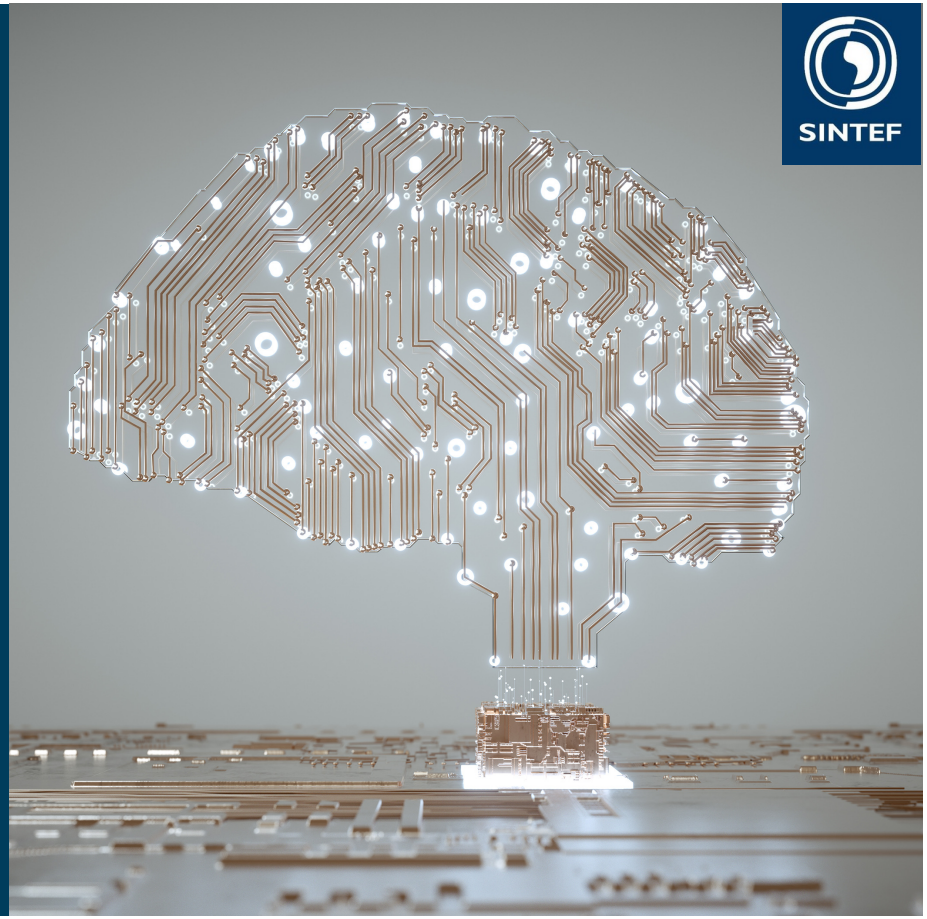
KI i cybersikkerhet: Derfor er ‘sec’ i DevSecOps viktigere enn noensinne i dagens forretningslandskap!

Kamer Vishi
IT-sikkerhetsleder

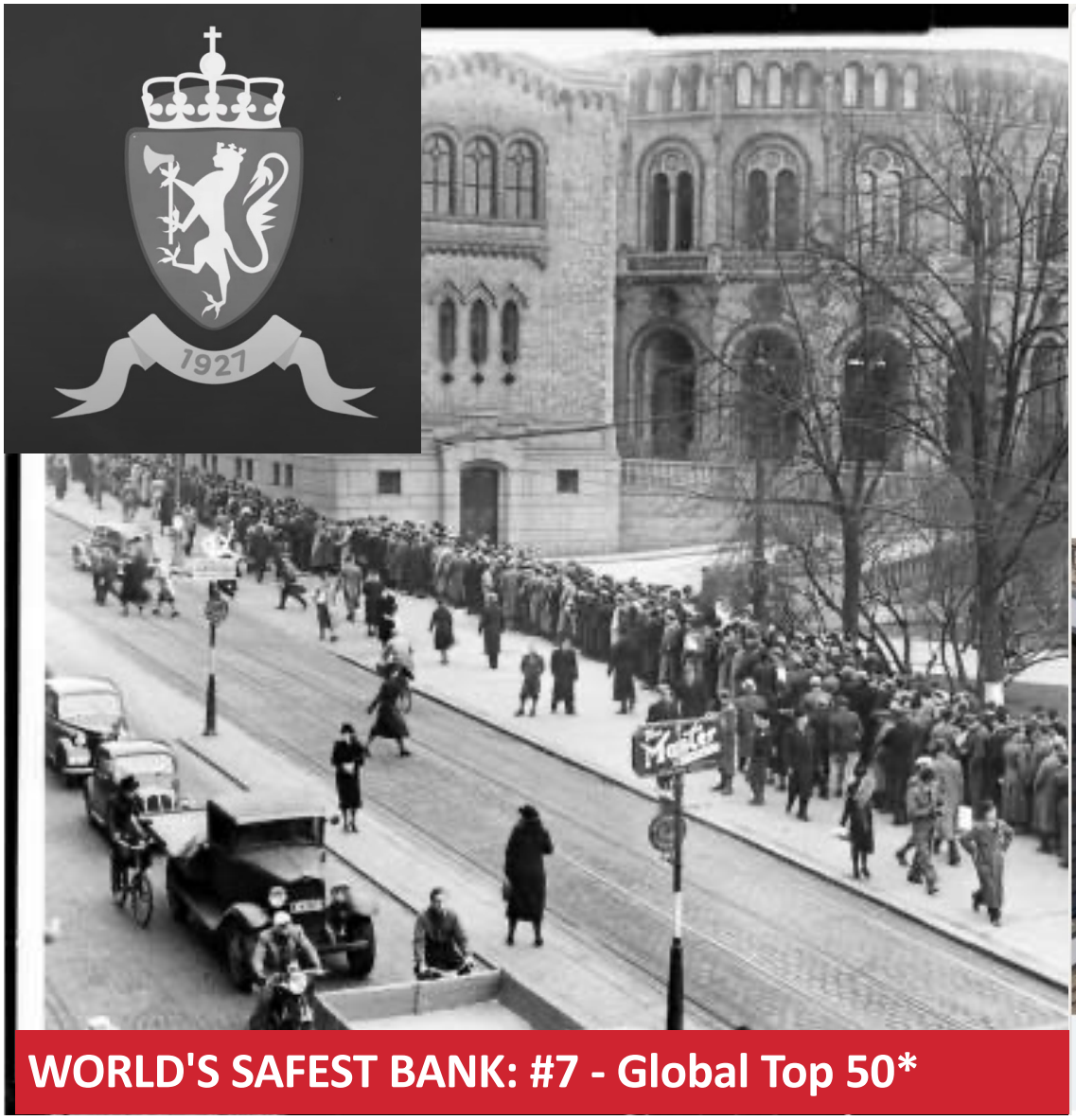
October 24, 2024



/usr/bin$ whoami

- **Kamer Vishi**
- Ph.D. in cybersecurity (IAM/Biometrics) from UiO
- Senior Security Manager at Kommunalbanken
- FIRST.org liaison member
- 15+ years in cybersecurity (Red+Blue Team)
- Former Security & Threat Intelligence Analyst, IR,TH,DE
- AFK: Loves grilling & eating🥩, keyboardist 🎹

kamer.vishi@kbn.com
x.com/cyb5r3Gene
linkedin.com/in/kamervishi



KBN
1,794 followers
3w •

https://www.youtube.com/watch?v=c2d-EEeRukk

Finansdepartementet besluttet fredag at DNB ASA, Kommunalbanken AS, Nordea Eiendomskreditt AS og Sparebank 1 SR-Bank ASA skal anses som systemviktige finansforetak i Norge, i tråd med råd fra Finanstilsynet.

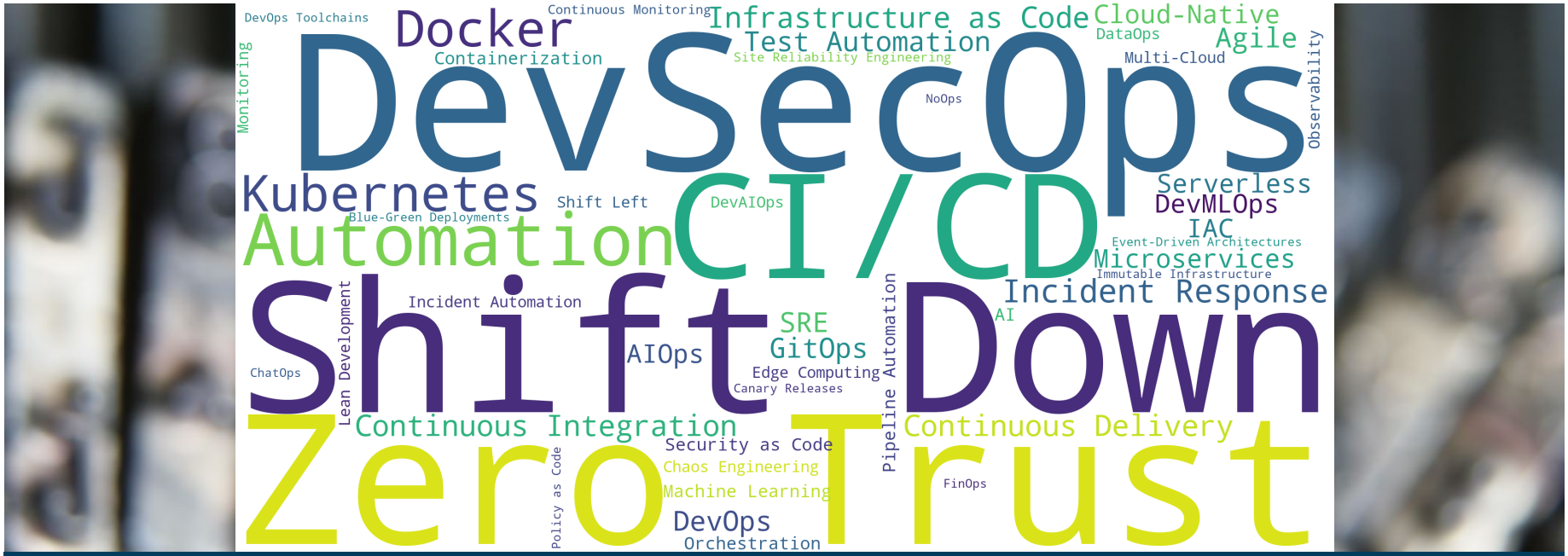
Finansdepartementet beslutter årlig hvilke finansforetak som skal anses som systemviktige. KBN er en systemviktig bank på bakgrunn av samfunnsrollen og posisjonen som den største aktøren i markedet for kommunale lån. Vi skal operere med lav risiko og samtidig ha evne til å bidra med lån uavhengig av økonomiske konjunkturer.

#bank #samfunnsoppdrag #kommunenorge

See translation

Beslutning om systemviktige finansforetak
regjeringen.no • 1 min read

*IMF & Verdensbank



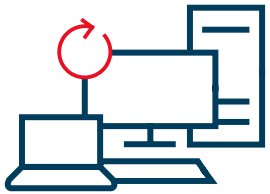
Why are we having this “conversation”?

The importance of “sec” in DevSecOps

Designing for failure: The mindshift

THEN

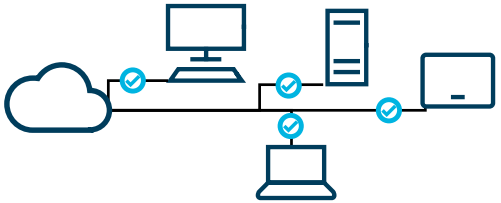
Reliability:
Designed not to fail



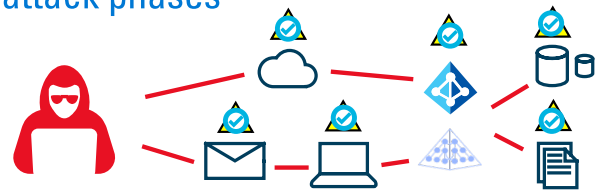
Prevent:
Every possible attack

NOW + AI

Resilience:
Designed to recover quickly



Assume Compromise:
Protect, detect, and respond along attack phases



1940 vs 2024

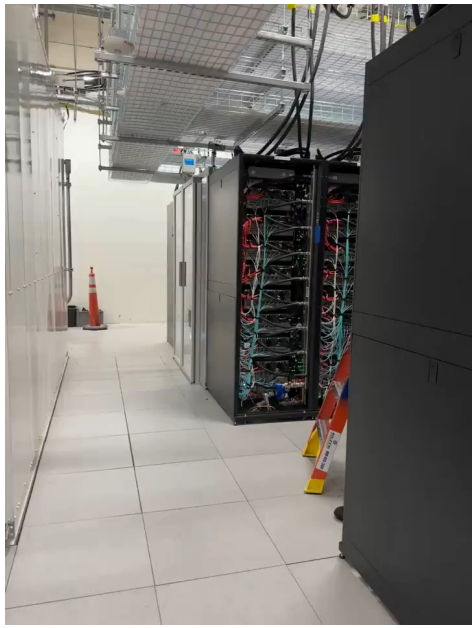
PHYSICAL BATTLE

- Early war production

Image: Bundesarchiv, Bild 183-L04352 / CC-BY-SA 3.0

AI BATTLE

- Cortex: Tesla AI-training supercluster



Video: Elon Musk/X.com

AI today

- Currently helping the tech world with:
  - Faster deployments
  - Improved security
  - Enhanced quality assurance
  - Intelligent monitoring and alerting
  - Predictive analytics

Prioritizations from 5 000 DevSecOps professionals worldwide

AI is a core part of software development

78%

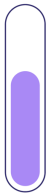
of respondents said they are currently using AI in software development or plan to in the next 2 years, up from 64% in 2023

Organizations are serious about automation

67%

of respondents said their software development lifecycle is mostly or completely automated

The toolchain struggle is real



64%

of respondents said they want to consolidate their toolchain

Software supply chain security is key

67%

of developers said a quarter or more of the code they work on is from open source libraries — but only 21% of organizations are currently using a software bill of materials (SBOM) to document the ingredients that make up their software components

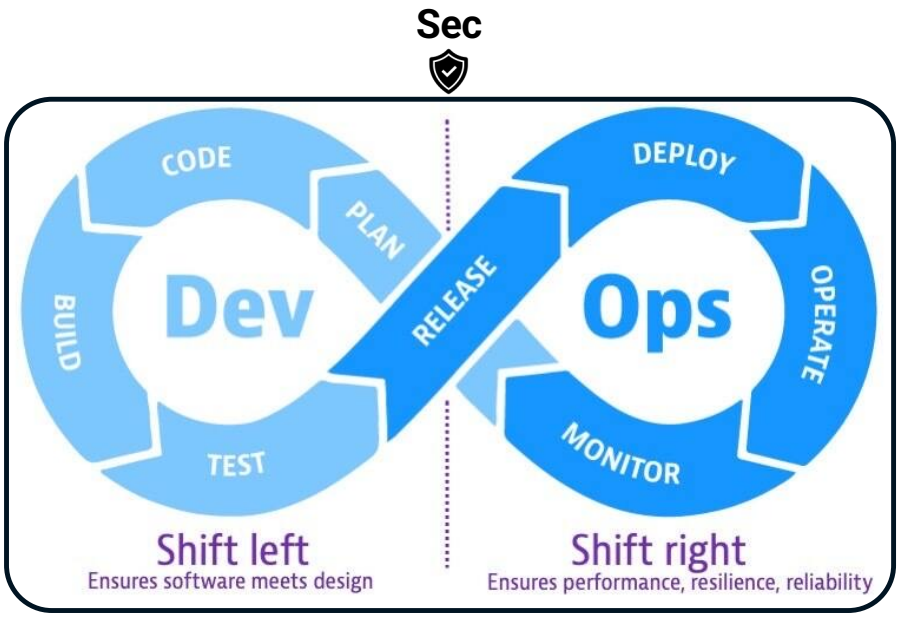
Top IT investment priorities

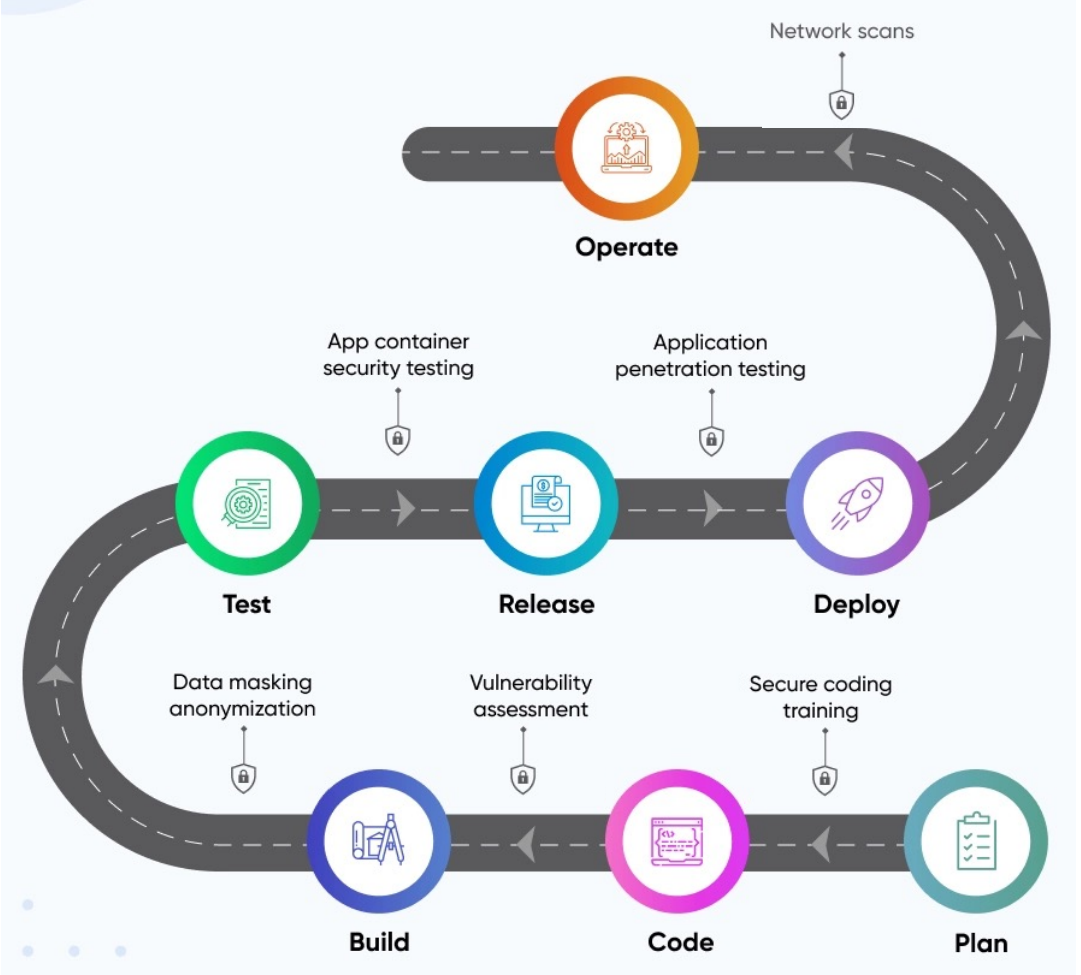
1. Security
2. AI
3. DevSecOps platform
4. Automation
5. Cloud computing

Source: GitLab's Global DevSecOps Report 2024

Rethinking the position: DevSecOps key checkpoints

Shifting too far left = overloaded developers



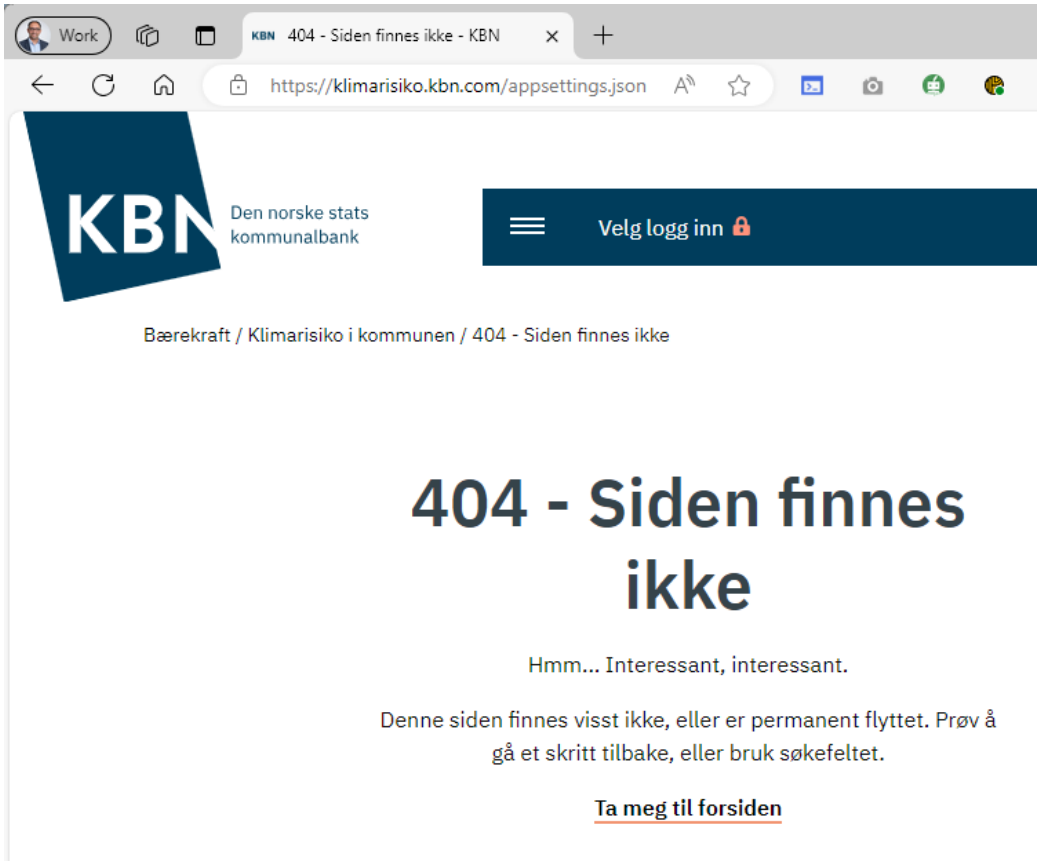


Based on: https://phoenix.security/shift-smart-shift-everywhere/

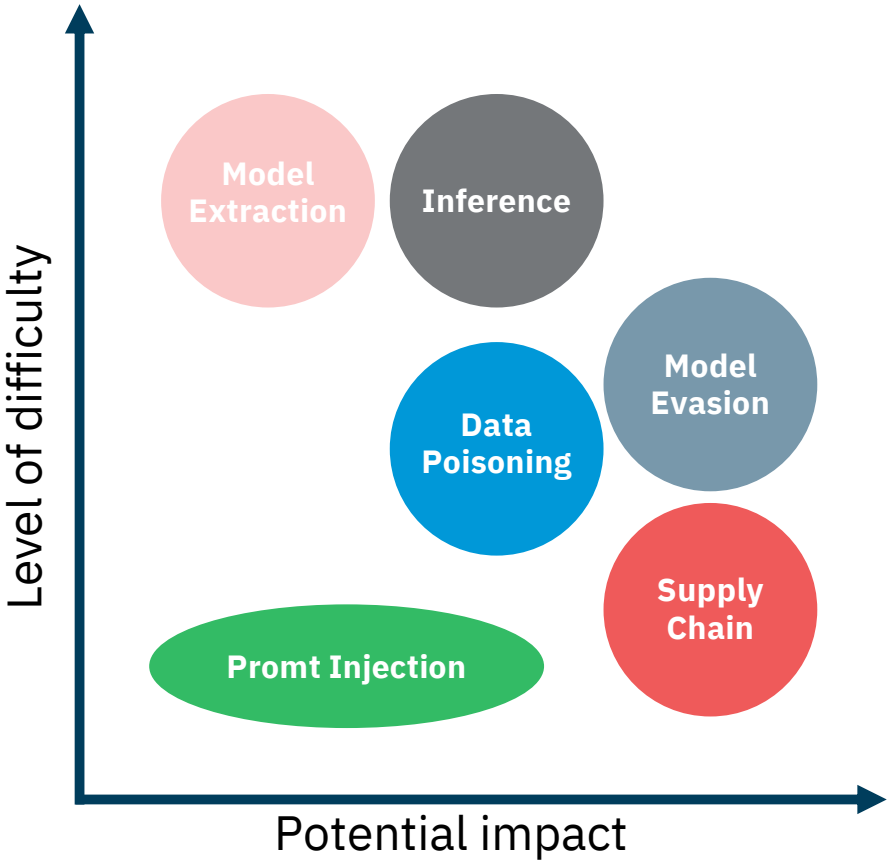
~~Shift Left~~ vs Shift Down

- **Gradual shift to AI-driven tools**
  - The industry's transition towards advanced automation is accelerating with the rise of LLMs and GenAI tools
  - Enhance collaboration and improve developer efficiency throughout the SDLC
- **Shift down,** but **«born left»!**
- **Security-as-Code (SaC)**
- Developers are seeing security scanning increasing across all categories (*SAST, DAST, container scanning, dependency scanning, and license compliance, secret detection*), but this uplift is not translating into vulnerability reduction, as **56% of respondents said it was difficult to get developers to actually prioritize fixing code**. – GitLab survey

AI-code assistant in action



DevSecOps: real threats in the AI era



- **Prompt Injection:** Manipulates AI prompts to bypass restrictions, causing unintended behavior or security risks.
- **Data Poisoning:** Corrupts AI training data, introducing biases or vulnerabilities.
- **Model Evasion:** Alters inputs to trick AI models into misclassifying or making wrong decisions.
- **Model Extraction:** Steals AI model's structure and behavior through extensive querying.
- **Inversion Attacks:** Reconstructs training data or infers private information from model outputs.
- **Supply Chain Attacks:** Targets vulnerabilities in AI-integrated services, plugins, or APIs.

Based on IBM X-Force Red

Cisco on Friday confirmed that some of its files have been stolen after a hacker offered to sell information allegedly belonging to the company.

The hacker known as IntelBroker on October 14 announced a “Cisco breach” on a popular cybercrime forum. The threat actor claimed to have obtained GitHub and SonarQube projects, source code, hardcoded credentials, certificates, confidential documents, Jira tickets, API tokens, AWS private buckets, encryption keys, and other types of information.

Real-world example: XZ utils backdoor (CVE-2024-3094)

Incident

- In 2021, a backdoor was introduced into XZ Utils, a widely-used compression tool, through malicious code in its repository. CVSS-score=10

Impact on CI/CD pipelines

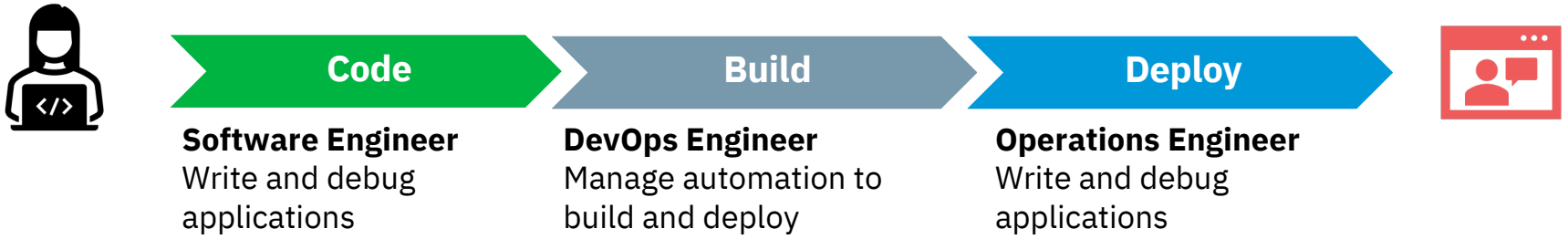
- Could compromise entire deployment pipelines, resulting in backdoored code in production environments.

DevSecOps with AI in practice

- By using AI-code assistants, automated checks can potentially identify unauthorized changes in dependencies, flag unusual commit patterns, and prevent compromised code from being integrated.

Software supply chain

- The software supply chain is composed of the components, libraries, tools, and processes used to develop, build, and publish a software artifact.



Compliance

Security

Sausage-as-a-service (SaaS)

- Modern software contains 80-90% open-source software*
- At least 70% of the containerized workloads are coming from external sources
- 90% of the first level dependencies have dependencies themselves

* Harvard Business School: «The Hidden Vulnerabilities of Open-Source Software”

Courtesy of FIRST VulnCon 2024

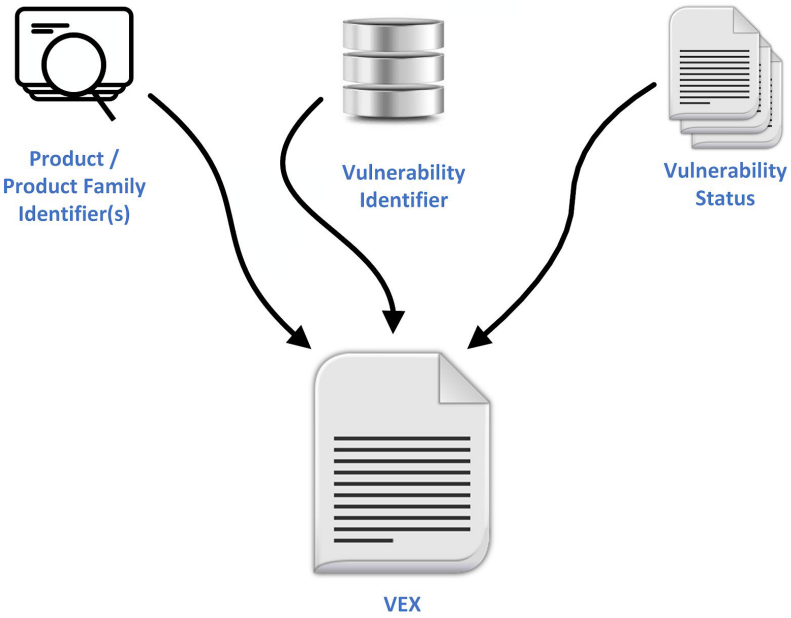
~~AI-powered~~ SBOM

- If the sausage is your software, the SBOM is the list of the ingredients!
- A “software bill of materials” (SBOM) is a comprehensive list of all the *software components*, *dependencies*, *services*, *compositions*, *vulnerabilities*, *extensions* and *metadata* associated with an application (*open source* and *third-party libraries* present in a codebase).
- SBOM standardized format (for automation), CEN/CENELEC (the European Committee for Electrotechnical Standardization) - *EU CRA*

Courtesy of FIRST VulnCon 2024

VEX

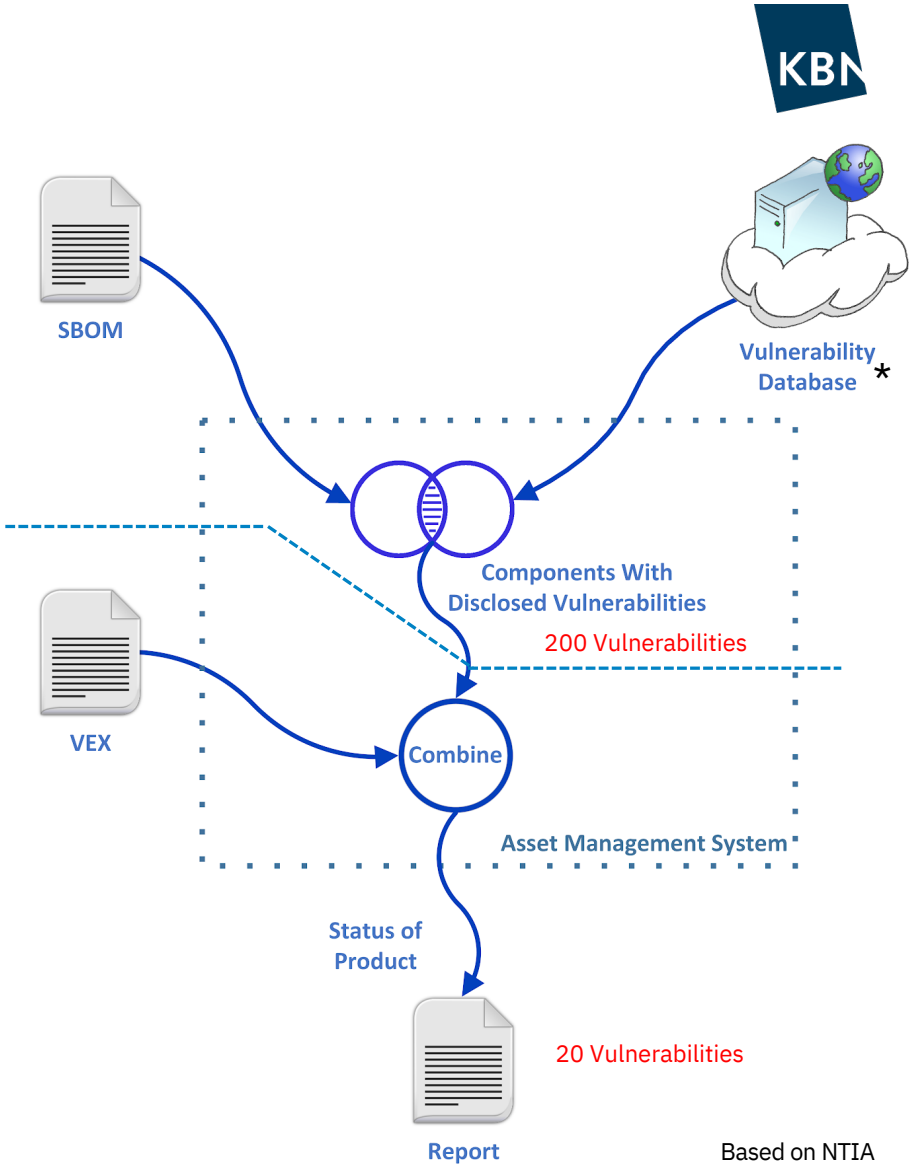
- **V**ulnerability **E**xploitability e**X**change (VEX) is a standardized format for sharing information about vulnerabilities and their exploitability.
- Is a piece of software (component!) actually affected by a vulnerability?
- Claims about impact from a particular author
- Can come from the supplier or a third party
- Many but not all use cases associated with SBOM
- Separate from SBOM, but linkable



Based on NTIA

SBOM + VEX example

- Software includes a vulnerable component
- SW supplier determines that the vuln doesn't affect the built software
  - E.g., relevant code isn't included by compiler
  - E.g., relevant code is present, but not used or exposed
- Supplier issues a VEX with the claim that the component is "not affected" and no action is required
- Consumer integrates SBOM data, vulnerability data, and VEX data to make some risk-based decision



Based on NTIA

* enisa.europa.eu/topics/vulnerability-disclosure
cisa.gov/known-exploited-vulnerabilities-catalog

AI-assisted SDLC capabilities

	Dev	SecOps	Everyone
Available features	Code suggestions Suggested reviewers Summarize MR changes Summarize my MR review	Explain this vulnerability Generate tests in MRs Explain this code	Issue comment summaries Value stream forecasting
Value	Ship software faster: Dev teams can code more efficiently and securely	Secure your end-to-end software supply chain: Faster and precise way to detect and resolve incidents	Improved collaboration throughout the SDLC: Increase velocity with automation and visibility

Kommunalbanken (KBN) har finansiert flere fremkomstmidler og kulturelle landemerker i Norge. Hvilke er de mest kjente prosjektene som KBN har vært med på å finansiere?

ⓘ Start presenting to display the poll results on this slide.

TAKK FOR MEG!

kamer.vishi@kbn.com

vishi.no

@cyb5r3Gene

/in/kamervishi