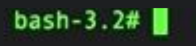
Security in Agile Development

Joakim



```
bash-3.2# █
```

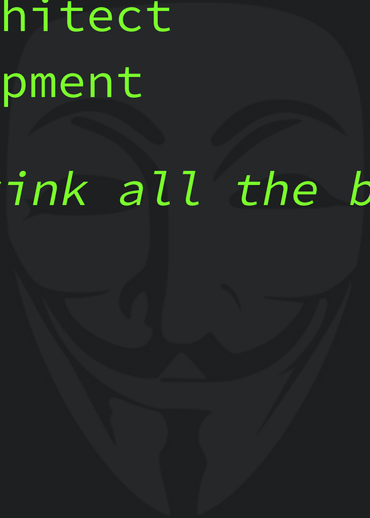
Who am I?

@JoakimTauren

Application Security Architect

@Visma Enterprise Development

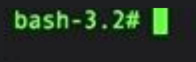
“Hack all the things, drink all the booze”



Current scope:

~100 dev teams

~900+ developers



```
bash-3.2# █
```

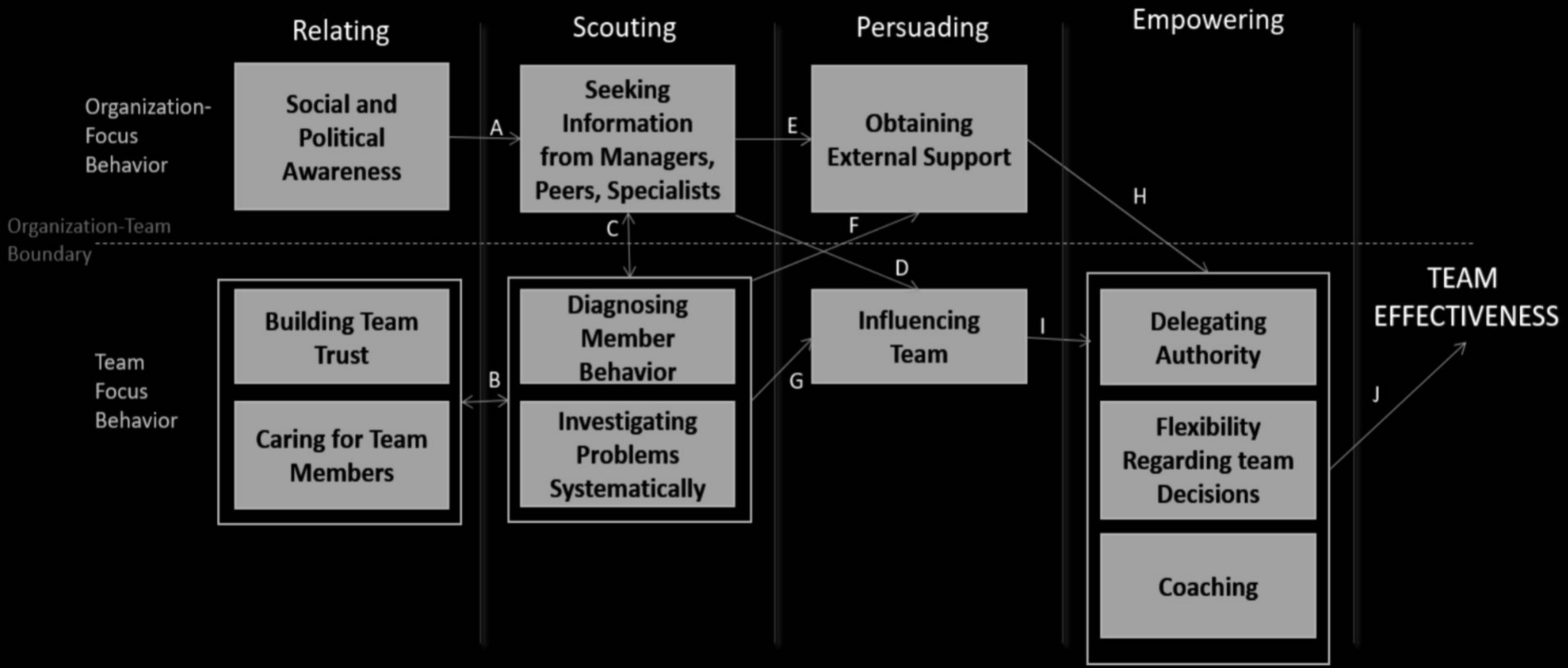
Governance model

- ~300 Dev teams
- 2000+ Developers
- 25+ Countries
- 70M+ lines of code

  In SAST

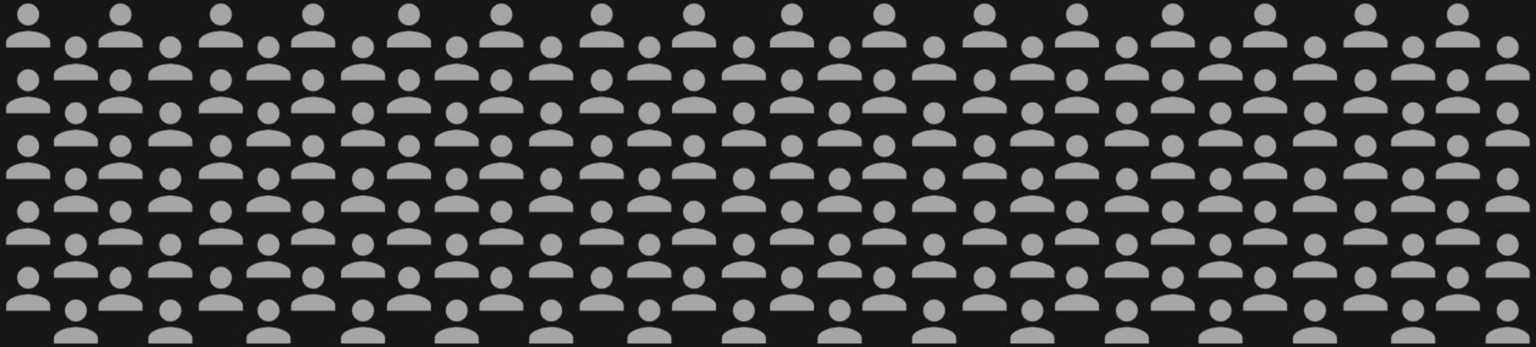
Security at scale?

The Effective Leadership of Self-Managing Work Teams


Relating
Scouting
Persuading
Empowering
Organization-Focus Behavior
Social and Political Awareness
A
Seeking Information from Managers, Peers, Specialists
E
Obtaining External Support
H
Organization-Team Boundary
C
F
D
TEAM EFFECTIVENESS
Team Focus Behavior
Building Team Trust
Caring for Team Members
B
Diagnosing Member Behavior
Investigating Problems Systematically
G
Influencing Team
I
Delegating Authority
Flexibility Regarding team Decisions
Coaching
J

Druskat, Vanessa Urch, and Jane V. Wheeler. “Managing from the Boundary: The Effective Leadership of Self-Managing Work Teams.” *The Academy of Management Journal*, vol. 46, no. 4, 2003, pp. 435–457. *JSTOR*, JSTOR, www.jstor.org/stable/30040637

SECURITY ENGINEERS 🌍



SECURITY TEAM

SWEDEN 🇸🇪

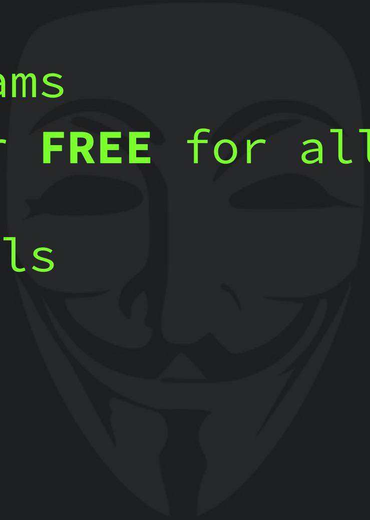
LITHUANIA 🇱🇹

NORWAY 🇳🇴

ROMANIA 🇷🇴

Security as a service

- Central services for methodology, tooling and manual testing
- Main Goal: Assist teams
- Provide: Services for **FREE** for all teams



Transparency on all levels

Confluence and Jira

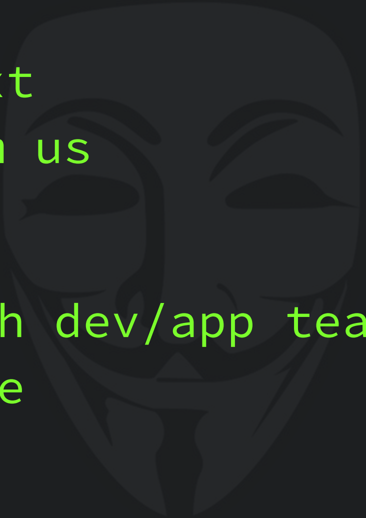
The Security Program

OWASP SAMM - Empower teams

- Security Training (ST)
- SSA,PSA,RA
- SPIP,PSOC,CTI
- SAST,DAST,MAVA,ATVS,Bug Bounty

The dev team

- Is responsible
- Knows the end users
- Aware of their context
- Receives support from us
- Own initiative



Security Engineer in each dev/app team

Service Owner accountable

Security Engineer

Role within each dev team

Evangelist/Champion of Security

Security culture promotor

Ensures Security is part of dev every day

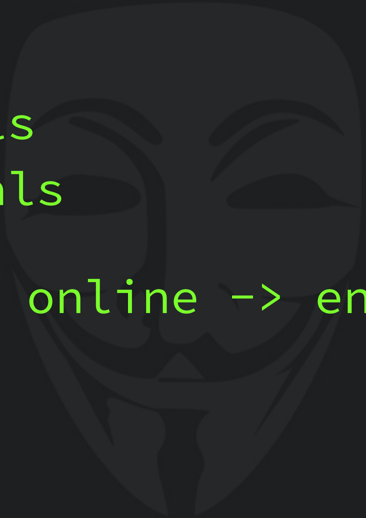
Security Guild

A community of:

- Security Engineers
- Security Professionals
- Like-minded individuals

Gathers every other week online -> engagement

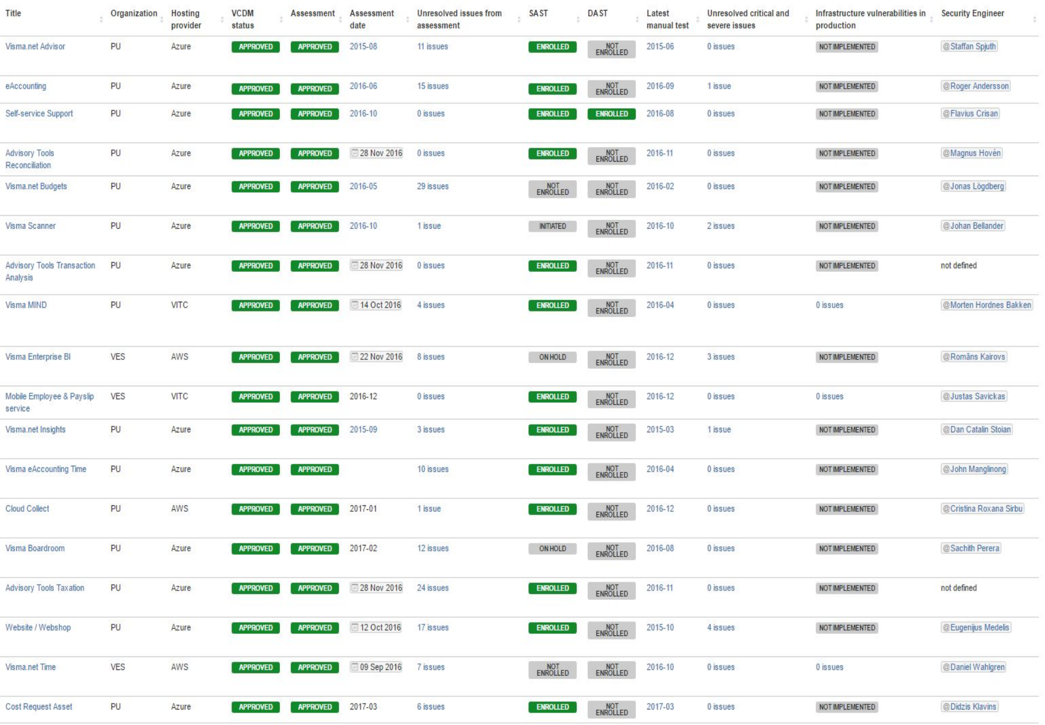
Has a chat channel



Target portfolio (Confluence)

Transparent list
(current sec status)
of ALL teams

Can be viewed by anyone
In Visma



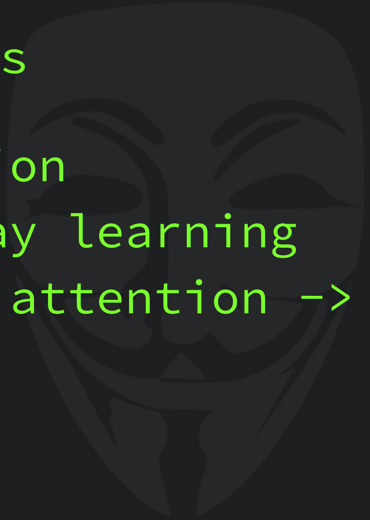
Title	Organization	Hosting provider	VCDM status	Assessment	Assessment date	Unresolved issues from assessment	SAST	DAST	Latest manual test	Unresolved critical and severe issues	Infrastructure vulnerabilities in production	Security Engineer
Visma.net Advisor	PU	Azure	APPROVED	APPROVED	2015-08	11 issues	ENROLLED	NOT ENROLLED	2015-06	0 issues	NOT IMPLEMENTED	@Staffan Spjuth
eAccounting	PU	Azure	APPROVED	APPROVED	2016-06	15 issues	ENROLLED	NOT ENROLLED	2016-09	1 issue	NOT IMPLEMENTED	@Roger Andersson
Self-service Support	PU	Azure	APPROVED	APPROVED	2016-10	0 issues	ENROLLED	ENROLLED	2016-08	0 issues	NOT IMPLEMENTED	@Flavius Crisan
Advisory Tools Reconciliation	PU	Azure	APPROVED	APPROVED	28 Nov 2016	0 issues	ENROLLED	NOT ENROLLED	2016-11	0 issues	NOT IMPLEMENTED	@Magnus Hovén
Visma.net Budgets	PU	Azure	APPROVED	APPROVED	2016-05	29 issues	NOT ENROLLED	NOT ENROLLED	2016-02	0 issues	NOT IMPLEMENTED	@Jonas Lögdberg
Visma Scanner	PU	Azure	APPROVED	APPROVED	2016-10	1 issue	INITIATED	NOT ENROLLED	2016-10	2 issues	NOT IMPLEMENTED	@Johan Bellander
Advisory Tools Transaction Analysis	PU	Azure	APPROVED	APPROVED	28 Nov 2016	0 issues	ENROLLED	NOT ENROLLED	2016-11	0 issues	NOT IMPLEMENTED	not defined
Visma MIND	PU	VITC	APPROVED	APPROVED	14 Oct 2016	4 issues	ENROLLED	NOT ENROLLED	2016-04	0 issues	0 issues	@Morten Hordnes Bakken
Visma Enterprise BI	VES	AWS	APPROVED	APPROVED	22 Nov 2016	8 issues	ON HOLD	NOT ENROLLED	2016-12	3 issues	NOT IMPLEMENTED	@Romāns Kairovs
Mobile Employee & Payslip service	VES	VITC	APPROVED	APPROVED	2016-12	0 issues	ENROLLED	NOT ENROLLED	2016-12	0 issues	0 issues	@Justas Savickas
Visma.net Insights	PU	Azure	APPROVED	APPROVED	2015-09	3 issues	ENROLLED	NOT ENROLLED	2015-03	1 issue	NOT IMPLEMENTED	@Dan Catalin Stoian
Visma eAccounting Time	PU	Azure	APPROVED	APPROVED		10 issues	ENROLLED	NOT ENROLLED	2016-04	0 issues	NOT IMPLEMENTED	@John Manglinong
Cloud Collect	PU	AWS	APPROVED	APPROVED	2017-01	1 issue	ENROLLED	NOT ENROLLED	2016-12	0 issues	NOT IMPLEMENTED	@Cristina Roxana Sirbu
Visma Boardroom	PU	Azure	APPROVED	APPROVED	2017-02	12 issues	ON HOLD	NOT ENROLLED	2016-08	0 issues	NOT IMPLEMENTED	@Sachith Perera
Advisory Tools Taxation	PU	Azure	APPROVED	APPROVED	28 Nov 2016	24 issues	ENROLLED	NOT ENROLLED	2016-11	0 issues	NOT IMPLEMENTED	not defined
Website / Webshop	PU	Azure	APPROVED	APPROVED	12 Oct 2016	17 issues	ENROLLED	NOT ENROLLED	2015-10	4 issues	NOT IMPLEMENTED	@Eugenijus Medelis
Visma.net Time	VES	AWS	APPROVED	APPROVED	09 Sep 2016	7 issues	NOT ENROLLED	NOT ENROLLED	2016-10	0 issues	0 issues	@Daniel Wahlgren
Cost Request Asset	PU	Azure	APPROVED	APPROVED	2017-03	6 issues	ENROLLED	NOT ENROLLED	2017-03	0 issues	NOT IMPLEMENTED	@Didzis Klavins

Security Self-Assessment

A number of questions for each team to answer

Core elements this serves

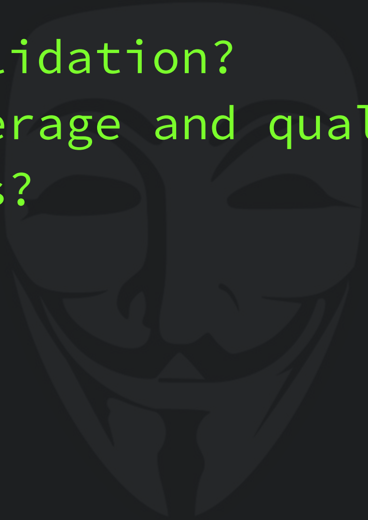
- Context based education
- Review process two-way learning
- Each item that needs attention -> Jira



Security Self-Assessment

Example questions:

- Client Side input validation?
- Input validation coverage and quality?
- Handling of passwords?
- Dynamic SQL?



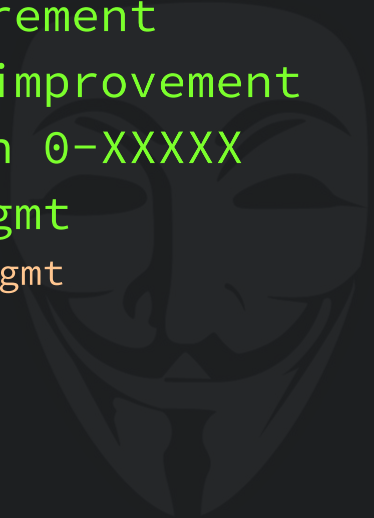
Security Self-Assessment

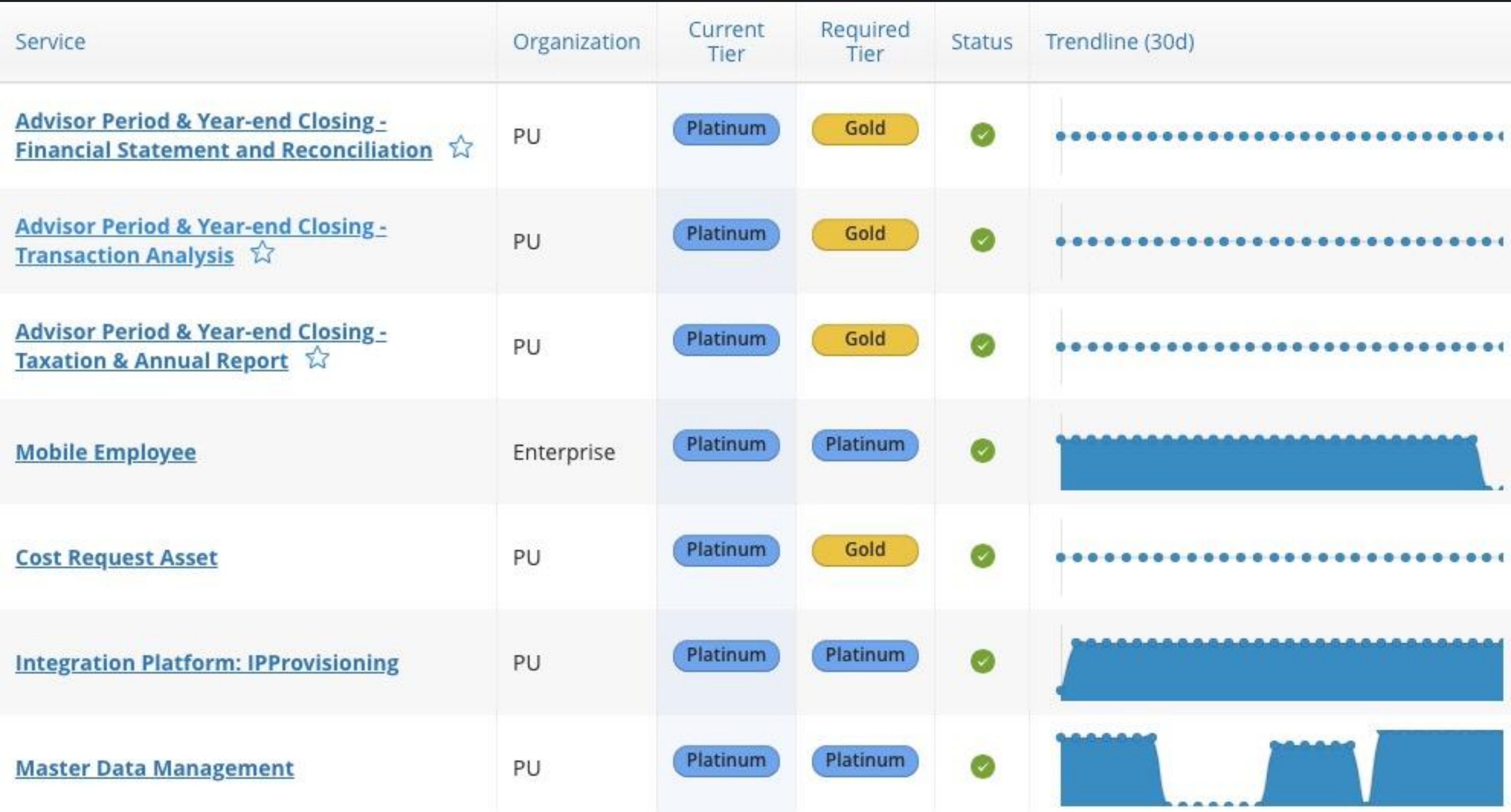
The challenge and key to successful assessments:

Transparency

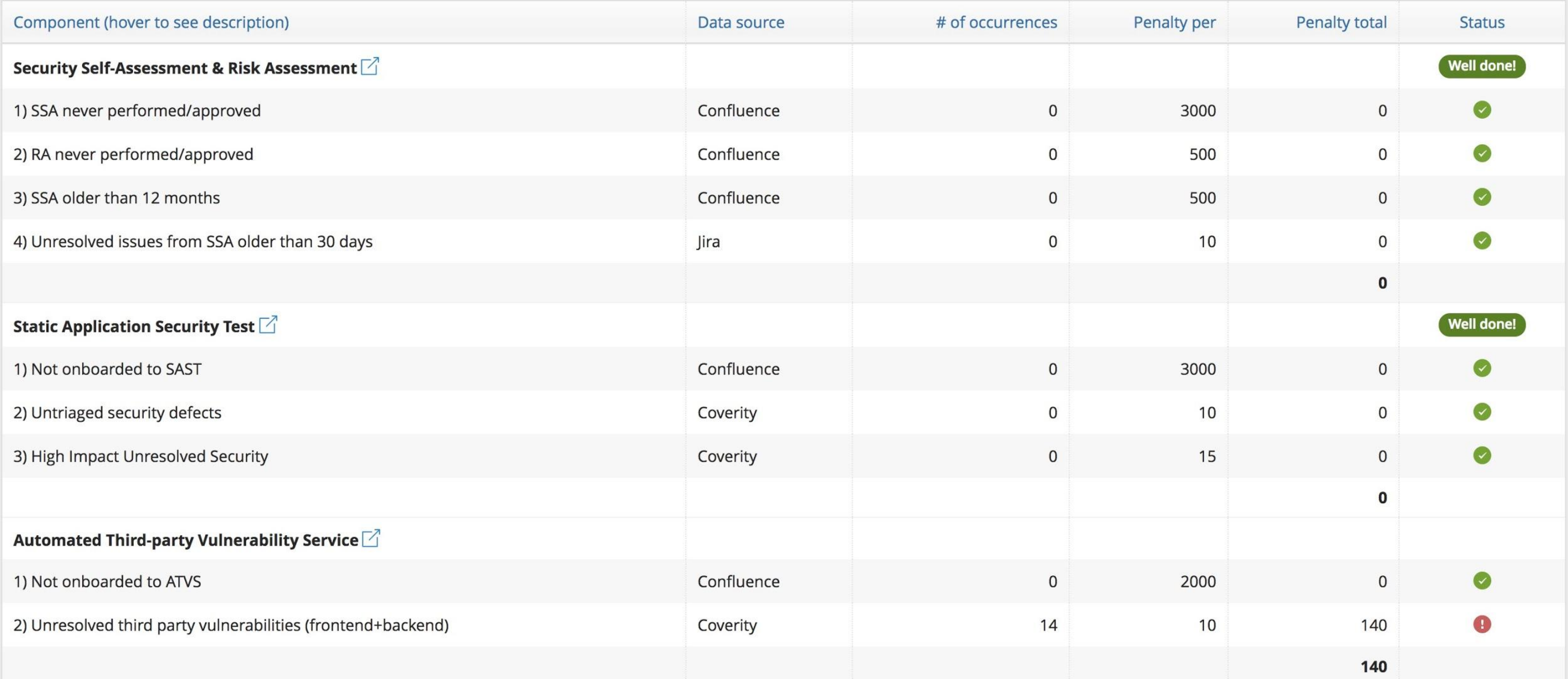
Security Maturity Index

- Transparent list (again!)
- Performance vs requirement
- Supports continuous improvement
- Numeric value between 0-XXXXX
- Tool for teams and mgmt
    - Required tier set by mgmt





Service	Organization	Current Tier	Required Tier	Status	Trendline (30d)
Advisor Period & Year-end Closing - Financial Statement and Reconciliation ☆	PU	Platinum	Gold	✓	
Advisor Period & Year-end Closing - Transaction Analysis ☆	PU	Platinum	Gold	✓	
Advisor Period & Year-end Closing - Taxation & Annual Report ☆	PU	Platinum	Gold	✓	
Mobile Employee	Enterprise	Platinum	Platinum	✓	
Cost Request Asset	PU	Platinum	Gold	✓	
Integration Platform: IPProvisioning	PU	Platinum	Platinum	✓	
Master Data Management	PU	Platinum	Platinum	✓	



Component (hover to see description)	Data source	# of occurrences	Penalty per	Penalty total	Status
Security Self-Assessment & Risk Assessment					Well done!
1) SSA never performed/approved	Confluence	0	3000	0	✓
2) RA never performed/approved	Confluence	0	500	0	✓
3) SSA older than 12 months	Confluence	0	500	0	✓
4) Unresolved issues from SSA older than 30 days	Jira	0	10	0	✓
				0	
Static Application Security Test					Well done!
1) Not onboarded to SAST	Confluence	0	3000	0	✓
2) Untriaged security defects	Coverity	0	10	0	✓
3) High Impact Unresolved Security	Coverity	0	15	0	✓
				0	
Automated Third-party Vulnerability Service					
1) Not onboarded to ATVS	Confluence	0	2000	0	✓
2) Unresolved third party vulnerabilities (frontend+backend)	Coverity	14	10	140	!
				140	

Security Maturity Index

Performance must be displayed to management

Tool for both management and team

Assists in evaluating needs

Transparency

From Security Maturity Index

⋮

Down to individual vulnerabilities

Product SOC

- Incidents
- Attribution
- Investigation
- Sherlock Holmes of Cyber
- Cyber Threat Intelligence

Product SOC

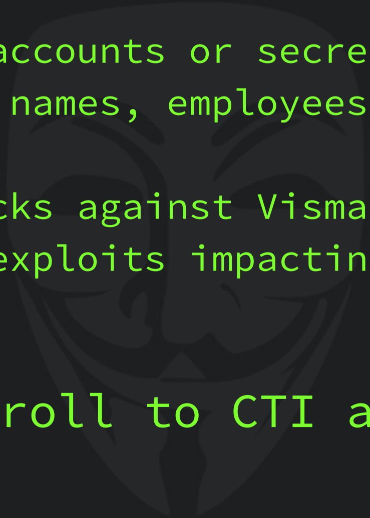
Successes 2019: 1 person behind bars (cannot disclose)

Ultimate goal:

- Police reports.
- More police reports..
- Even more police reports...

Cyber Threat Intelligence

Security analysts monitor and search for:



- Anyone distributing Visma accounts or secrets on black markets
- Mentionings of Visma brand names, employees, or services together with hostile language
- Chatter about pending attacks against Visma infrastructure
- Vulnerabilities and 0-day exploits impacting our technology stack
- and many other topics...

Any team in Visma can enroll to CTI as a Service, at no additional cost.

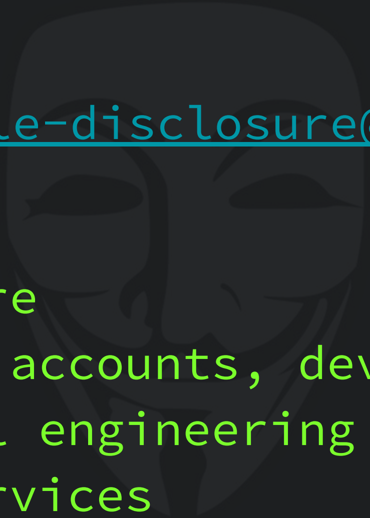
Recorded Future

VISMA

Responsible Disclosure

https://www.visma.com/trust-centre/security/

responsible-disclosure@visma.com



- Reproducible
- Coordinated disclosure
- Target only your own accounts, devices and information
- No phishing or social engineering
- Don’t disrupt the services

Bounty plz?

```
[root VISMA ~]# █
```

hackerone

VISMA

Bug Bounty

Teams can onboard for free!

Final steps towards true maturity

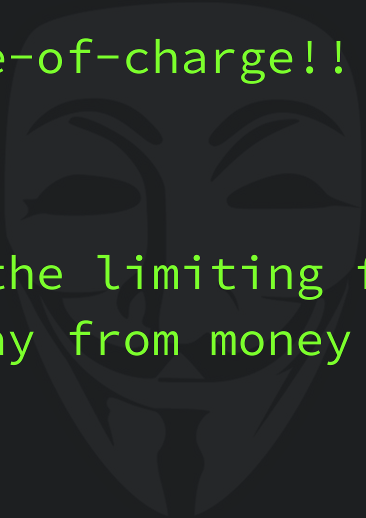
We do have prerequisites for onboarding

- 0 known vulnerabilities

Wrap-up, the tools

- Coverity (SAST)
- Detectify (DAST)
- Protecode + Retire.js (ATVS)
- “Internal” Hackers (6 persons)(MAVA)
- RecordedFuture (CTI)

So… Security as a Service?



The cool thing?

- All services are free-of-charge!!

Why?

- Money should not be the limiting factor
- Abstract the team away from money

Conclusions

Transparency and gamification works!

True maturity = police reports, Bug Bounties

Provide services for free!!

Each time you reuse a password..