

# Security & Visma SMB

Practical implementation of a  
Security Program for a  
manufacturer and consumer of  
Cloud Services



# Topics



Purpose of this presentation is to share our experience from Visma Software SMB in improving the security of our cloud services.

## Topics:

- Why security is important to Visma
- Visma Security Program for Service Development and delivery
  - Overview
  - Selected parts
- Results so far
- Demo of Manual Security Testing
- OSAMM
- Agile vs Waterfall, experiences from our deployment
- Threat Modelling

[Espen.Johansen@visma.com](mailto:Espen.Johansen@visma.com)

**Why?**

# Visma Software SMB

ERP for entry-level to mid-size companies for SE, FI, NL, DK and NO

8

Cloud ERP

19

On-prem ERP

10

Payroll/HRM

25

Addons

## Strategic Goals

- Cloud benefits to all small businesses
- Increase productivity of all employees by access to ERP processes
- APP-ification of ERPs
- Data analytics

3.400

MNOK Revenue

41%

Cloud CMRR

600k

Customer contracts

# Why-story



**10K**



**350K**



**1.000K**

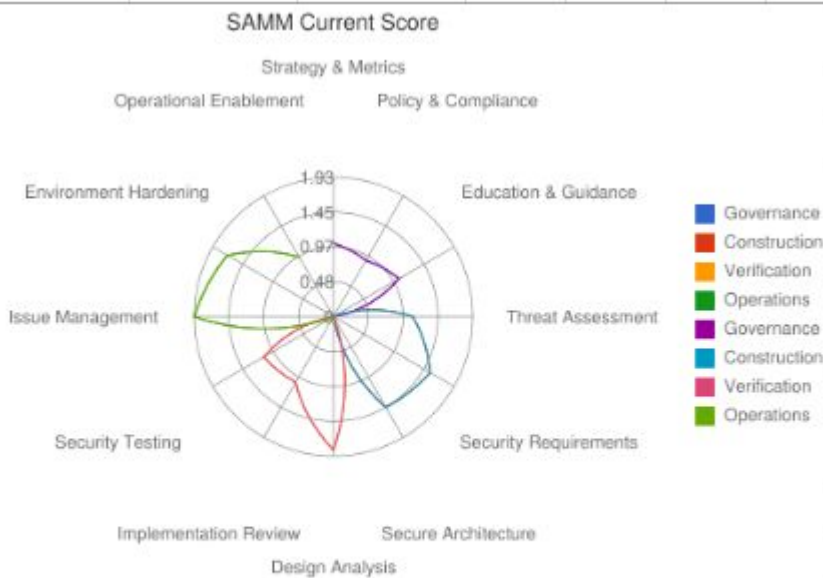
# Security Program

## Selected assumptions for the Security Program:

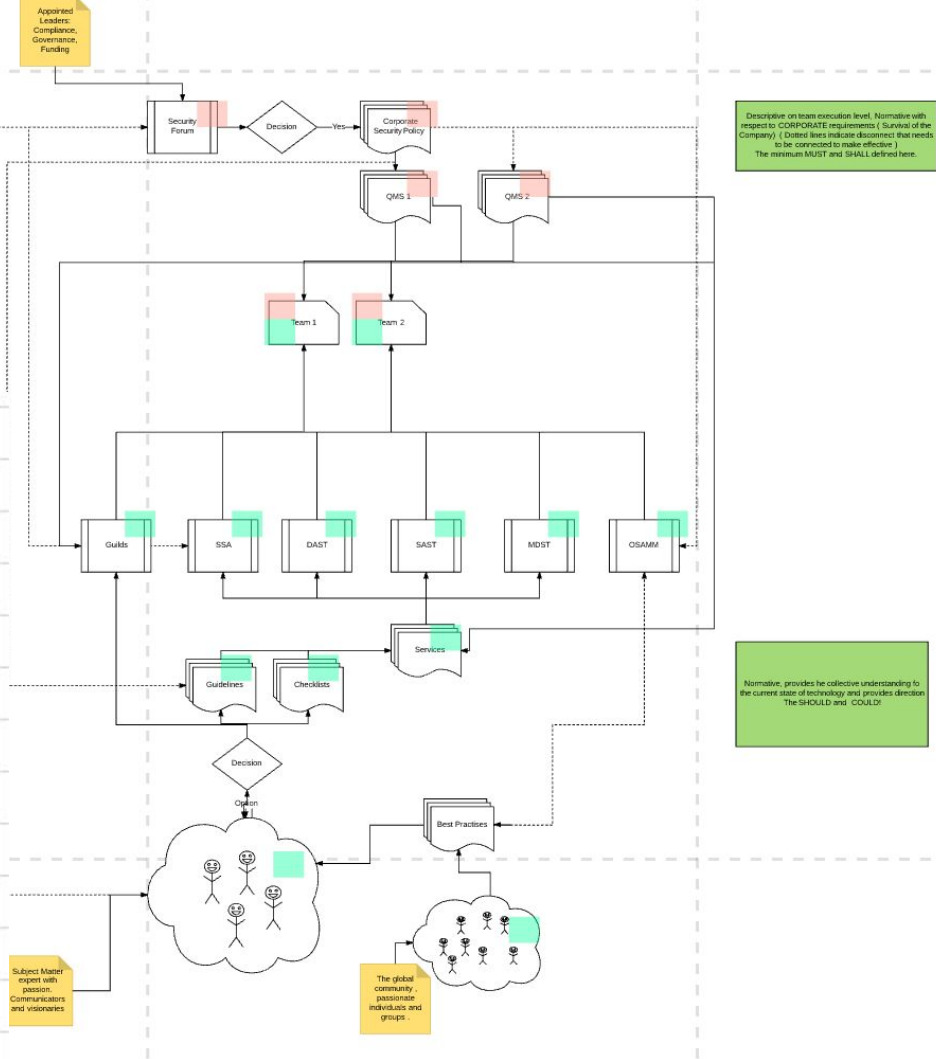
- Someone has motivation to do harm or take advantage of the systems/services provided by Visma
- All networks are **hostile** (traffic can be monitored and altered by an attacker)
- An attacker will not restrict him/herself to a standard browser
- Humans make mistakes
- Environments that the systems reside in are **constantly changing** with **limited control**
- Architects and developers do not have all information to design systems perfectly
- New attack techniques and vulnerabilities are **constantly evolving**
- Disclosing a user password removes the **accountability** of that user's actions in the system
- *A Shared secret is not a secret*

# Security Program

- Governance model
- Competency building



- Governance
- Construction
- Verification
- Operations
- Governance
- Construction
- Verification
- Operations



# Governance model

50+ application teams  
20+ cities

Security Champions  
Security as a service  
Central services for risk  
Security Engineers in  
Transparency on all

Title	Organization	Hosting provider	VCD St	Assessment	Assessment	Unresolved issues from	SAST	DAST	Latest	Unresolved critical and	Infrastructure vulnerabilities in	Security Engineer
Visma.net Advisor	PU	Azure	APPROVED	APPROVED								
eAccounting	PU	Azure	APPROVED	APPROVED								
Self-service Support	PU	Azure	APPROVED	APPROVED								
Advisory Tools Reconciliation	PU	Azure	APPROVED	APPROVED								
Visma.net Budgets	PU	Azure	APPROVED	APPROVED								
Visma Scanner	PU	Azure	APPROVED	APPROVED								
Advisory Tools Transaction Analysis	PU	Azure	APPROVED	APPROVED								
Visma MIND	PU	VITC	APPROVED	APPROVED								
Visma Enterprise BI	VES	AWS	APPROVED	APPROVED								
Mobile Employee & Payslip service	VES	VITC	APPROVED	APPROVED								
Visma.net Insights	PU	Azure	APPROVED	APPROVED								
Visma eAccounting Time	PU	Azure	APPROVED	APPROVED								
Cloud Collect	PU	AWS	APPROVED	APPROVED								
Visma Boardroom	PU	Azure	APPROVED	APPROVED								
Advisory Tools Taxation	PU	Azure	APPROVED	APPROVED								
Website / Webshop	PU	Azure	APPROVED	APPROVED								
Visma.net Time	VES	AWS	APPROVED	APPROVED								
Cost Request Asset	PU	Azure	APPROVED	APPROVED								

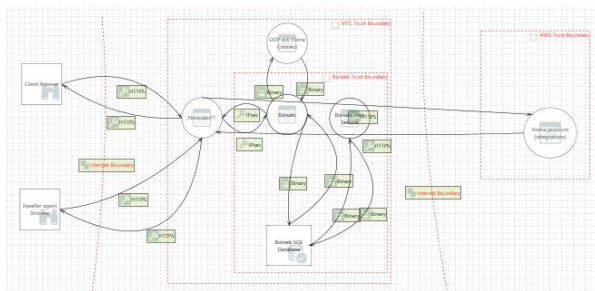
Transparency



# Competency building

## 5 levels of training:

1. Top Level Management : Capability to manage Security.
2. Mid Level Management : Capability to manage Security.
3. Developers / Architects / QA/Testers : Inspire and enable to build secure solutions.
4. Security Engineers : Inspire and enable to build & deliver secure solutions.
5. Central Security Team: Be the available experts for the teams.



> SA06 - Client side input validation

✓ SA07 - Input validation coverage and quality

Is input received via all interfaces of the attack surface validated before it is processed/persisted?

Is input validation centralized in one component or is it implemented independently in all interfaces?

Identify all code fragments or components that implement input validation. Review the input validation code of at least a sample

> SA08 - Input validation coverage

> SA09 - Validation extensions and uploaded files

# Security Testing

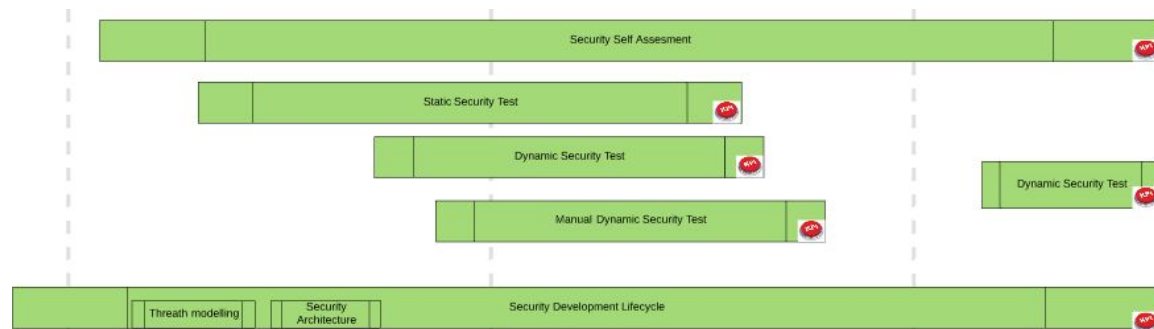
Static Application Sec Test

Dynamic Application Sec Test

Manual Security Tests

Penetration Testing

Bug Bounty



# Deployment



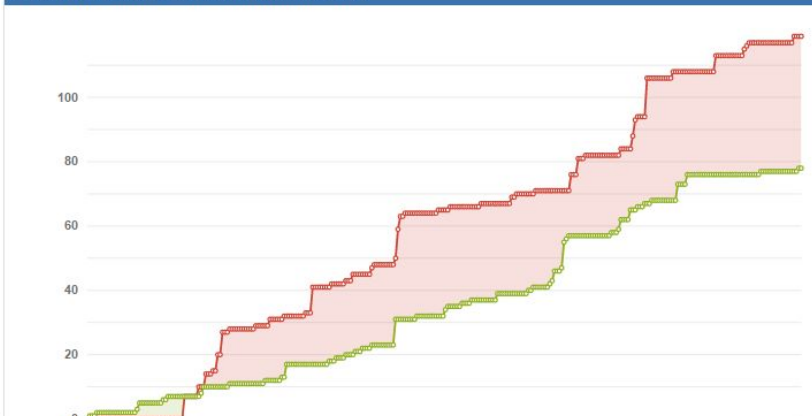
Customers of  
Visma

# Information handling

Problem to solve: 1000+ sales and support people + about 300 partners and their employees + about 500.000 customers + 50 teams / 700 internal people.

Our solution: Transparency and common model for communication

Created vs Resolved Chart: PU Security TP Critical+Severe



Service name	JIRA key	VCDM status	Assessment	Assessment date	Unresolved issues from assessment	SAST	DAST	Latest manual sec test	Unresolved critical and severe issues	Unresolved recommended issues	Security Engineer
Visma.net Advisor	ADV	APPROVED	APPROVED			ENROLLED	NOT ENROLLED				

# Results so far

Transparency:



Acknowledgement:



Internal awareness:



Increased customer value:



# 1

Secure systems is an opportunity for competitive advantage

# 2

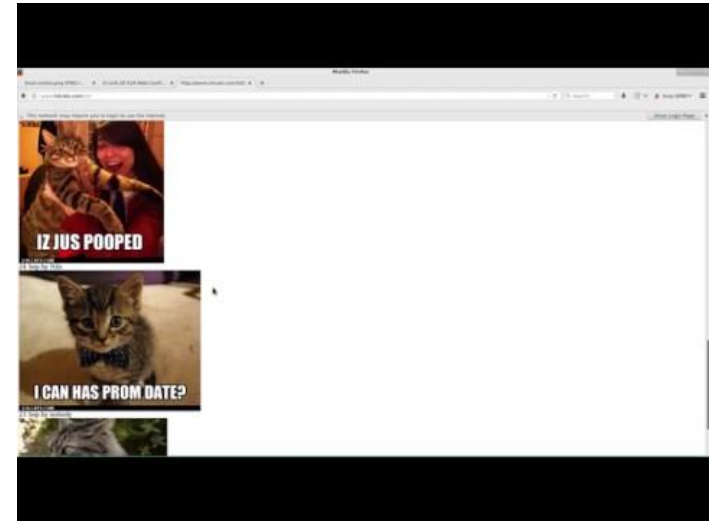
Visma is focusing on core business and relying on partners in other areas

# 3

Key success factor for delivering secure systems is culture, competency & hard work

# A short deep dive into MDST

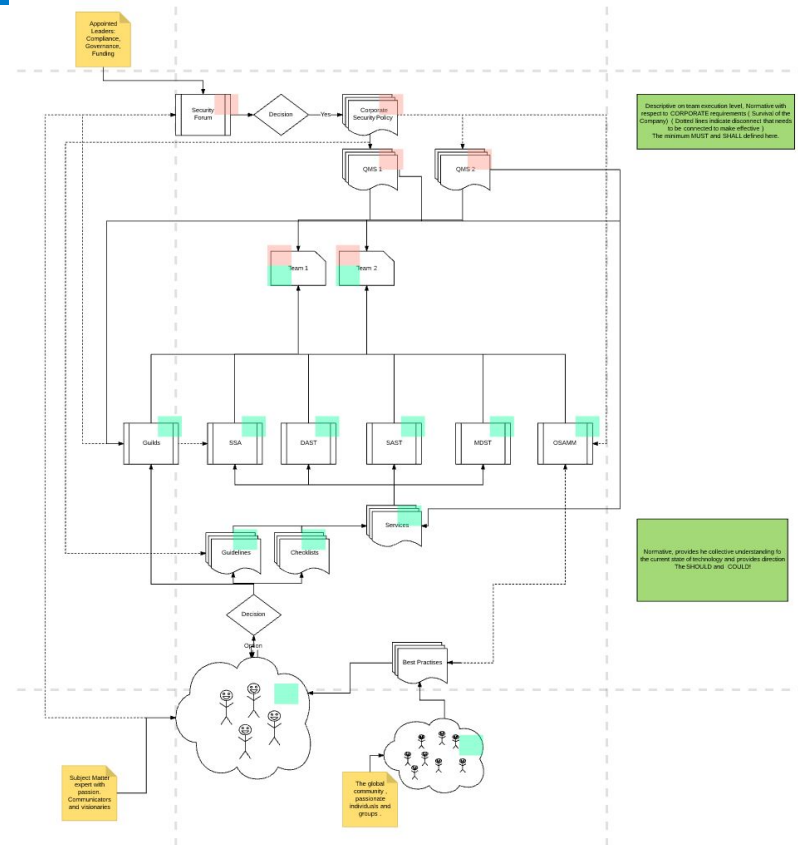
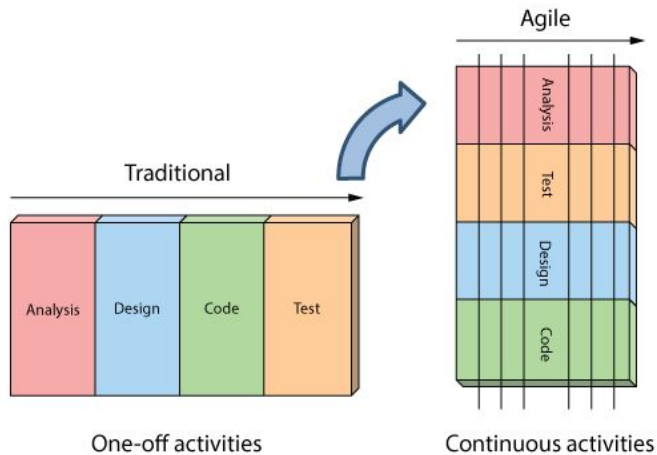
Aurelijus, Short Demo of one of the OWASP top 10 vulns. - XSS



# Agile meets Waterfall

Self organisation vs management driven?  
Iterative vs Extensive Specification?

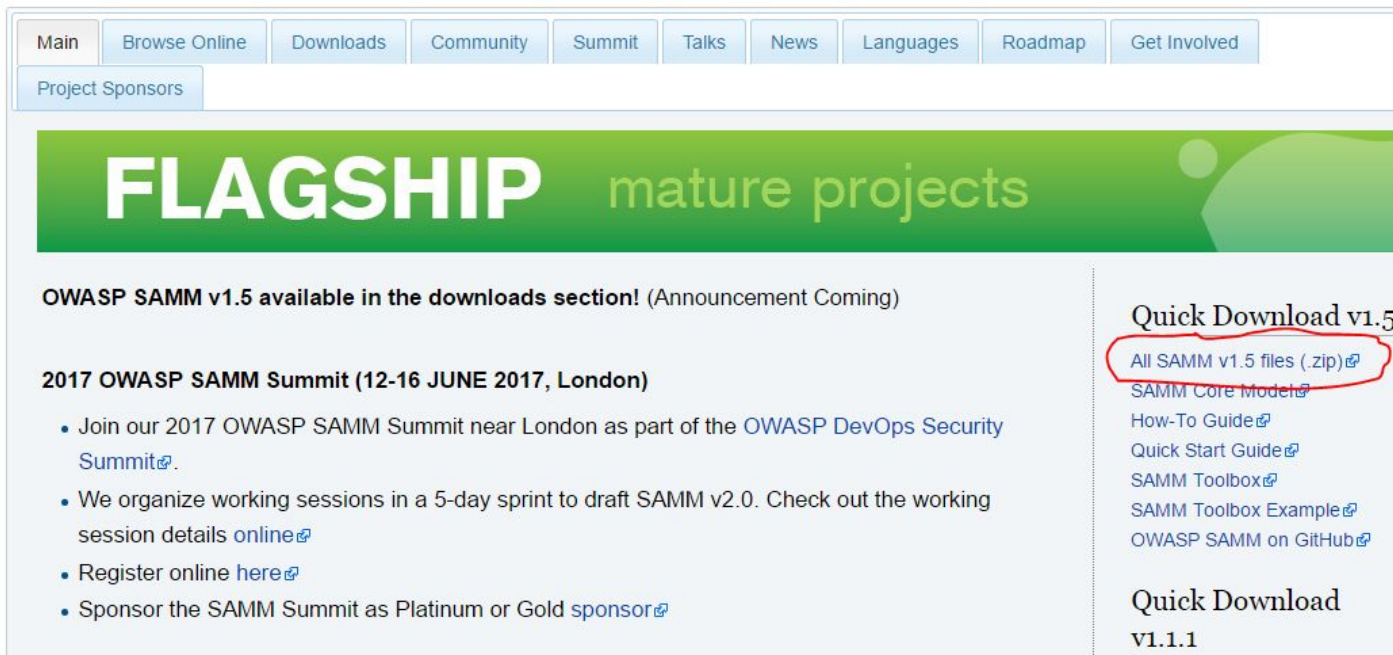
[http://www.agilenutshell.com/agile\\_vs\\_waterfall](http://www.agilenutshell.com/agile_vs_waterfall)





# OSAMM deeper dive

## OWASP SAMP Project



The screenshot shows the OWASP SAMP Project website. At the top, there is a navigation bar with tabs for Main, Browse Online, Downloads, Community, Summit, Talks, News, Languages, Roadmap, and Get Involved. Below this is a 'Project Sponsors' tab. A large green banner reads 'FLAGSHIP mature projects'. Below the banner, there is a section for 'OWASP SAMP v1.5 available in the downloads section! (Announcement Coming)'. To the right, there is a 'Quick Download v1.5' section with a red circle around the link 'All SAMP v1.5 files (.zip)'. Below this are links for 'SAMP Core Models', 'How-To Guide', 'Quick Start Guide', 'SAMP Toolbox', 'SAMP Toolbox Example', and 'OWASP SAMP on GitHub'. At the bottom right, there is a 'Quick Download v1.1.1' section.

Main | Browse Online | Downloads | Community | Summit | Talks | News | Languages | Roadmap | Get Involved

Project Sponsors

# FLAGSHIP

 mature projects

**OWASP SAMP v1.5 available in the downloads section!** (Announcement Coming)

**2017 OWASP SAMP Summit (12-16 JUNE 2017, London)**

- Join our 2017 OWASP SAMP Summit near London as part of the [OWASP DevOps Security Summit](#).
- We organize working sessions in a 5-day sprint to draft SAMP v2.0. Check out the working session details [online](#).
- Register online [here](#).
- Sponsor the SAMP Summit as Platinum or Gold [sponsor](#).

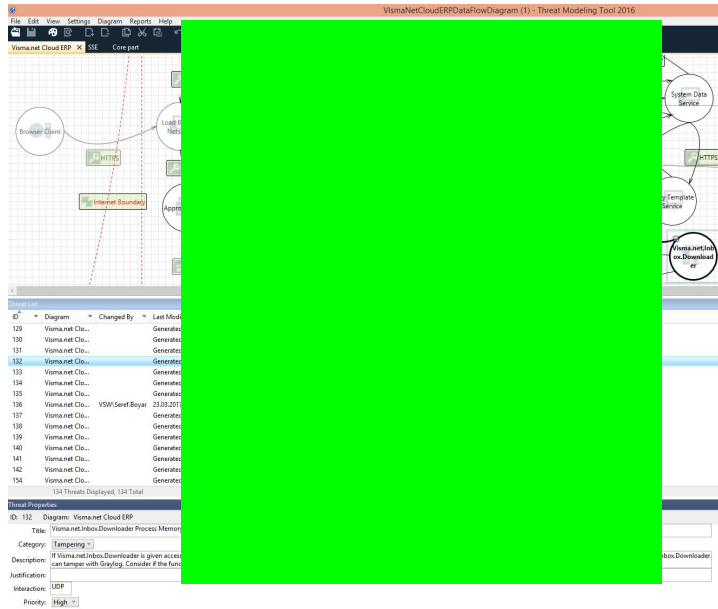
### Quick Download v1.5

- [All SAMP v1.5 files \(.zip\)](#)
- [SAMP Core Models](#)
- [How-To Guide](#)
- [Quick Start Guide](#)
- [SAMP Toolbox](#)
- [SAMP Toolbox Example](#)
- [OWASP SAMP on GitHub](#)

### Quick Download v1.1.1

# Threat Modelling

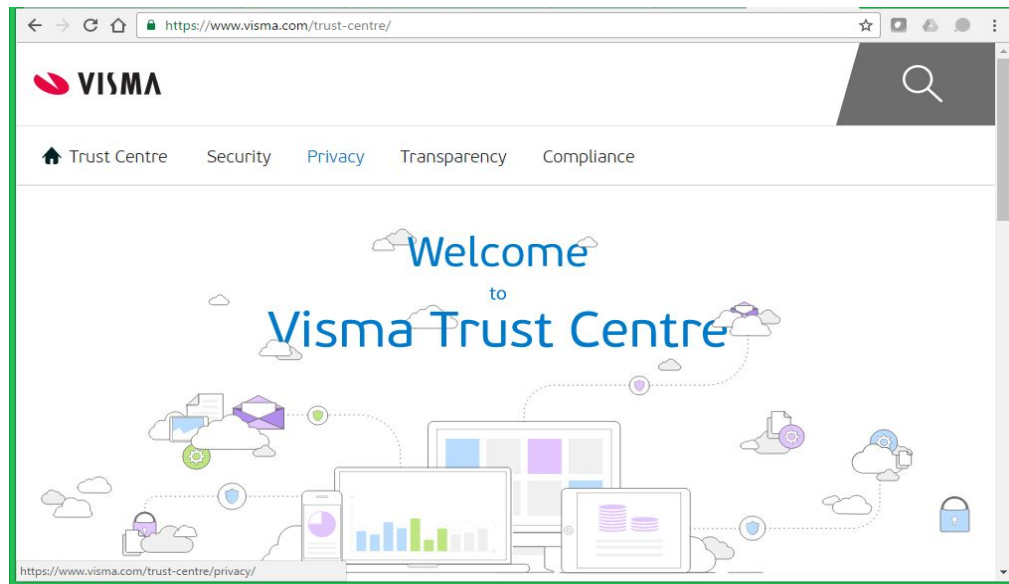
Demo:



# Q&A and more information

[Espen.Johansen@visma.com](mailto:Espen.Johansen@visma.com)

Learn more 





# WS` s and discussion topics

# Security Program: Selected elements

Espen

Security As a Service

Competency building / Training / Culture Building

Distributed decision model (SSA, DAST, SAST)

# Security Program: Selected elements

Espen

Manage risk in a Cloud Environment

# Security Program: Selected elements

Espen

Security As a Service

Competency building

Distributed decision model (SSA, DAST, SAST)



# Threat Intelligence

# Automated Security Reporting

## Challenge :

Our systems are very complex organisms and have 100-1000 dependencies each. ( Libraries, Components, Operating Systems, Virtualization Layers, Network, etc). Each of these have a person with a responsibility.

Security Vulnerabilities in these are discovered and disclosed several times a day in multiple open and closed communities all over the world.

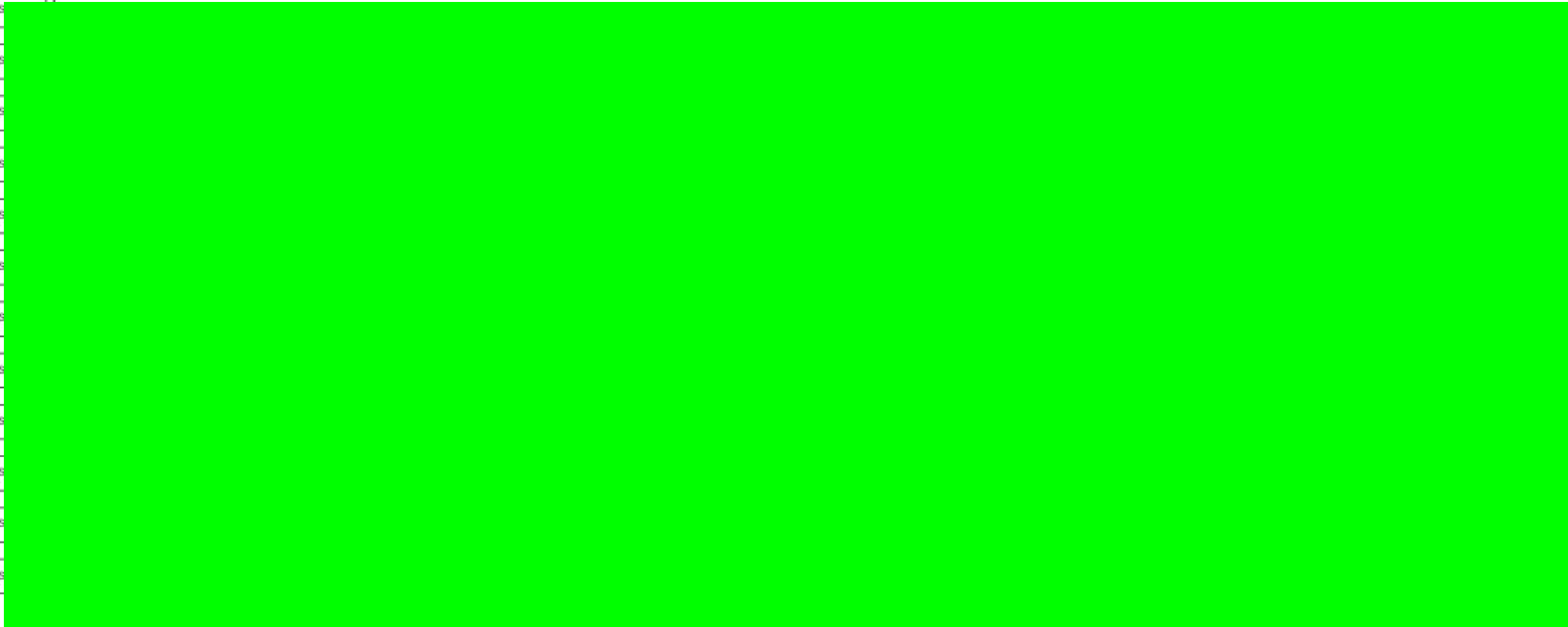
To maintain strong security and provide a strong message of TRUST to our clients and prospects we need to handle this complexity every minute of every day. 24/365.

# Process

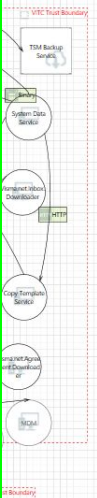
## Schematic:

1. Gather Threat Intelligence.
2. Analyse intelligence.
3. Create Actions that is possible to implement.
4. Dispatch Actionable intelligence to the right person.
  - a. Make note of 4 and enter into follow up system.
  - b. Follow up trough competency sharing and training as well as transparent metrics.
  - c. Repeat loop 1-4 for X days. if ROOT cause not fixed in X days, GOTO 5
5. Update Divisional Risk management report, consider replacing “right person” with “updated” person. -> HRM procedure MAY be utilized.

# Illustration of the system



n = easy



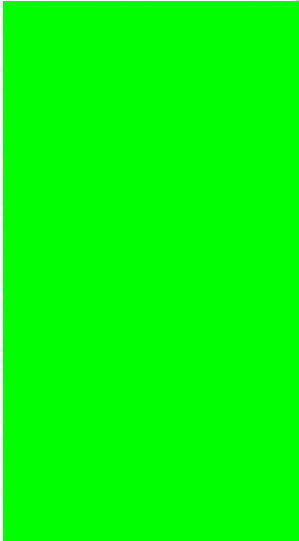
Search

Share Export

project = COV AND component = "Infrastructure Vulnerability Scanner" AND resolution = Unresolved

Basic

Order by



Coverity / COV-41

1 of 1

# Microsoft Windows SMBv1 Remote Code Execution - Shadow Brokers (ETERNALCHAMPION, ETERNALSYSTEM) - Zero Day

## Details

Type:	Bug	Status:	<b>OPEN</b> (View Workflow)
Priority:	Critical	Resolution:	Unresolved
Component/s:		Security Level:	Standard (Anyone can log work on this issue)
Labels:	None		

## People

Assignee: Unassigned

Reporter:

Votes: Vote for this issue

Watchers: Start watching this issue

Level Status: In Work

Changes in this version:

Final release notes:

## Dates

Created: Monday 12:13 PM  
Updated: Monday 12:13 PM

## Collaborators

