Security & Visma SMB

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

VISMA

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

VISMA

Why?

VISMA

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

VISMA

Security Program

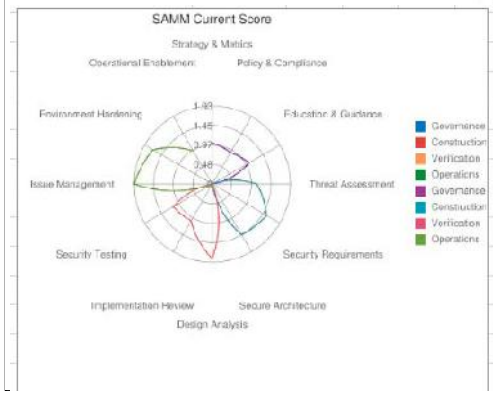
Selected assumptions for the Security Program:

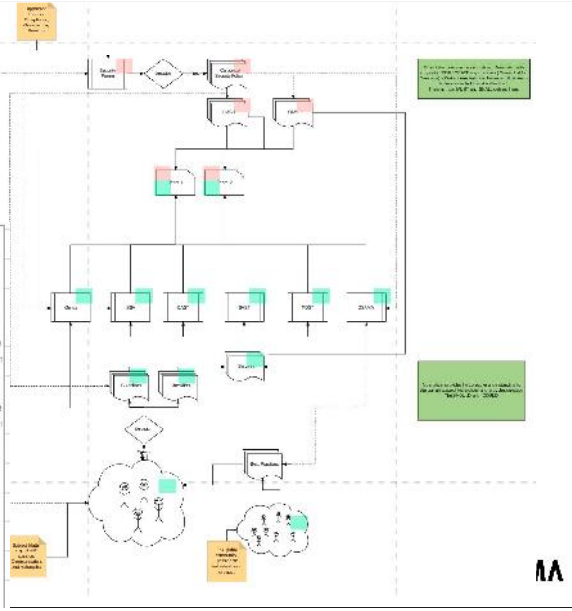
- Someone has motivation to do harm or take advantage of the systems/services provided by Visma
- All networks are **hostile** (traffic can be monitored and altered by an attacker)
- An attacker will not restrict him/herself to a standard browser
- Humans make mistakes
- Environments that the systems 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*

VISMA

Security Program

- **Governance model**
- **Competency building**





Governance model

50+ application tean
20+ cities

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

VISMA

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.

VISMA

Security Testing

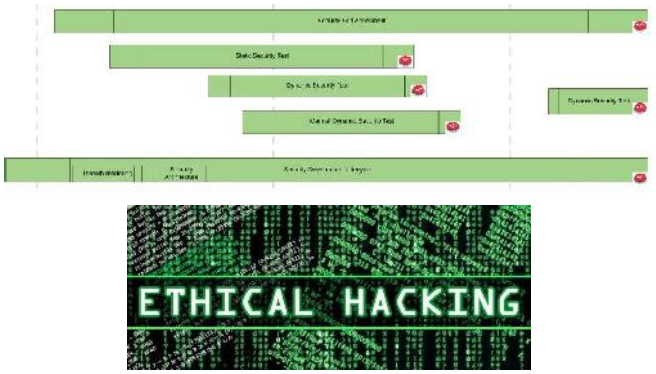
Static Application Sec Test

Dynamic Application Sec Test

Manual Security Tests

Penetration Testing

Bug Bounty



VISMA

Deployment

build
IaaS
Microsoft

deploy
PaaS
VISMA

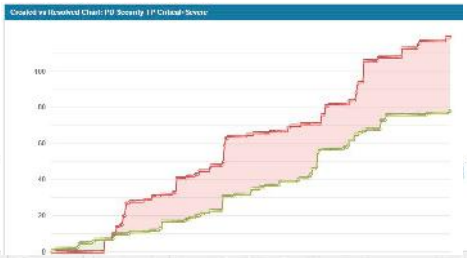
buy
SaaS
Customers of Visma

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



VISMA

Results so far

Transparency:

Acknowledgement:

Internal awareness:

Increased customer value:

VISMA

1

Secure systems is an opportunity for competitive advantage

2

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

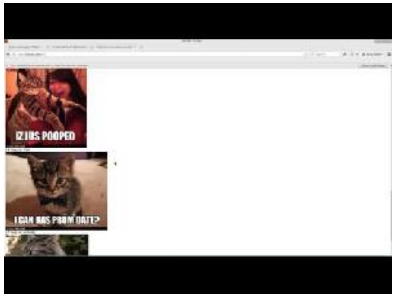
3

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

VISMA

A short deep dive into MDST

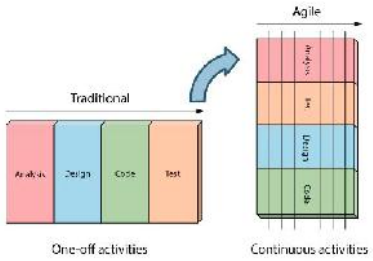
Aurelijus, Short Demo of one of the OWASP top 10 vulns. - XSS

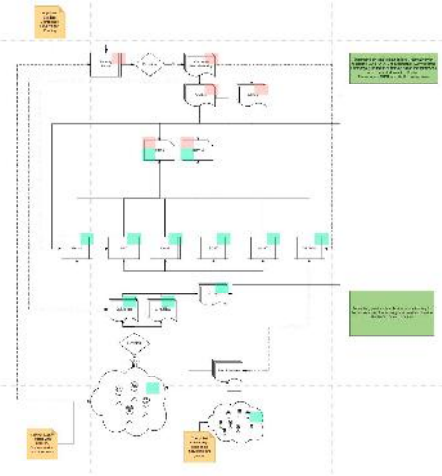


VISMA

Agile meets Waterfall

Self organisation vs management driven?
Iterative vs Extensive Specification?
http://www.agilenutshell.com/agile_vs_waterfall





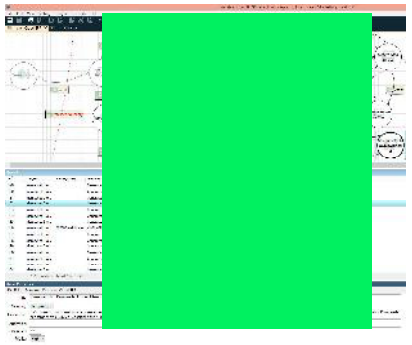
ISMA

OSAMM deeper dive

VISMA

Threat Modelling

Demo:

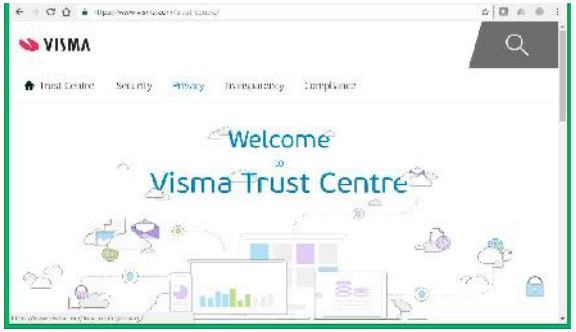


VISMA

Q&A and more information

Espen.Johansen@visma.com

Learn more



VISMA

VISMA

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.

VISMA

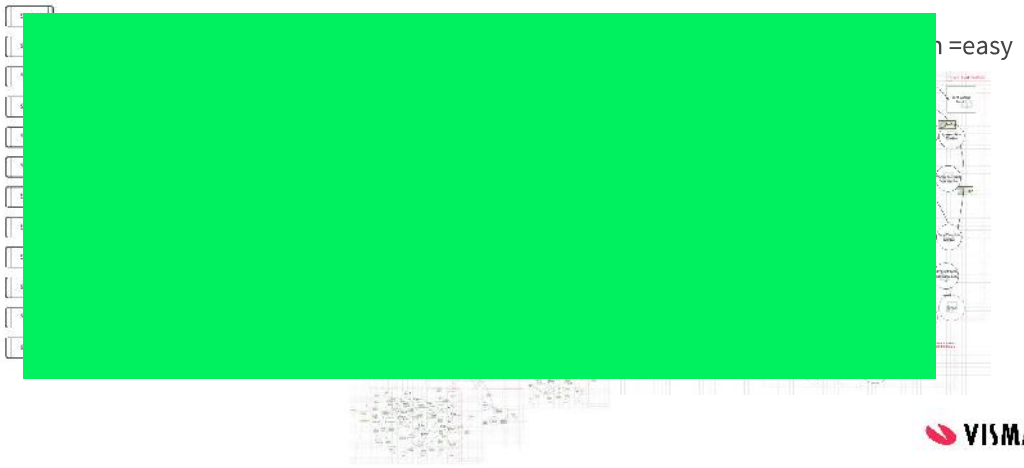
Process

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.

VISMA

Illustration of the system



VISMA

Search Save as 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 [redacted]

Edit Comment Assign More Start specifications Ready for Dev Workflow

Details

Type: Bug
Priority: Critical
Component/s: [redacted]
Labels: None

Status: OPEN (View Workflow)
Resolution: Unresolved
Security Level: Standard (Anyone can log work on this issue.)

Main Support Processing Documentation Time Tracking

Level Status: In Work
Changes in this version:
Final release note:

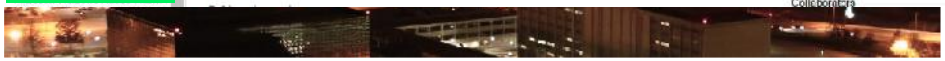
People

Assignee: Unassigned
Assign to me
Reporter: [redacted]
Votes: Vote for this issue
Watchers: Start watching this issue

Dates

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

Collaborators



VISMA