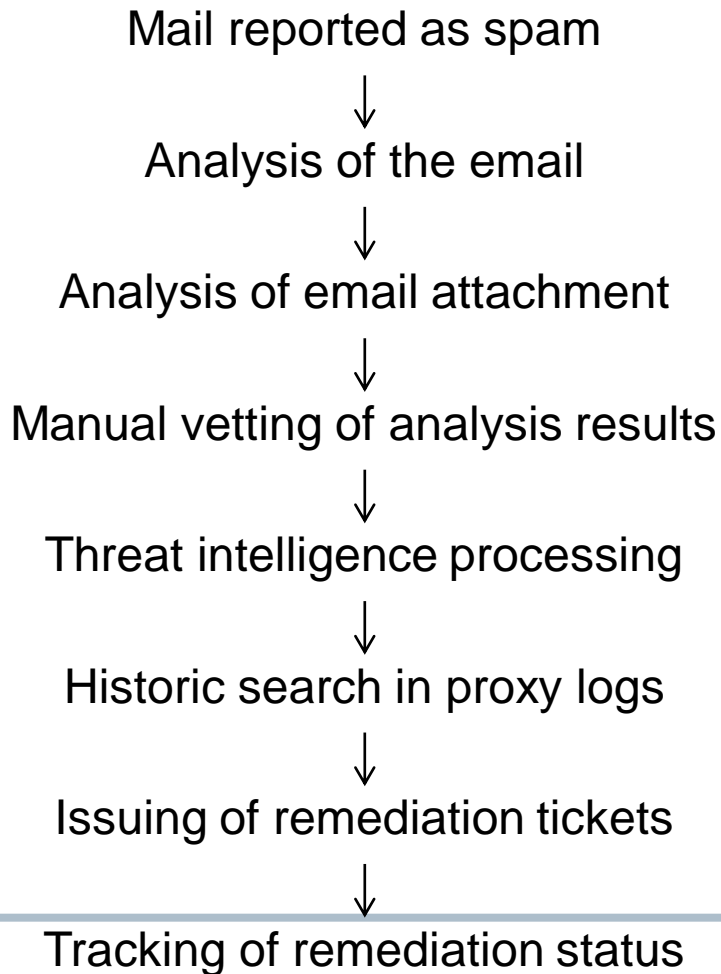
2. validate Import job and selected Tickets

3. import selected Tickets to RT

13 tickets total  
select tickets:  invalid  problematic  valid  hide already imported tickets

	Ticket subject	Evidence	User	CISO	Status	Valid	
<input type="checkbox"/>	Malware Infection of Host				validated	problematic	Details edit delete
<input type="checkbox"/>	Malware Infection of Host				validated	valid	Details edit delete
<input type="checkbox"/>	Malware Infection of Host				validated	valid	Details edit delete
<input type="checkbox"/>	Malware Infection of Host				validated	valid	Details edit delete
<input type="checkbox"/>	Malware Infection of Host				validated	invalid	Details edit delete

## Example: How do we handle it today



### Request Tracker

Opens source ticketing system + many customizations

#25317: Malware Infection of Host "[REDACTED].siemens.net" Goto Ticket...

[View draft mail](#)

Overview

#	Subject	Status	Created	GID	Username	Hostname	OrgUnit	Organization	Company	Location	Country	Incident Number	Owner/Ref
25317	Malware Infection of Host "[REDACTED].siemens.net"	open	94 min ago	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

The Basics

To close this ticket, please set both the system status and the password reset value!

Status: open

Subject: Malware Infection of Host "[REDACTED].siemens.net"

System Status  
Select one value

(no value)

Ticket Description

[REDACTED]

[REDACTED]



[REDACTED]

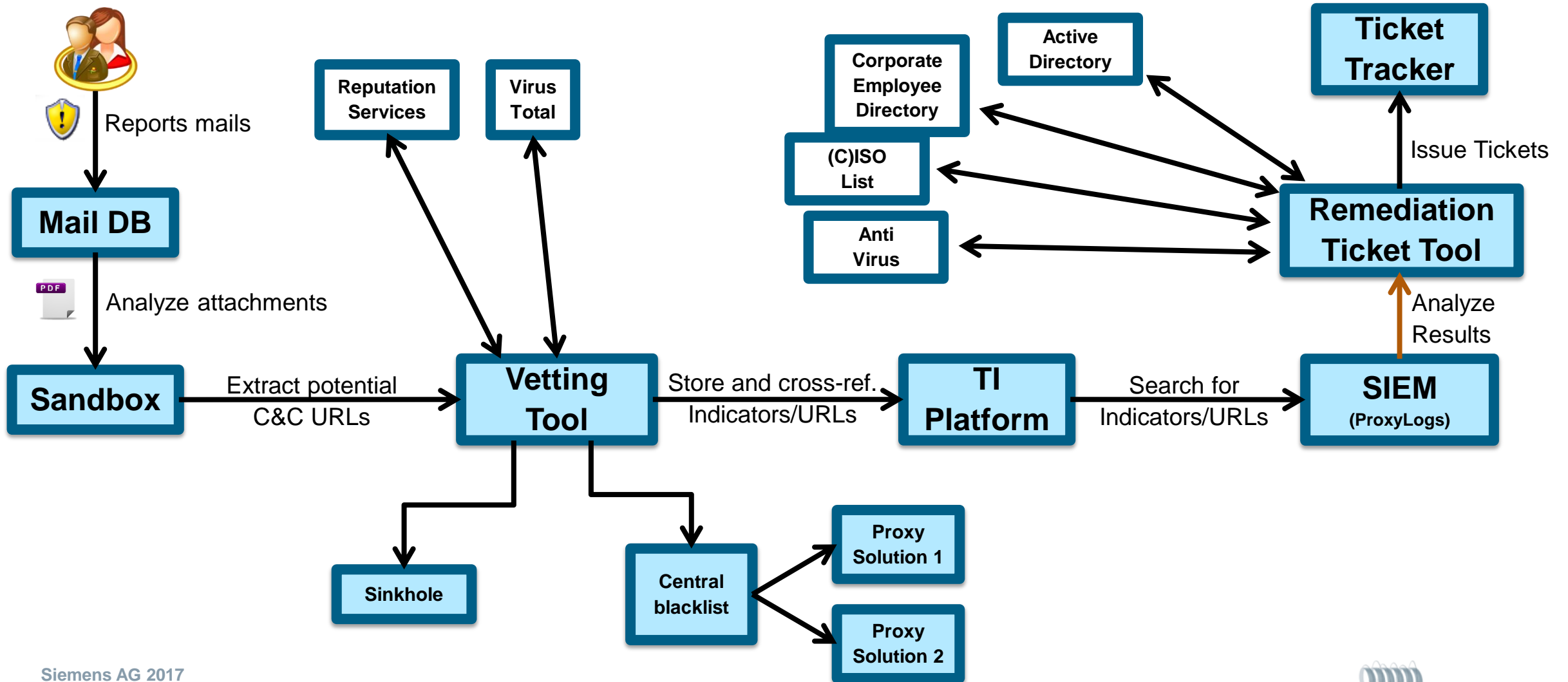
[REDACTED]

[REDACTED]



## Evolution 3 – What's next?

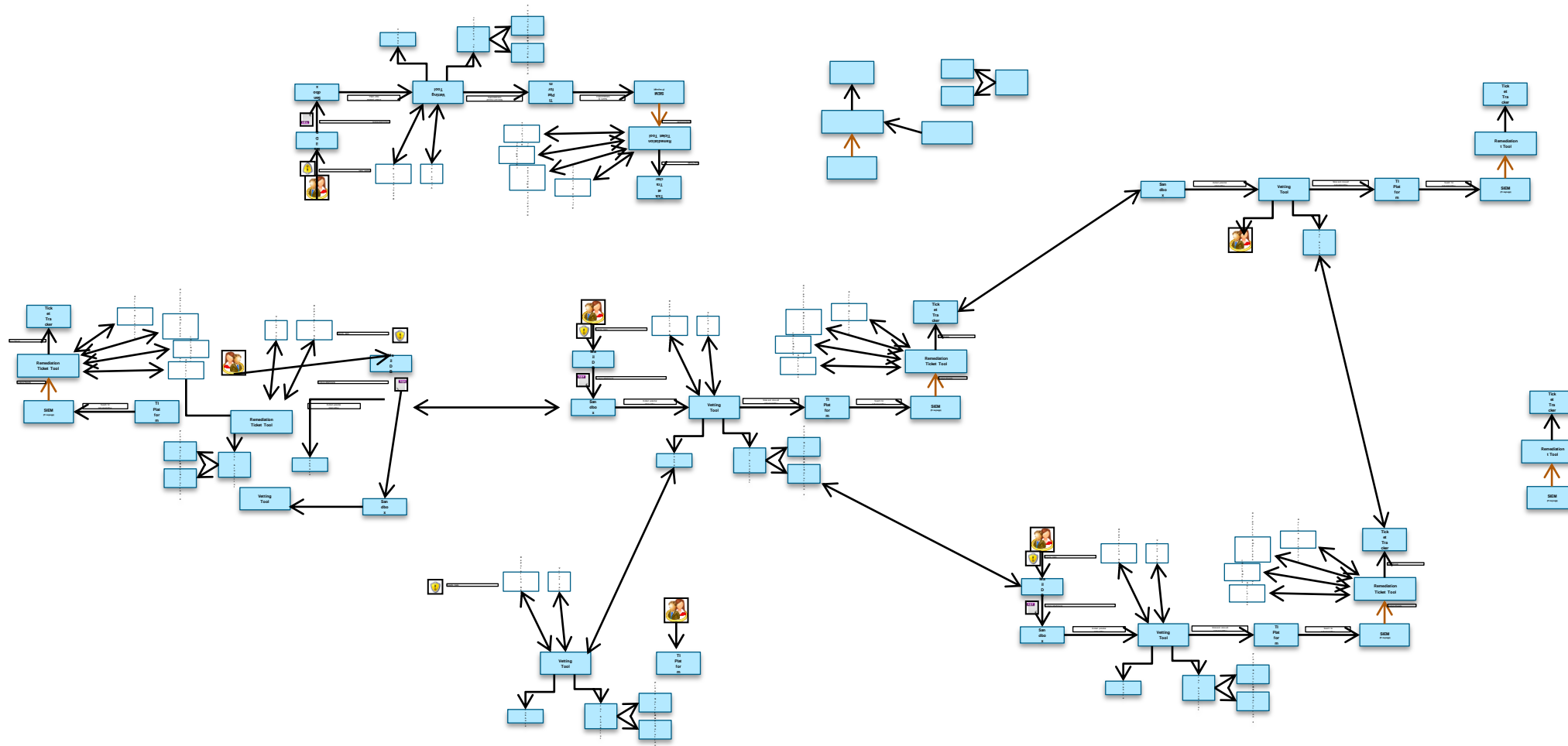
# What's next?

Manual step   
 Automated step 



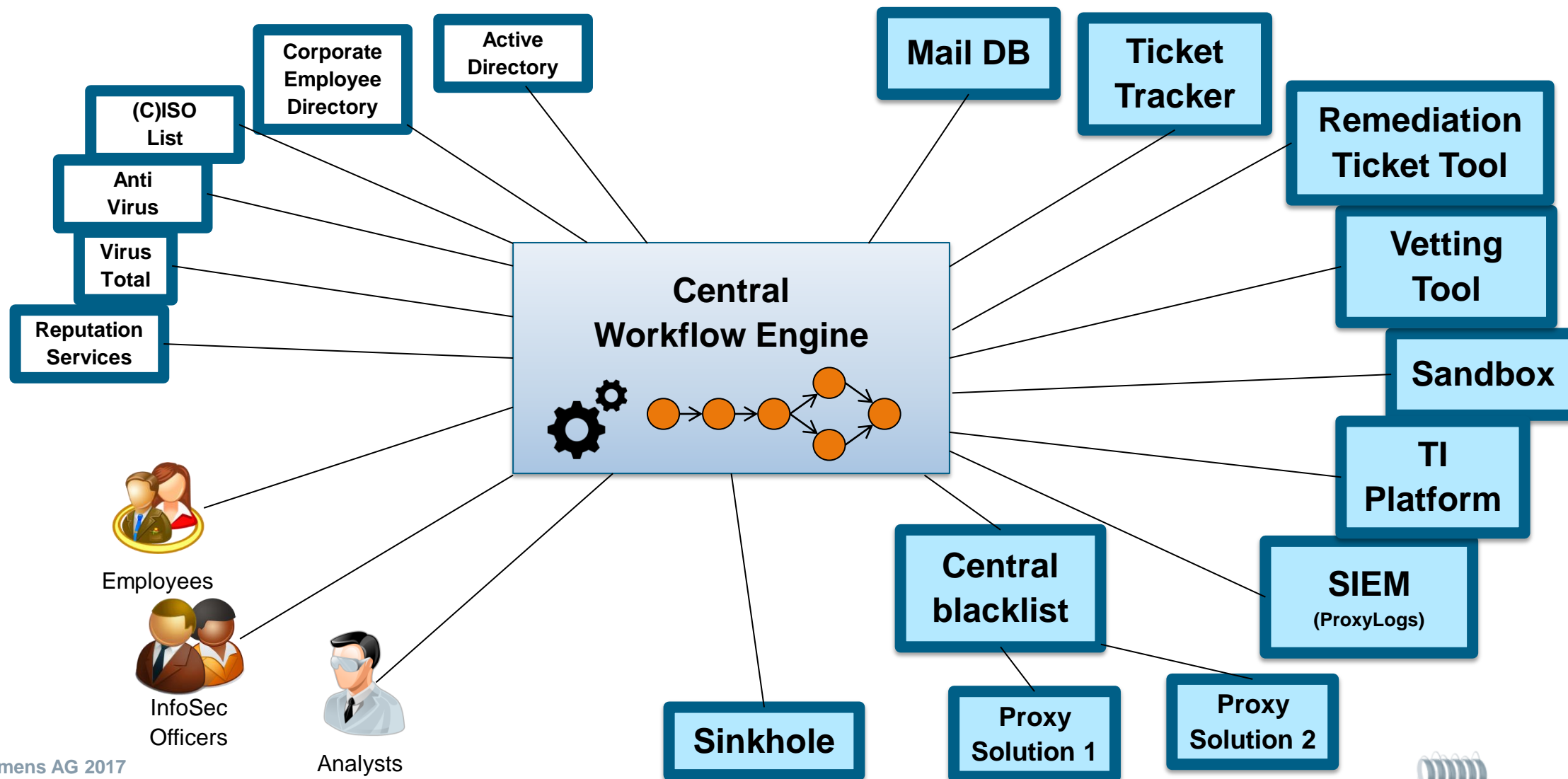
# What's next?

Manual step   
Automated step 





# What's next?



## What's next?

### INCIDENT HANDLING PLAYBOOK

In case of "Suspicious email reported"

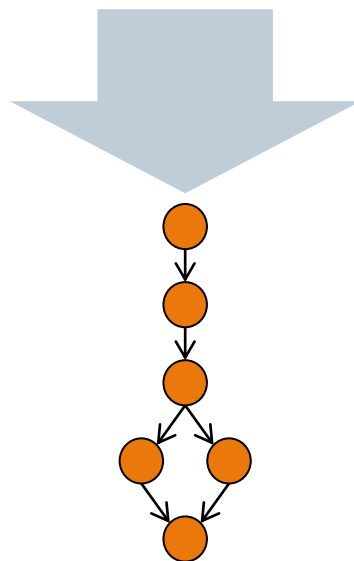
Step 1: Analyze email and extract URLs

Step 2: Analyze sample in Sandbox

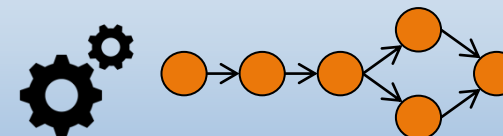
Step 3: If Threat Index > 10 then ...

...

...



### Central Workflow Engine



# Lessons Learned

# Make it easy!

Use the same interface to access your internal and external services/data sources.

# Works for us $\neq$ Works for you

Every company/institution is different

# 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.

# 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.

## Questions?



**Enrico Lovat**  
**Florian Hartmann**  
**Philipp Lowack**

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

[enrico.lovat@siemens.com](mailto:enrico.lovat@siemens.com)

[hartmann.florian@siemens.com](mailto:hartmann.florian@siemens.com)

[philipp.lowack@siemens.com](mailto:philipp.lowack@siemens.com)

[cert@siemens.com](mailto:cert@siemens.com)

<https://www.cert.siemens.com>