Securing Tomorrow's Foundations

Safeguarding critical infrastructure in the Age of NIS2-Directive

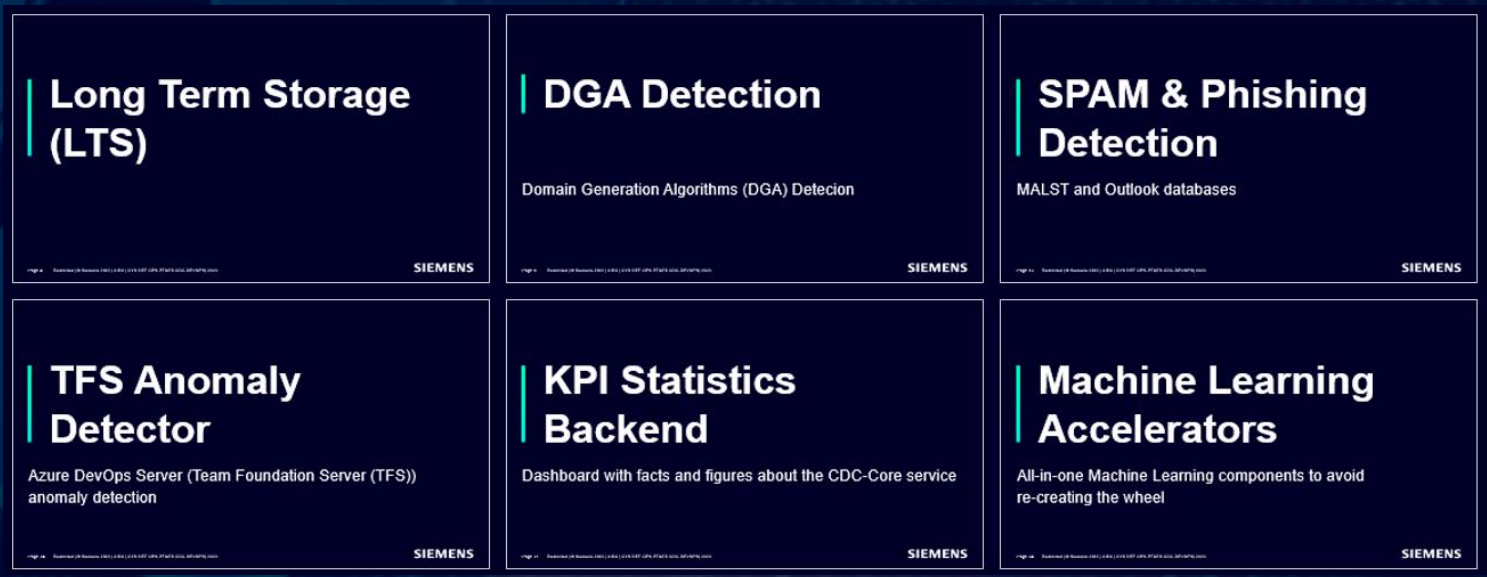
SIEMENS

AI en Zero Trust als hulpmiddelen om de beveiliging van IoT-systemen te verbeteren en te beschermen tegen bedreigingen in een dynamisch en complex landschap

Dedicated Team - AISA

Artificial Intelligence and Security Analytics Team

- Goal: Support CDC with AI/ML capabilities
- Focus: Extend MDR to support AI/ML
- Started in 2018
- Projects Oriented



DGA Detection

Domain Generation Algorithms (DGA) Detecion

SIEMENS

DGA Detection – Motivation

This solution does not scale

www.bad-domain.com

www.dfg45sfd3.com

SIEMENS

DGA Detection
Domain Generation Algorithms

Adversaries use DGAs instead of a static pool of domains. Advantage of making much harder for the defender

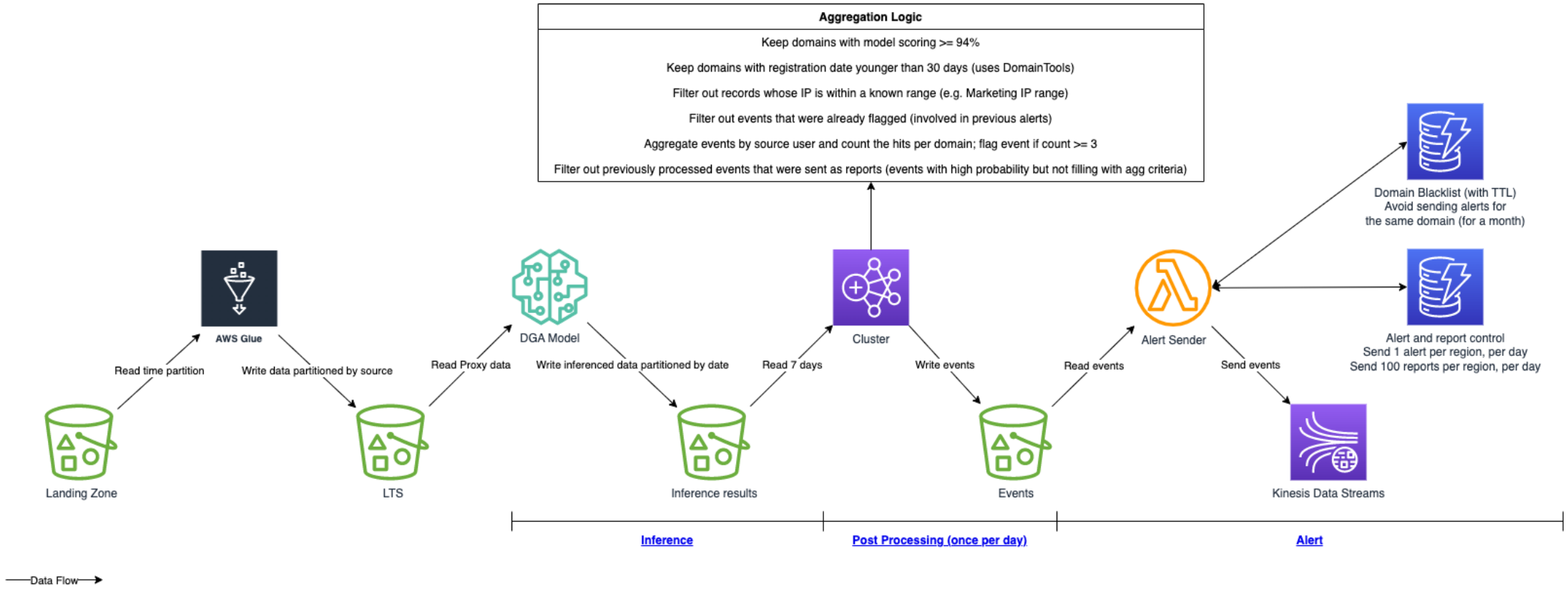
earnestnessbiophysicalohax.com
kwtoestnessbiophysicalohax.com
rvcxestnessbiophysicalohax.com
hjbtestnessbiophysicalohax.com
txmoestnessbiophysicalohax.com

```python
def map_to_lowercase_letter(s):
    return ord('a') + ((s - ord('a')) % 26)

def next_domain(domain):
    dl = [ord(x) for x in list(domain)]
    dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
    dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
    dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
    dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
    return ''.join([chr(x) for x in dl])

seed = 'earnestnessbiophysicalohax.com'
domain = seed
for i in range(5):
    print(domain)
    domain = next_domain(domain)
```

SIEMENS

DGA Detection – Architecture

- Process PROXY data
- Aggregate and find possible malicious domains
- If a user has some requests of potential DGAs associated, it triggers an alert

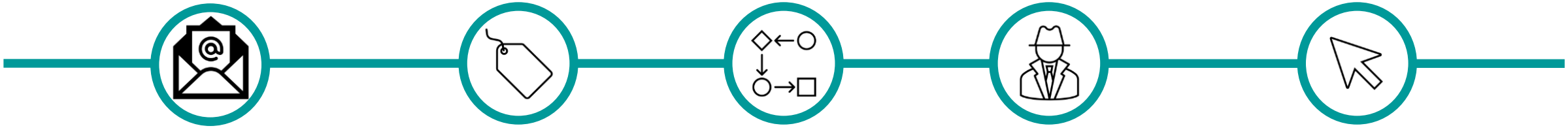


SPAM & Phishing Detection

MALST and Outlook databases

SIEMENS

Phishing Detection within Siemens (without AI)



An email arrives at some destination within Siemens domain

If an employee thinks the email is suspicious, he/she can report it as such in the MS Outlook application

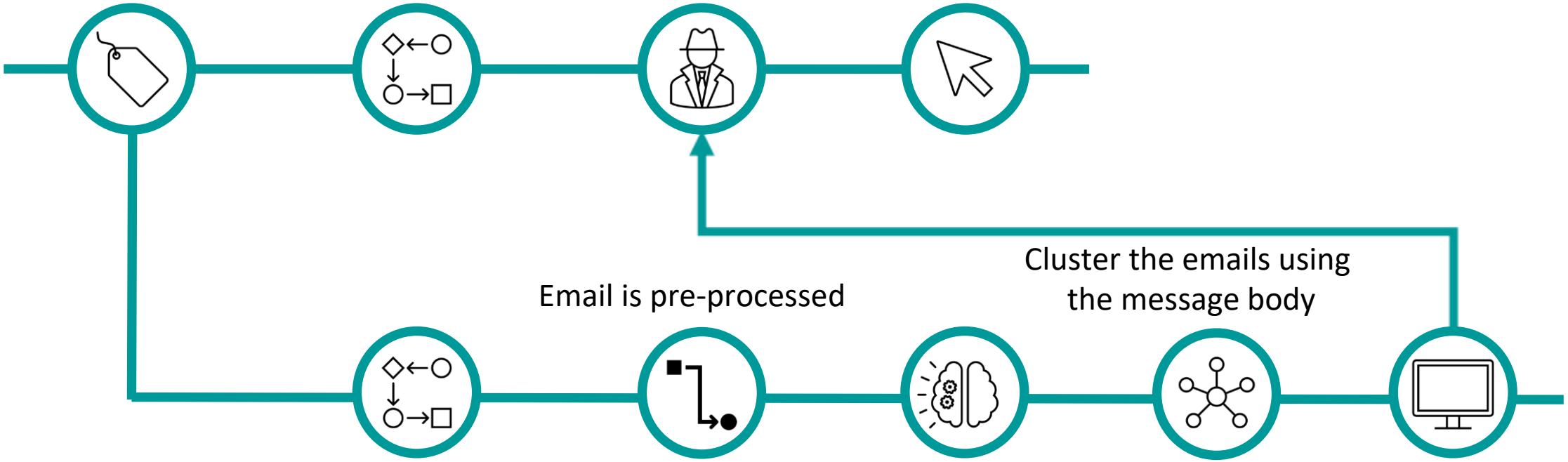
The email goes through a data pipeline which analyses its contents and creates a ticket*

The ticket is triaged by a CDC Analyst

Follow-up actions are triggered

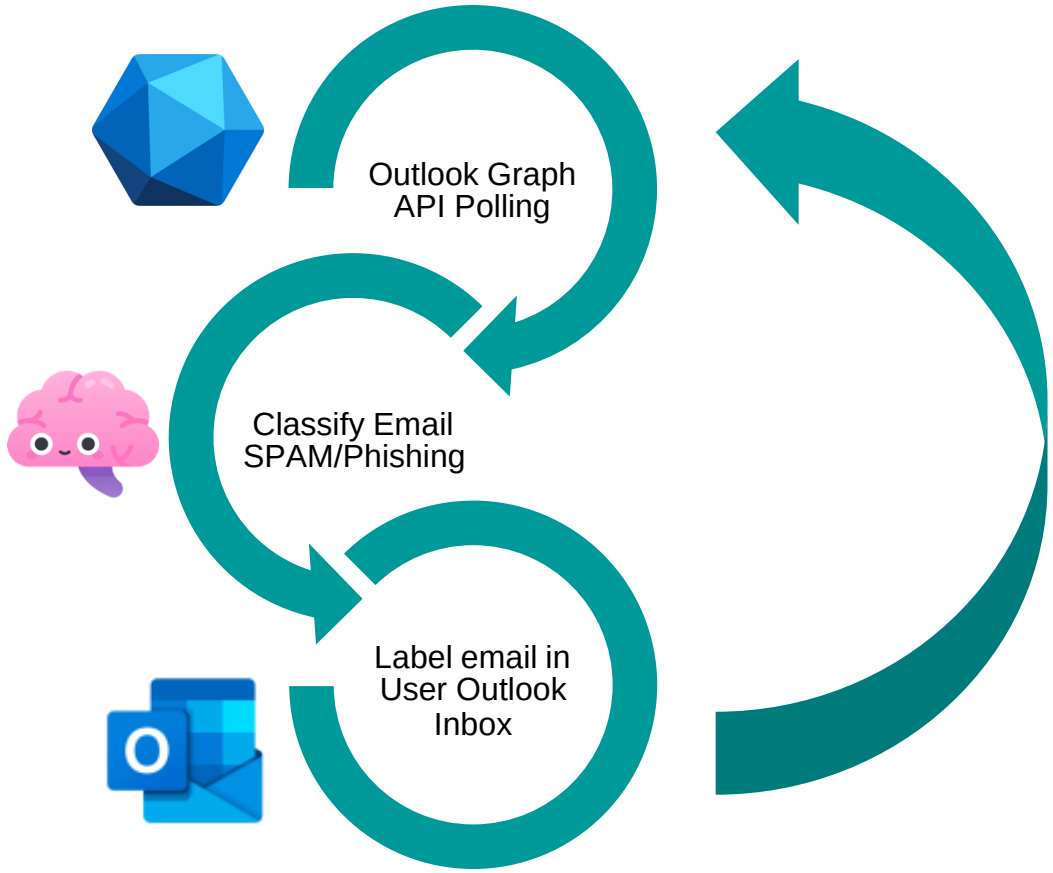
*email body is not used for grouping emails

Phishing Detection within Siemens (with AI)



SIEMENS

Board Members SPAM & Phishing Detection - Workflow



Users sign-up on our service

Their email inbox gets monitored

For every new email, our pipeline is triggered and the email gets labeled accordingly

Users can modify thus providing feedback to the ML Model

SIEMENS

GenAI - Identification of faulty notifications

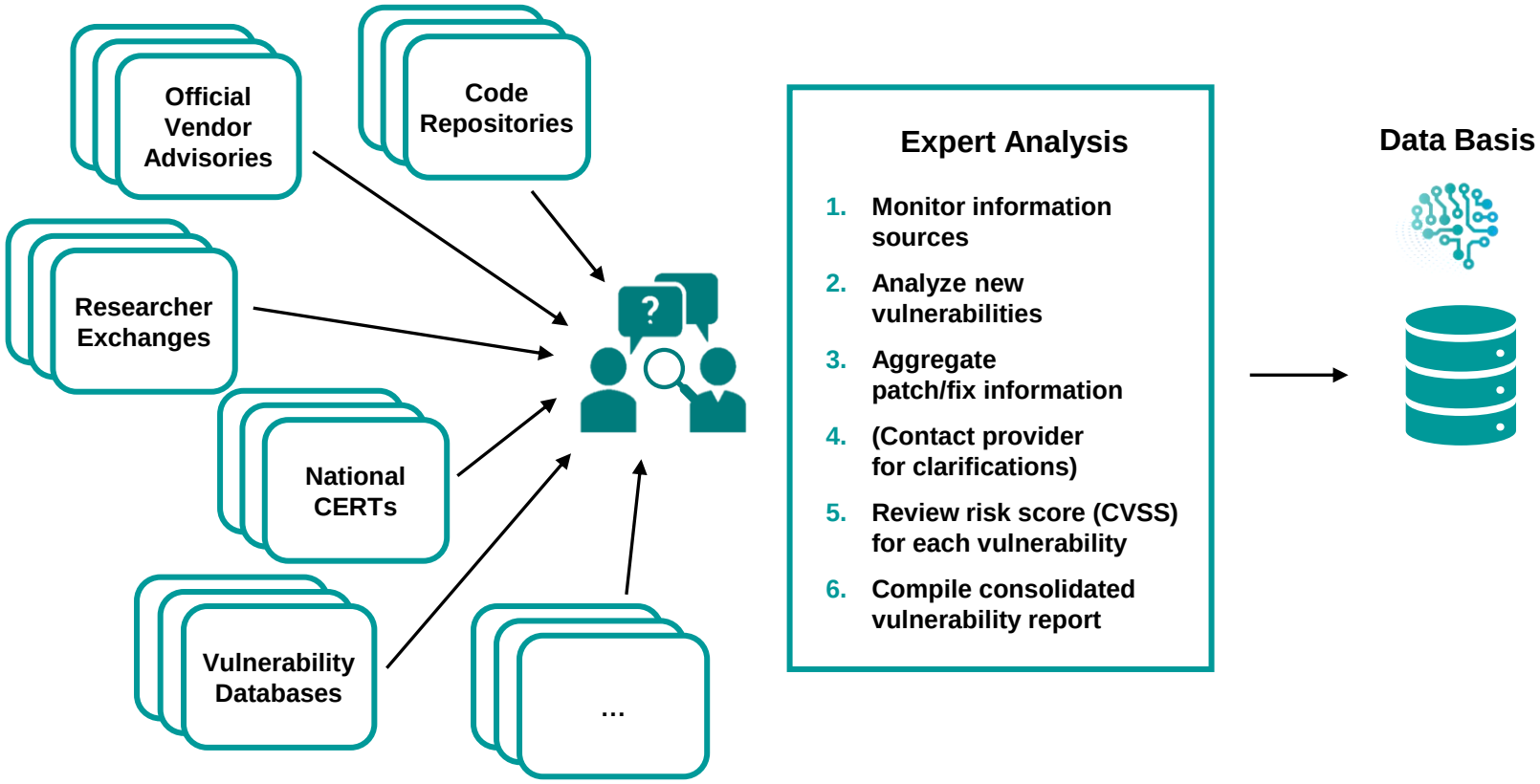
Vilocify - Vulnerability Services

Efficient handling of vulnerabilities

SIEMENS

Vulnerability Intelligence – a sophisticated system

Vilocify Vulnerability Services are based on a **unique monitoring infrastructure** using thousands of information sources, merged by security experts into consumable and actionable information.



Highlights

- **Proven technology** on high Siemens quality standards to detect and patch vulnerabilities
- **Existing internal and external business** with major corporate customers
- **20 years of experience** protecting the world's most critical products and infrastructure

Asset facts:

- **1000+** of vulnerability information sources
- **200,000+ third-party** components in database, constantly growing as any component can be requested
- **1000+ active new users** per month (internal/external)

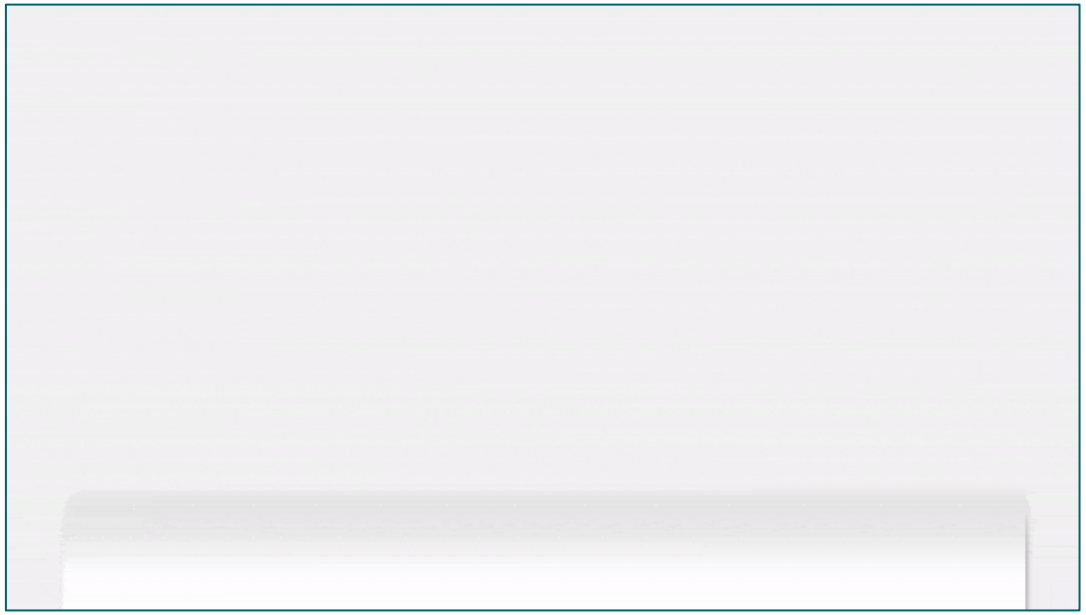
SIEMENS

Vilocify Vulnerability Services – Management Portal Basic

Defining lists of components

Creation of lists of components tailored to customer specific needs by selecting them from our curated catalog or by providing structured data.

Can’t find a component? No problem, we can add it.



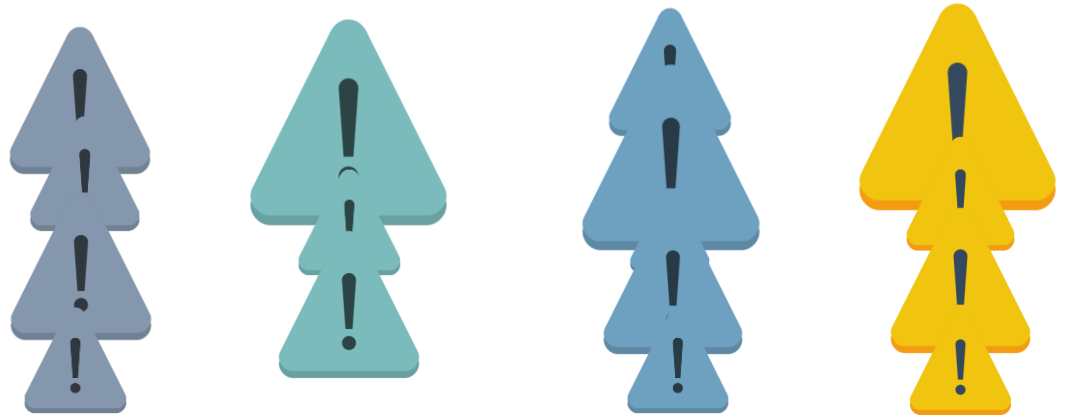
Receiving alerts

Receive alerts through our Management Portal to help you to identify your vulnerabilities and upcoming end-of-life dates.

With our experts' analysis customers have all the necessary information available to quickly take action.

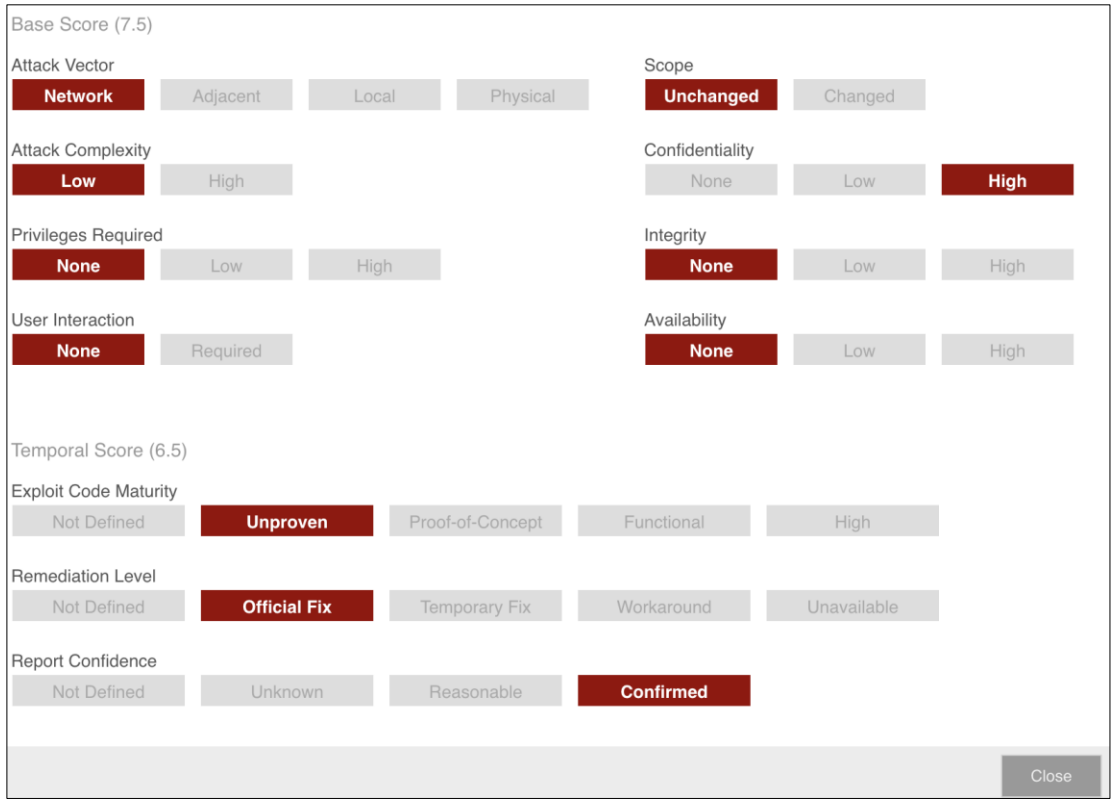
SIEMENS

Generative AI
Enabler for efficient vulnerability detection



Identification of faulty notifications

- Automated review (coherence)
- Relation vuln. description + CVE + CWE
- Report generation
- Ticket triage



Reviews with less human intervention

SIEMENS

Digitalization changes everything

SIEMENS

Securing Tomorrow's Foundations starting Today

Safeguarding critical infrastructure in the Age of NIS2-Directive

SIEMENS