Defendable Products

Ståle Pettersen
Head of Product & Application Security in Schibsted
Sikkerhetsfestivalen
28.Aug 2023

@kozmic / @kozmic@infosec.exchange
stale.pettersen@schibsted.com
Hobbies:

Agenda

- Background (Cybersecurity program)
- Guiding principles
- Implementation and roll out
- Lessons learned

FINN
blocket
Bergens Tidende
The Mindfulness App
VG
AFTONBLADET
tori
Aftenposten
Hjemmelegene
FIXRATE
albert
pej
let's deal
helthjem
Godare
FUNDING PARTNER
advized
tibber
E24
compricer
Dooris
CAPCITO
VEKTKLUBB
Askøyværingen
KUNDKRAFT.
unloc
Rakentaja.fi
hygglo
Prisjakt
HYPOTEKET
OIKOTIE
MORGENLEVERING
zoopit
homely
inzpire.me
klart
Lendo
Omni
insurello
Bilbasen
MAT KANALEN
dba
Tillit
bytbil
vinguiden.
SYD
tv.nu
PodMe
bookis
nettbil
ROCKER
Bygdanytt.
mittanbud
servicefinder
Dintero
Strilen
wellobe
Vestnytt
torn
Distribution Innovation
Mindler
SVENSKA DAGBLADET
Stavanger Aftenblad

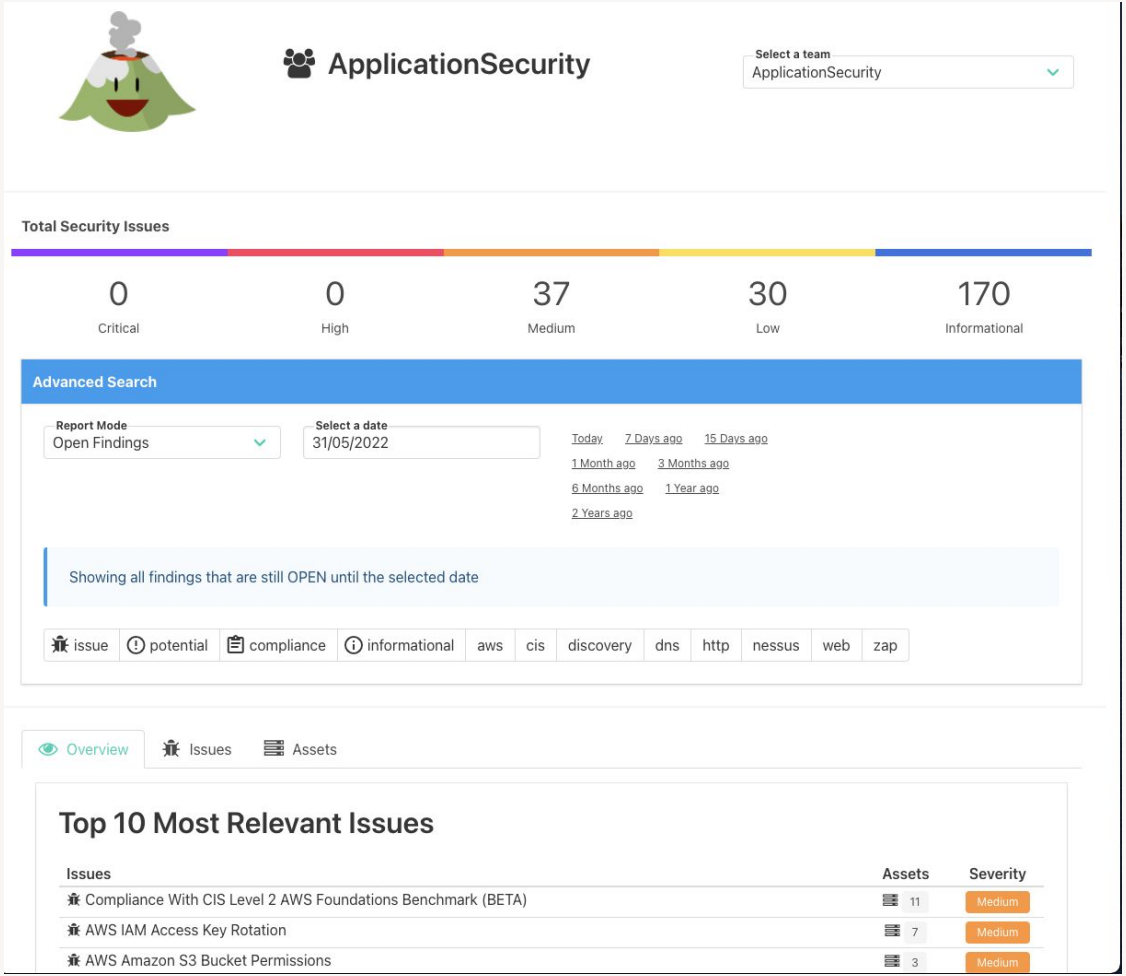
Schibsted tech in numbers

- 1 000+ Developers spread across 150+ teams
- 10 000+ Git repositories
- "All" programming languages in use
- 500+ Cloud accounts (AWS + GCP)
- 100+ Kubernetes clusters
- 51 879 Domains and subdomains

```
→ ~ curl -s -H "authorization: custom $(cat ~/.appinv-secrets/application-inventory-api-token-pro)" https://security.schibsted.io/api/v1/domains | jq -r | wc -l
51879
```

Vulcan

- Infrastructure security scanner (unauthenticated)
- Teams, members and assets
- Self managed
- Open source



Budget approved

Finish

2019 | 2020 | 2021 | 2022

NIST Cybersecurity Framework

Start

Minimum Target baseline:

Level 3

CYBER SECURITY ROADMAP

	2020	2021	2022
Program stream			
Infrastructure stream			
Application stream	Inventory + Secure by default + Application Security + Cloud Security + Threat modelling + Training		
Operations stream			
Change stream			

security.schibsted.io/web/?domain=schibsted.com

Logged in as: Ståle Pettersen Log out

Scanned Assets | AWS Accounts

Search scanned assets

schibsted.com | Search

schibsted.com

Scanned by

- Detectify Deep Scan
- Detectify Asset Monitoring
- Vulcan

Tracked by

- AWS Route53
- OnDMARC
- Ports Group

Made with love from Product & Application Security team.

Scanned Assets

security.schibsted.io/web/?domain=schibsted.cc

Logged in as: Ståle Pettersen Log out

Scanned Assets | AWS Accounts

Search scanned assets

schibsted.cc | Search

schibsted.cc

Scanned by

- Detectify Deep Scan
- Detectify Asset Monitoring
- Vulcan

Tracked by

Made with love from Product & Application Security team.

Guiding Principles

Creating a security culture across Schibsted

There is no technical silver bullet for product security

Teams need to be aware of the risks, then get empowered to improve security through training and tools.

Usability is more important than security

GitHub

Integrate security with the team's current workflow

Appropriate level of requirements and alerts

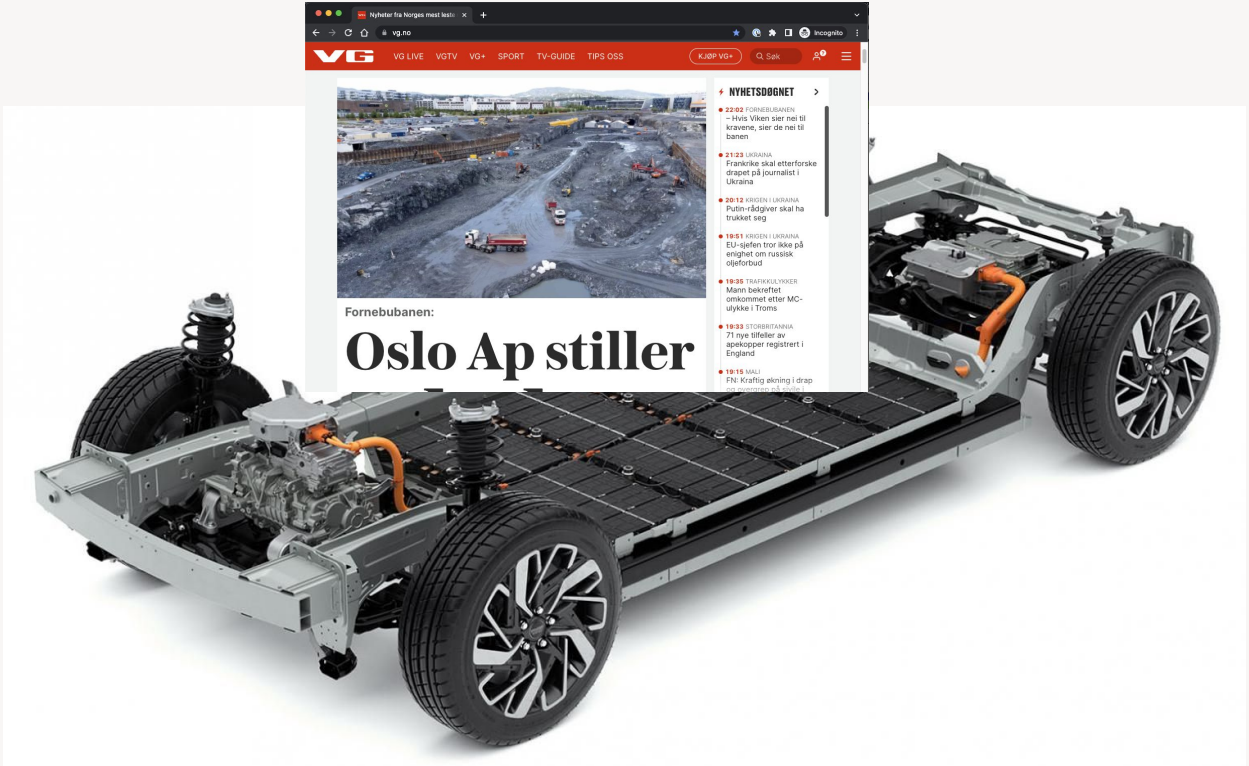
Be non-intrusive

Get high adoption through easy to use tools

Easy to operate / non-intrusive → Hard to operate / intrusive

Hammer (Public Domain): https://en.wikipedia.org/wiki/Hammer#/media/File:Claw-hammer.jpg
Nasa image (CC): https://www.flickr.com/photos/nasa2explore/9807793664

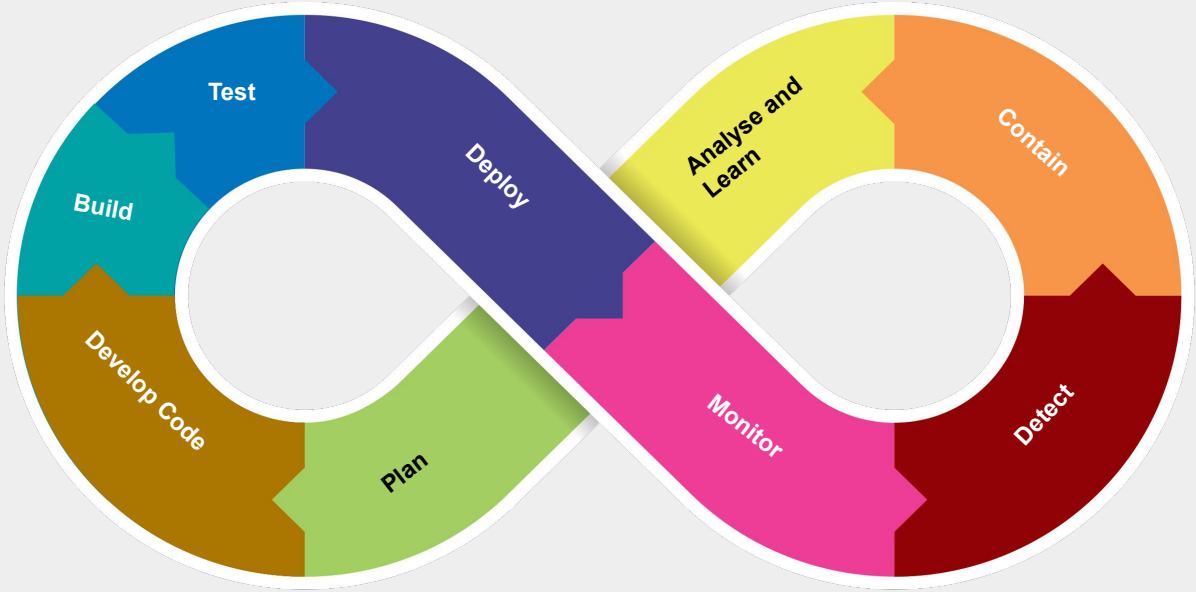
Why we prefer the Golden Path: provide a base



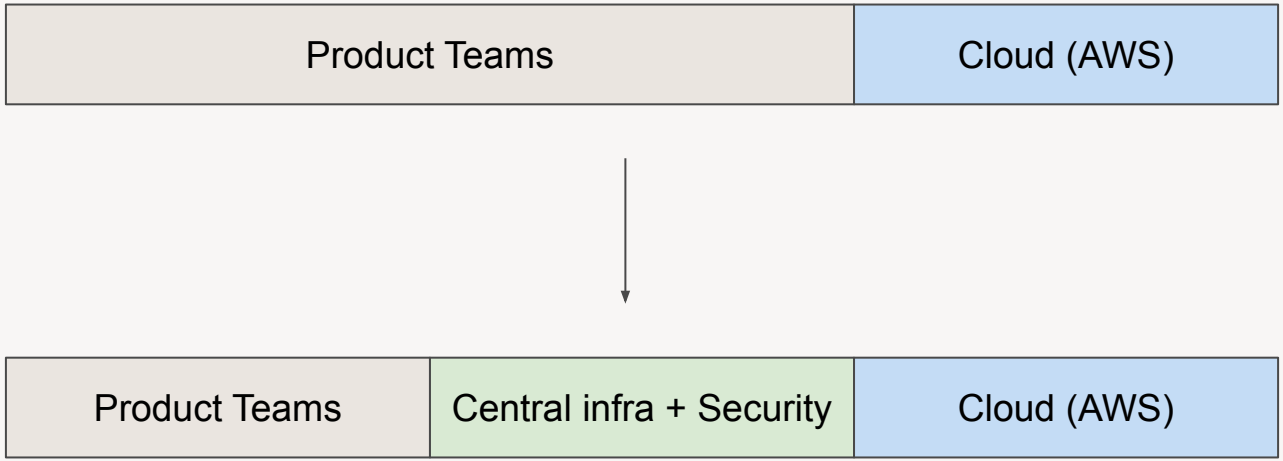
Product teams will be provided a base to build upon

Hyundai and Kia base: https://topgear.com.my/news/hyundai-and-kias-new-electric-car-base-will-go-up-to-600bhp

Security in the SDLC (Software Development Life Cycle)



Shared k8s: Shared responsibility model



Golden path security improvements

AWS Kubernetes (AWS EKS) hardening

- AWS Bottlerocket as host OS: Security & k8s focused OS
- Audit capability for Schibsted’s Security team
- GuardDuty for EKS Protection
- Run auditing tool Kubescape periodically to detect security issues
- Limit network access by deploying Cilium (network isolation, prevent spoofing, ++)
- IP allow listing by default
- WAF and DDoS protection preconfigured with a on/off toggle

What we bought of security capabilities

$

Dynamic Application Security Testing (DAST)

$

detectify

RAPID7 | insightAppSec

BURPSUITE

Probely

netsparker

Detectify

$

- Good UX
- Low false positives
- Quality findings
- Crowdsourcing model
  - Quick to add checks e.g. Log4Shell and Spring4Shell

detectify

AWS GuardDuty

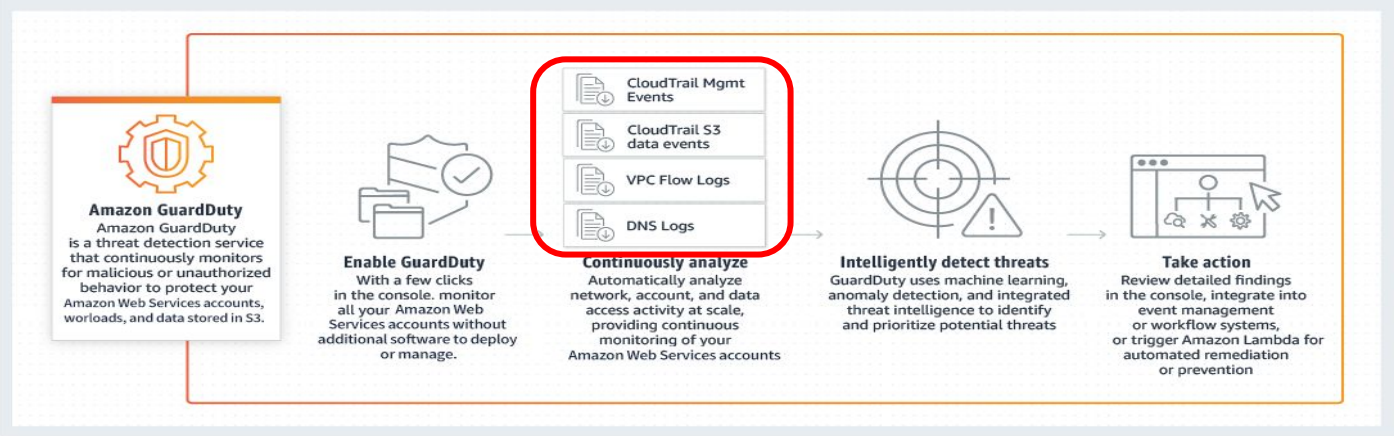
Easy to roll out centrally to 400+ AWS accounts

Identifies basic misconfigurations (i.e. public S3 buckets)

Detects breaches

Low false positives

Great ROI! (~1% AWS spend)



Static Application Security Testing (SAST)

$

Identify insecure code before it is deployed to production, preventing potentially exposing our systems and data to attackers.

snyk

Contrast
SECURITY

SAST solution: GitHub Advanced Security

$

Great Developer experience/UX

- Embedded into existing developer workflows!
- All vulnerability details and data flow analysis accessible inline in Pull requests, No need to leave GitHub for more details
- We can write our own custom checks with CodeQL

```
23 +  @GetMapping("/ping-test")
24 +  public String test(@RequestParam String host) throws IOException {
25 +    Runtime rt = Runtime.getRuntime();
26 +    String cmdString = "ping " + host;
27 +
28 +    log.info("Executing '{}'", cmdString);
29 +    rt.exec(cmdString);
```

Check failure on line 29 in applicationinventory/src/main/java/com/schibsted/security/inventory/api/VulnerableAPI.java

Code scanning

Uncontrolled command line Critical

User-provided value flows to here and is used in a command.

Show more details

Show paths Dismiss

```
30 +
31 +    return "great success!";
32 +  }
33 + }
```

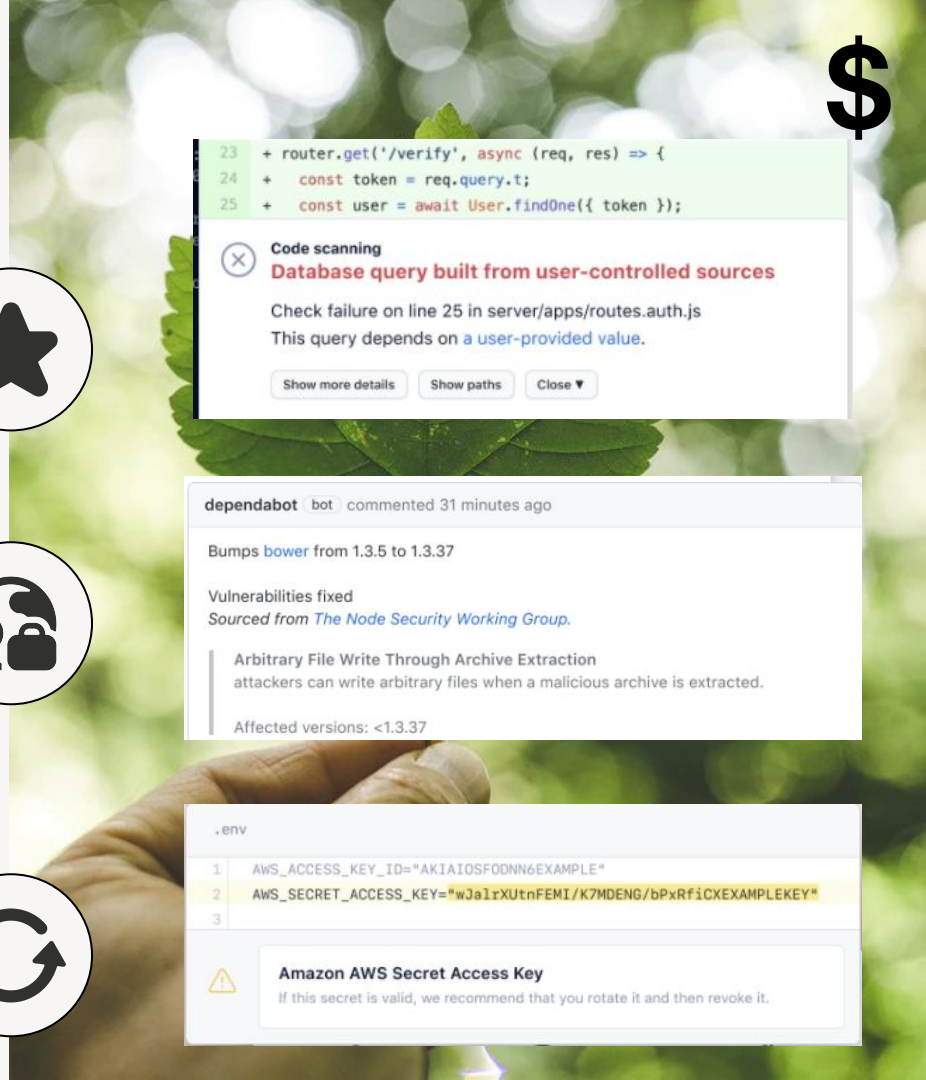
Helps developers directly in Pull request

GitHub Advanced Security

CodeQL scanning finds security holes in your code (SARIF format)

Dependabot **detects dependencies** with security problems

Secret scanning looks for checked-in secrets



Cloud Security Posture Management (CSPM)

Cloud misconfigurations is the most common root cause for data breaches in the cloud.
With a CSPM tool we can help to prevent those in all our cloud environments for all brands.

CloudGuard Check Point SOFTWARE TECHNOLOGIES LTD

PRISMA BY PALO ALTO NETWORKS

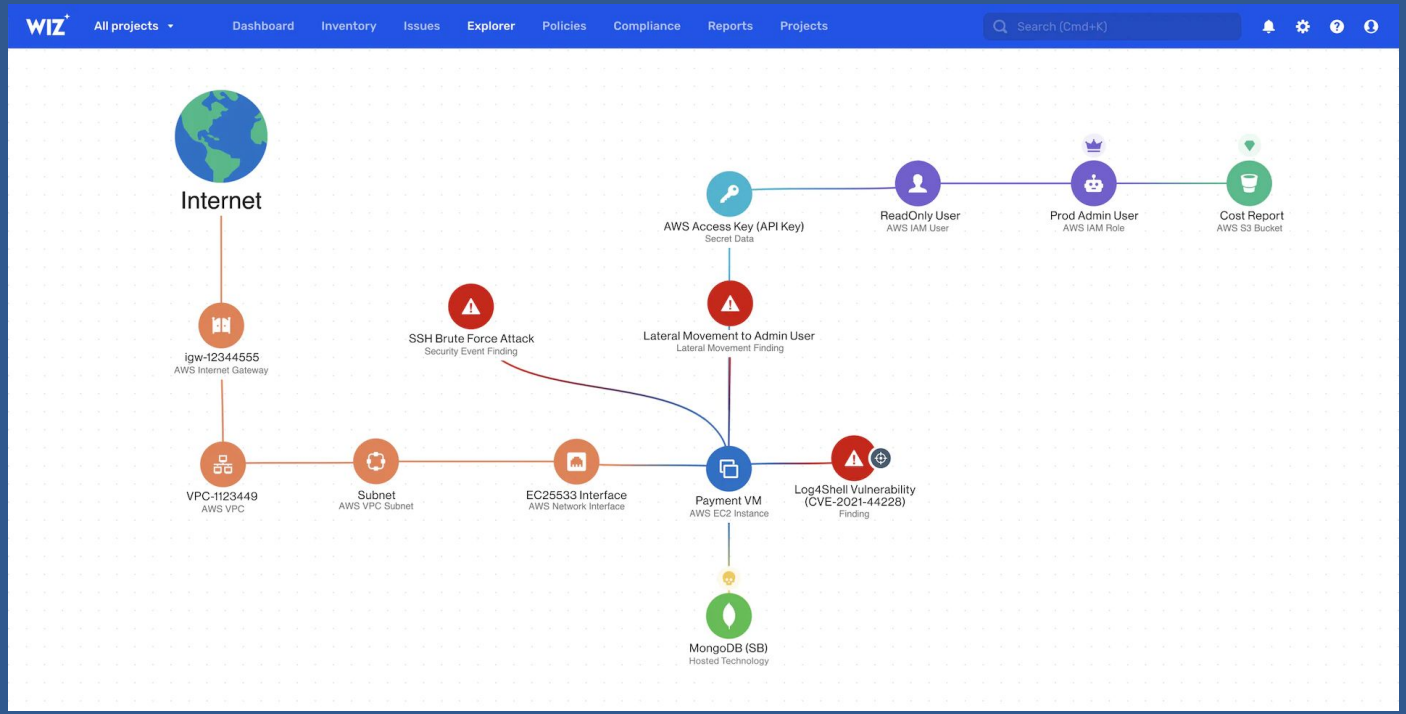
WIZ

CSPM vendors evaluate in collaboration with FINN, News Media, Lendo, Developer Foundations and ETech.

CSPM vendor chosen: Wiz

Vulnerability with public exploit on server with External Exposure and High privileges

Differentiate actual critical findings from other less critical security issues.



Private Bug Bounty program

$

hackerone

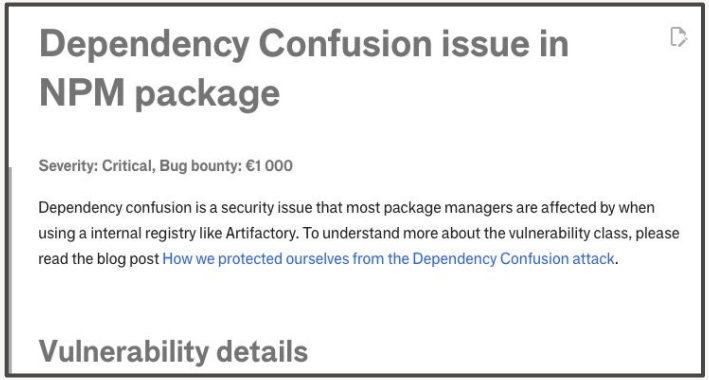
INTIGRITI

ETHICAL HACKING PLATFORM

Private Bug Bounty program

$

- Platform: Intigriti
  - Reason: Cost + Norwegian community
- Currently run 6 private bug bounty programs
- **~1000 domains in scope** across all programs
- 17 Critical findings since September 2022
- Share write-ups internally of the most interesting vulnerabilities
- Great Return of investment, highly recommended!



Dependency Confusion issue in NPM package

Severity: Critical, Bug bounty: €1 000

Dependency confusion is a security issue that most package managers are affected by when using a internal registry like Artifactory. To understand more about the vulnerability class, please read the blog post How we protected ourselves from the Dependency Confusion attack.

Vulnerability details

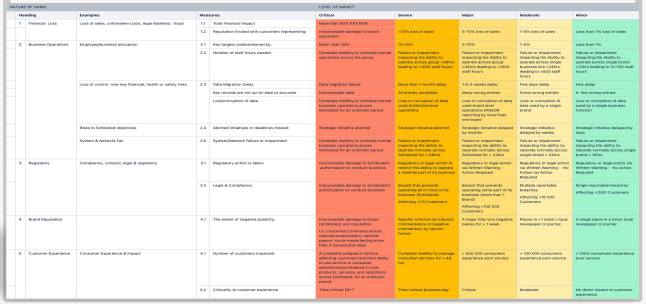
INTIGRITI
ETHICAL HACKING PLATFORM

What money can't buy: Security culture

Defendable Products training package, over 1000 developers trained

1.

HARM assessment



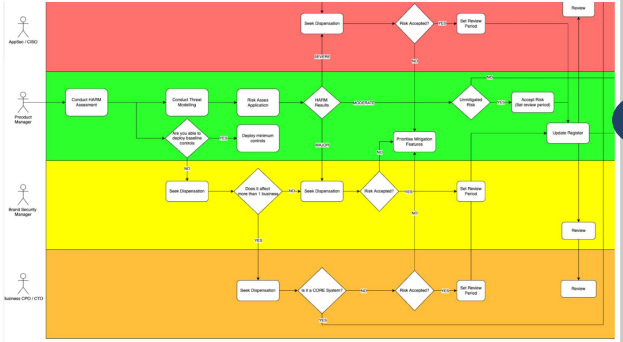
NATURE OF HARM				LEVEL OF IMPACT				
	Heading	Examples	Measures		Critical	Severe	Major	Moderate	Minor
1	Financial Loss	Loss of sales, unforeseen costs, legal liabilities, fraud	1.1	Total Financial Impact	More than XXX XXX NOK				
			1.2	Reputation Eroded with customers representing:	Irrecoverable damage to brand reputation	>10% loss of sales	5-10% loss of sales	1-5% loss of sales	Less than 1% loss of sales
2	Business Operations	Employee/Business disruption	2.1	Key targets undeachieved by:	More than 10%	10-15%	5-10%	1-5%	Less than 1%
			2.2	Number of staff hours wasted	Complete inability to continue normal operations across the group	Failure or Impairment Impacting the Ability to operate across group - wasting >xxxx staff hours leading to >XXX staff hours	Failure or Impairment Impacting the Ability to operate across group - wasting >xxxx staff hours leading to >XXX staff hours	Failure or Impairment Impacting the Ability to operate across single brand - wasting >xxxx staff hours leading to >XXX staff hours	Failure or Impairment Impacting the Ability to operate across single brand - wasting >xx XXX staff hours
		Loss of control over key financial, health or safety risks	2.3	Data Migration Delay	Data migration failure	More than 1-month delay	11to 4 weeks delay	Few days delay	Few delay
				Key records are not up-to-date or accurate	Irrecoverable data	All entries unreliable	Many wrong entries	Some wrong entries	A few wrong entries
				Loss/corruption of data	Complete inability to continue normal business operations across Schibsted for an unknown period	Loss or corruption of data used Schibsted level operations	Loss or corruption of data used brand level operations (Incorrect reporting by more than one brand	Loss or corruption of data used by a single brand	Loss or corruption of data used by a single business function
		Risks to Schibsted objectives	2.4	Aborted initiatives or deadlines missed:	Strategic initiatives aborted	Strategic initiative aborted	Strategic initiative delayed by months	Strategic initiative delayed by weeks	Strategic initiative delayed by days
		System & Network Fail	2.5	System/Network Failure or Impairment	Complete inability to continue normal business operations across Schibsted for an unknown period	Failure or Impairment Impacting the ability to operate normally across Schibsted for > 24hrs	Failure or Impairment Impacting the ability to operate normally across Schibsted for > 12hrs	Failure or Impairment Impacting the ability to operate normally across single brand > 12hrs	Failure or Impairment Impacting the ability to operate normally across single brand > 5hrs
3	Regulatory	Compliance, conduct, legal & regulatory	3.1	Regulatory action is taken:	Irrecoverable damage to Schibsted's authorisation to conduct business	Regulatory or legal action to Schibsted's authorisation to conduct a market or part of its business	Regulatory or legal action Affecting >10 000 Customers - Action Required	Regulatory or legal action Affecting >1 000 Customers - No Follow Up Action Required	Regulatory or legal action via Media Reporting - No Action Required
			3.2	Legal & Compliance:	Irrecoverable damage to Schibsted's authorisation to conduct business	Breach that prevents operating all or most of its business (Schibsted) Affecting >1 0 Customers	Breach that prevents operating some part of its business (Affecting more than 1 Brand) Affecting >100 000 Customers	Multiple reportable breaches Affecting >10 000 Customers	Single reportable breaches Affecting <1000 Customers
4	Brand Reputation		4.1	The extent of negative publicity:	Irrecoverable damage to brand (Schibsted) and reputation i.e. Consumer commerce across Schibsted's portfolio of brands, papers, social media lasting more than 3 consecutive days	Specific criticism by industry commentators or negative commentary by opinion former	A major little runs negative press for > 1 week	Press in >1 minor / local newspaper or journal	A single piece in a minor local newspaper or journal
5	Customer Experience	Consumer Experience & Impact	5.1	Number of customers impacted	A complete collapse in service affecting customers and their ability to access Schibsted's products, services, and operations across Schibsted, for an unknown period	Complete inability to manage consumer services for > 48 hrs	> 300 000 consumers experience poor service	> 100 000 consumers experience poor service	> 1000 consumers experience poor service
			5.2	Criticality to customer experience	Time critical 24/7	Time critical business day	Critical	Moderate	No direct impact to customer experience

2.

Threat modelling Miro board

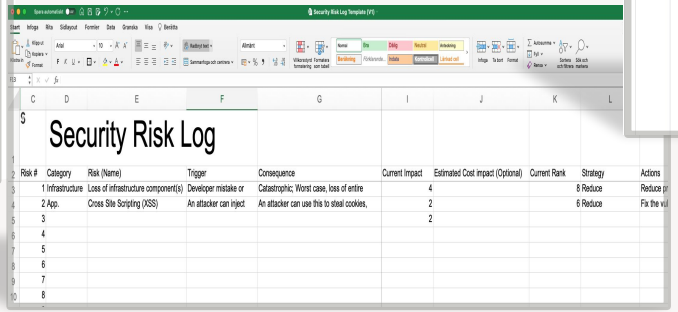
5.

Sharing the risk and getting a exception approval



4.

Risk log

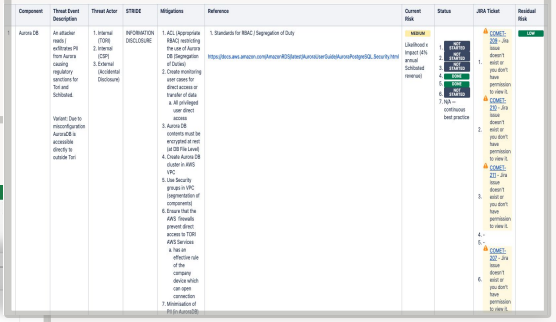


Security Risk Log

Risk #	Category	Risk (Name)	Trigger	Consequence	Current Impact	Estimated Cost impact (Optional)	Current Rank	Strategy	Actions
1	Infrastructure	Loss of infrastructure component(s)	Developer mistake or	Catastrophic, Worst case, loss of entire	4			8 Reduce	Reduce pr
2	App.	Cross Site Scripting (XSS)	An attacker can inject	An attacker can use this to steal cookies,	2			6 Reduce	Fix the vul
3					2				
4									
5									
6									
7									
8									

3.

Threat Model Confluence page



Component	Threat Event Description	Threat Actor	STRIDE	Mitigations	Reference	Current Risk	Status	JIRA Ticket	Residual Risk
1 Aurora DB	An attacker reads / exfiltrates PII from Aurora causing regulatory sanctions for Tori and Schibsted. Variant: Due to misconfiguration AuroraDB is accessible directly to outside Tori	1. Internal (TORI) 2. Internal (CSP) 3. External (Accidental Disclosure)	INFORMATION DISCLOSURE	1. ACL (Appropriate RBAC) restricting the use of Aurora DB (Segregation of Duties) 2. Create monitoring user cases for direct access or transfer of data a. All privileged user direct access 3. Aurora DB contents must be encrypted at rest (at DB File Level) 4. Create Aurora DB cluster in AWS VPC 5. Use Security groups in VPC (segmentation of components) 6. Ensure that the AWS Firewalls prevent direct access to TORI AWS Services a. has an effective rule of the company device which can open connection 7. Minimisation of PII in AuroraDB	1. Standards for RBAC / Segregation of Duty https://docs.aws.amazon.com/amazon-RDS/latest/AuroraUserGuide/AuroraPostgreSQL.Security.html	MEDIUM Likelihood x Impact (4% annual Schibsted revenue)	1. NOT STARTED 2. NOT STARTED 3. NOT STARTED 4. DONE 5. NOT STARTED 6. NOT STARTED 7. NA — continuous best practice	1. COMET-208 - Jira issue doesn't exist or you don't have permission to view it. 2. COMET-210 - Jira issue doesn't exist or you don't have permission to view it. 3. COMET-211 - Jira issue doesn't exist or you don't have permission to view it. 4 - 5 - 6. COMET-202 - Jira issue doesn't exist or you don't have permission to view it.	LOW

Sorry, we couldn't avoid it… we introduced…

Sorry, we couldn't avoid it… we introduced…

Security policies

Policies

This pages links to all the policies related to Product and Application Security.

- Static application security testing (SAST) Policy
- Dynamic application security testing (DAST) Policy
- Cloud Security Posture Management (CSPM) Policy
- Secret scanning Policy
- Software Composition Analysis Policy

SAST Policy

Must

- The code repositories which are associated to the Products classified as Severe, Major or Moderate in a HARM assessment must be on-boarded to a SAST tool.
- The security of the Source Code is the brand/team's responsibility.
- The time to remediate the issues raised by SAST tool is tied to the HARM assessment and severity of the finding. See table below for remediation requirements.

Finding Criticality	HARM Impact Category	Required time (working days) to mitigation or accept risk
Critical	Severe	2 days
High	Severe	7 days
Medium	Severe	14 days
Critical	Major	5 days
High	Major	12 days
Medium	Major	21 days

Cybersecurity program, did we reach our initial goal?

Budget approved

Today

2019 | 2020 | 2021 | 2022

Start

End result:
We have mapped our security capabilities to the NIST levels, and we will were able to hit NIST level 3, **except in three teams**.

NIST Cybersecurity Framework

Minimum Target baseline:
Level 3

Mistakes were made

- Did not negotiate pricing above what we expected
  - Bad negotiation terms, extra approval round internally for extra budget
- Communicate communicate communicate!
  - Some information was not read by key stakeholders, so they caught by surprise with the rollout. Should have done multiple communications
- All tools was not available during the developer training
  - If you have time, roll out security tools/capabilities before doing developer training (we didn't have time to do this in the ideal order)

Plans going forward

- Unified view of vulnerabilities (Vulcan)
- Optimise and tune all security tools
  - Tight timeline in program, so not enough time to tweak everything
- Automated Risk Scoring System
  - Tells teams what their next risk reducing activity should be
- Cloud Security: Deny certain high risky API's
- Launch Security Champion-ish program

The end!

Please reach out! Let's collaborate and share! :)

stale.pettersen@schibsted.com
infosec.exchange/@kozmic
twitter.com/kozmic/