SIG-ISM Vulnerability Assessment

SIG-ISM Vulnerability Assessment

- ★ **GN4-3 WP8 -** Vulnerability Assessment as a Service
- ★ Discussion and feedback from SIG-ISM

Agenda:

Present a bit of our work
Inform of variants options
Get feedback on service structure

Vulnerability Assessment as a service
How could and should a service be made?

What is your current status on the area?

Menti and open dialogue

Do you have a service, how/what? What requirements are important?

Mentimeter

No we do not have a service

In Norway Unit (Directorate) have a kind of assessment in a high level..

It is quite ad hoc now, no structured recurring test

[SURF] We used to, but it was discontinued a few years ago. It's on the roadmap for the SURFsoc as a recurring service though.

We do it internally and we have a penetration testing company who does it for specific services /CSC

I run the EGI Software Vulnerability Group - where we handle vulnerabilities reported which may be relevant to the EGI infrastructure - plus stuff on vulnerability prevention

In Germany was a check (by the universtiy for the military) and a training how to continue these checks locally

ANSWERS FROM MENTI

7

VAaaS - Vulnerability Assessment as a Service (goals)

1. Evaluate products together within NRENs/Organisations

   Wiki / Spread knowledge on findings

2. Cloud offering? Service? Definitions?

3. Integrate with SSO/SAML and API testing
4. Cookbook and integrations with SOC-tools

Different security assessments

- ★ Vulnerability scanning (often automated, “predefined outcome”)
- ★ Penetration testing (often manual, can be physical/social, can change direction)
- ★ System audit (combined auto/manual)
- ★ Security assessment (group or individual report and extends more than technical)
- ★ Risk assessment (group work and helps prioritise changes/mitigation)

Vulnerability assessment - just a step in the middle

0. Patch management, hardening and secure coding
1. Asset inventory
2. Information classification
3. Threat assessment
4. Vulnerability assessment
5. Risk evaluation
6. Risk management/mitigation
7. Verification / pentesting / redteaming
8. Goto 0

Cookbook and integrations with SOC-tools

Getting discovery scans and asset inventory

Creating scanning profiles

Setting what you are allowed to scan (resources and auth)

Agent local scanning ?

For desktop computer and servers

Create local agent, for scanning local software and versions.

Credentials handling

Workshops and community

MOU with Holm Security to get their commercial feed for usage within the Academic sector (work in progress)

Make a webinar and collaboration on Open Source tools

Find talent and get them “new friends” and share information

Development and interaction

REST API

- Initiate scan (ip, profile, resultreceiver)
- Update asset list for scanning profile

Examples: open source/free tools you could use

- Scanning/testing: Nmap, OpenVAS, w3af, burp suite
- Forensics: Caine Linux distro, Yara, Volatility
- Intrusion detection: Surricata
- Information sharing: MISP
- Vulnerability database: vuldb.com
- Checking things: virustotal.com, app.any.run, URLscan, cyberchef, hybrid-analysis.com, capesandbox.com

Products, status and placement our service is using now

Greenbone - one appliance

OpenVAS - everyone

NMAP - everyone, make a guide/cheatsheet

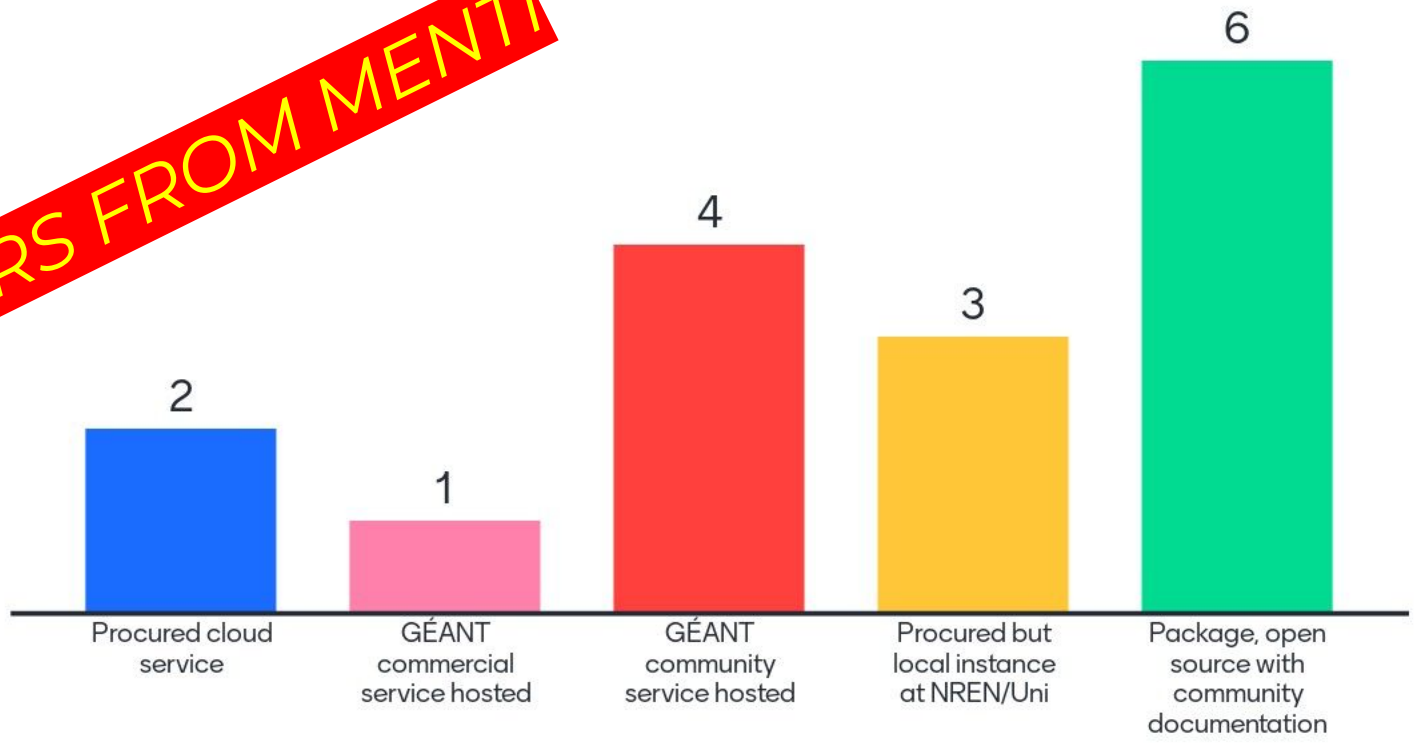
Procurement? Establish a service? Cookbook? Container?

Menti and open dialogue

What Vulnerability services are interesting for GÉANT to work on?

Mentimeter

ANSWERS FROM MENTI



Feedback on work?

Post-Summary: There is interest in packaging and maintaining an opensource version for Vulnerability Assessment and also perhaps extend scope for authenticated scans and code review automation.

Please get in touch to either Alf Moens or David Heed