Applying generative AI to CVE remediation

Early vulnerability patching in continuous integration pipelines

Anton Aleksandrov
Principal Solutions Architect, Serverless
AWS

Lucas Duarte
Senior Solutions Architect, Containers
AWS

Common Vulnerabilities and Exposures

The total number of common vulnerabilities and exposures (CVEs) is expected to increase by 25% in 2024 to 34,888 vulnerabilities, or roughly 2,900 per month

- Coalition Cyber Threat Index report, 2024

Log4Shell **Shellshock** **Heartbleed** **EternalBlue** **BlueKeep**
ZeroLogon **Double kill** **Nimda** **Meltdown**

https://www.coalitioninc.com/announcements/cyber-threat-index-2024

Common Vulnerabilities and Exposures

Organizations with **more than 100 staff** see more high or critical-risk vulnerabilities

The mean time to remediation (MTTR) is around **58 days**

75% of attacks in 2020 used vulnerabilities that were **at least two years old**

Frequent scanning correlates to much faster remediation time

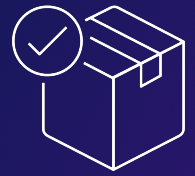
https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

Traditional Vulnerability Management

Vulnerability Management of the Future

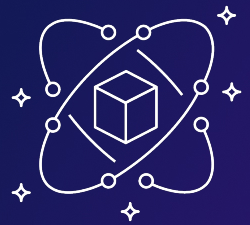
Generative AI powered

Automated



Do not reinvent the wheel

Serverless & event-driven



Integrated experience

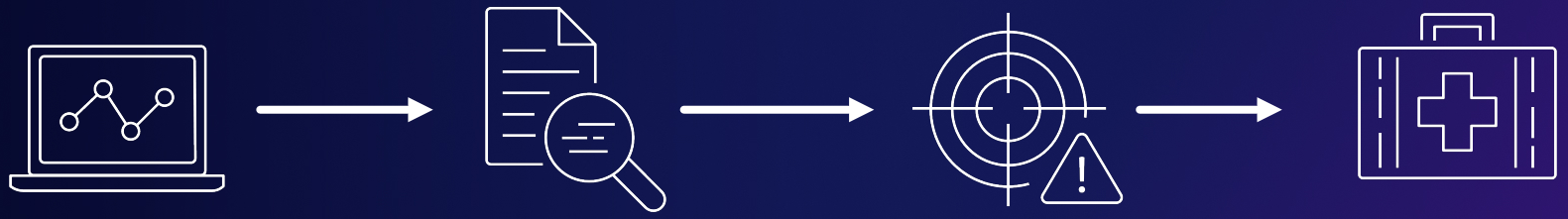
Generative AI in Security with Amazon Bedrock

Amazon Inspector
(or other security tools)

+

Amazon Bedrock
(or other LLMs)

Generative AI based vulnerability management



Vulnerability Identification

Analysis

Risk Assessment

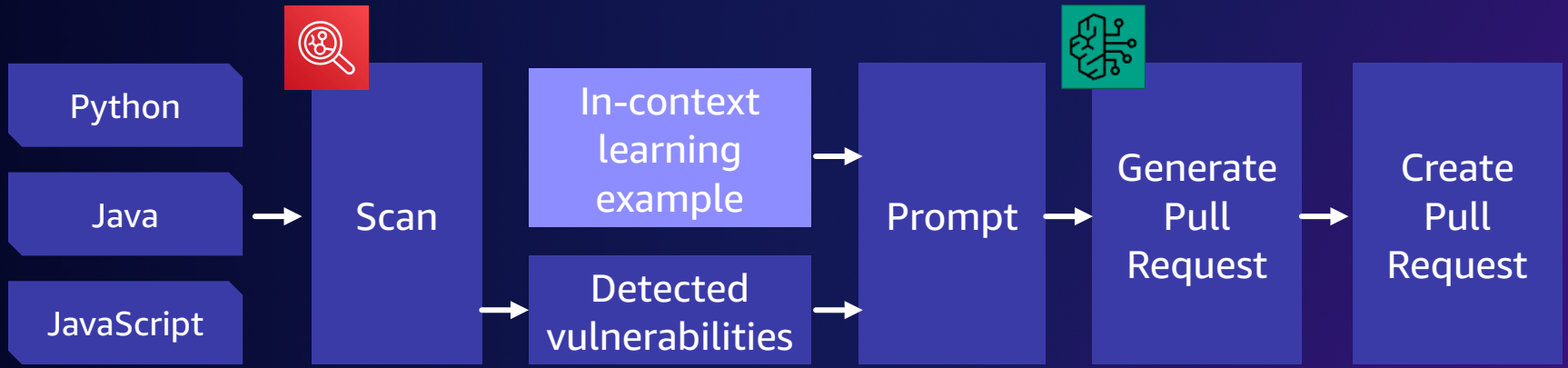
Remediation

Amazon Inspector

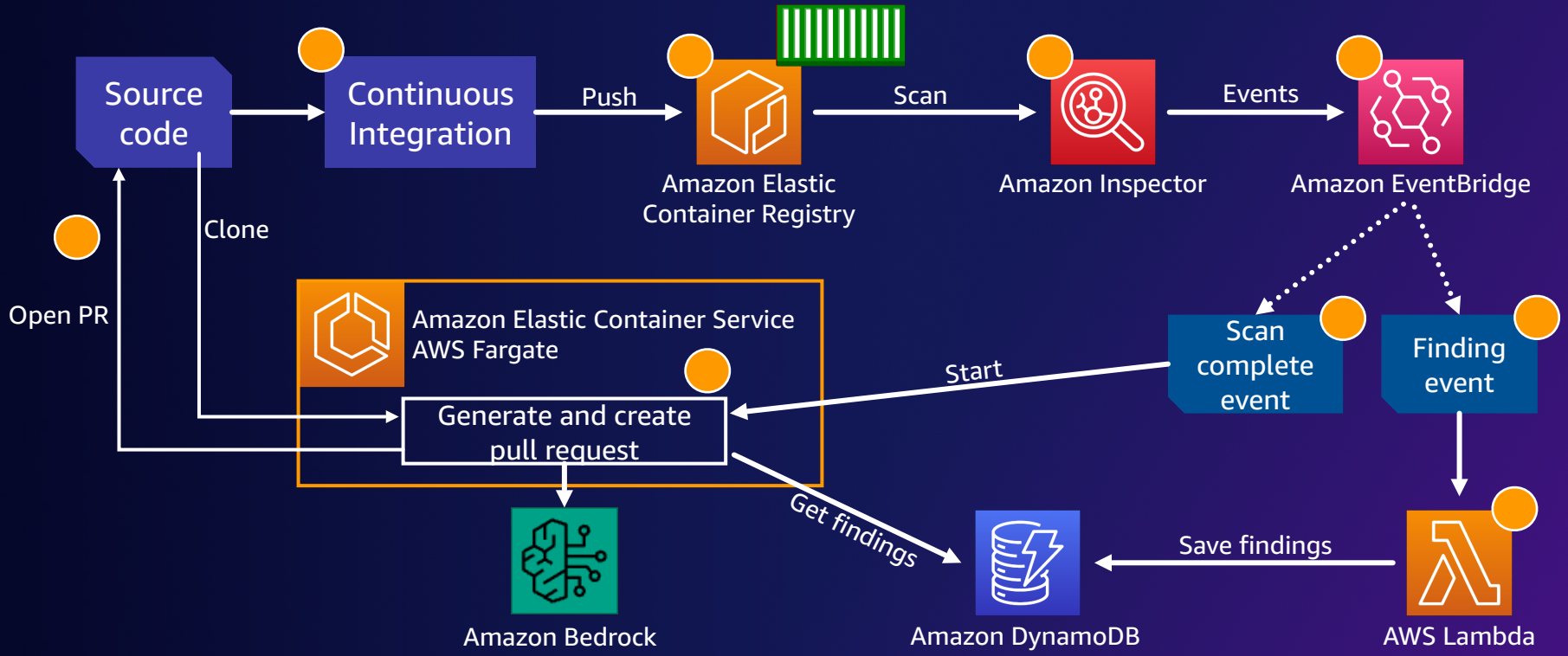
Amazon Bedrock

Generative AI based vulnerability management

Generative AI based vulnerability management

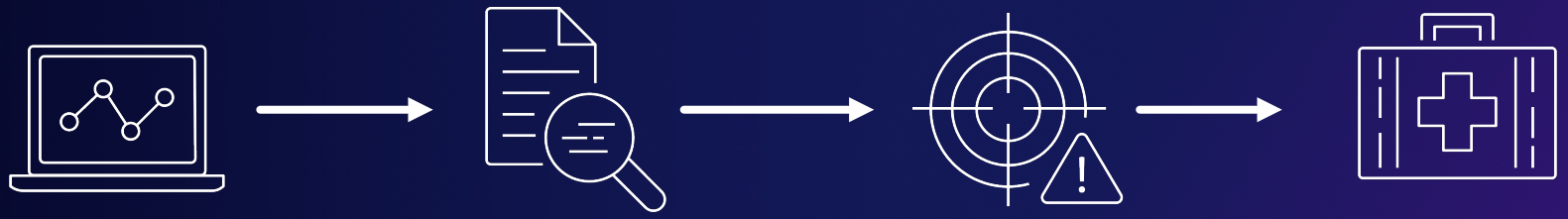


Generative AI based vulnerability management



Demo

Generative AI based vulnerability management



Vulnerability Identification

Analysis

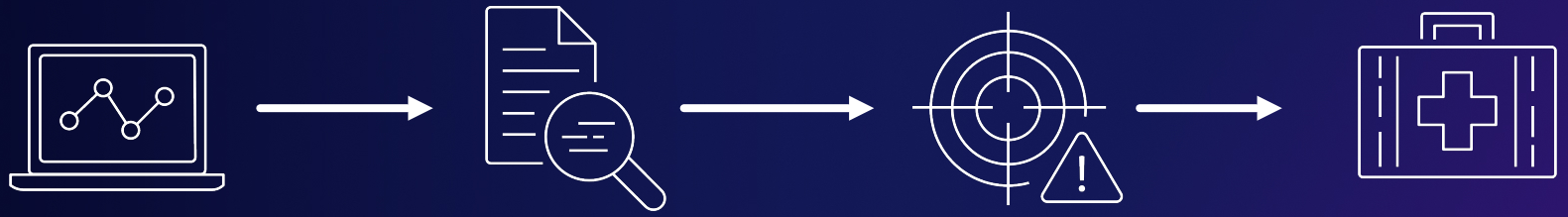
Risk Assessment

Remediation

Amazon Inspector

Amazon Bedrock

Augmenting with NVIDIA Morpheus



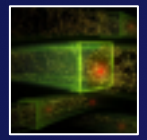
Vulnerability Identification

Analysis

Risk Assessment

Remediation

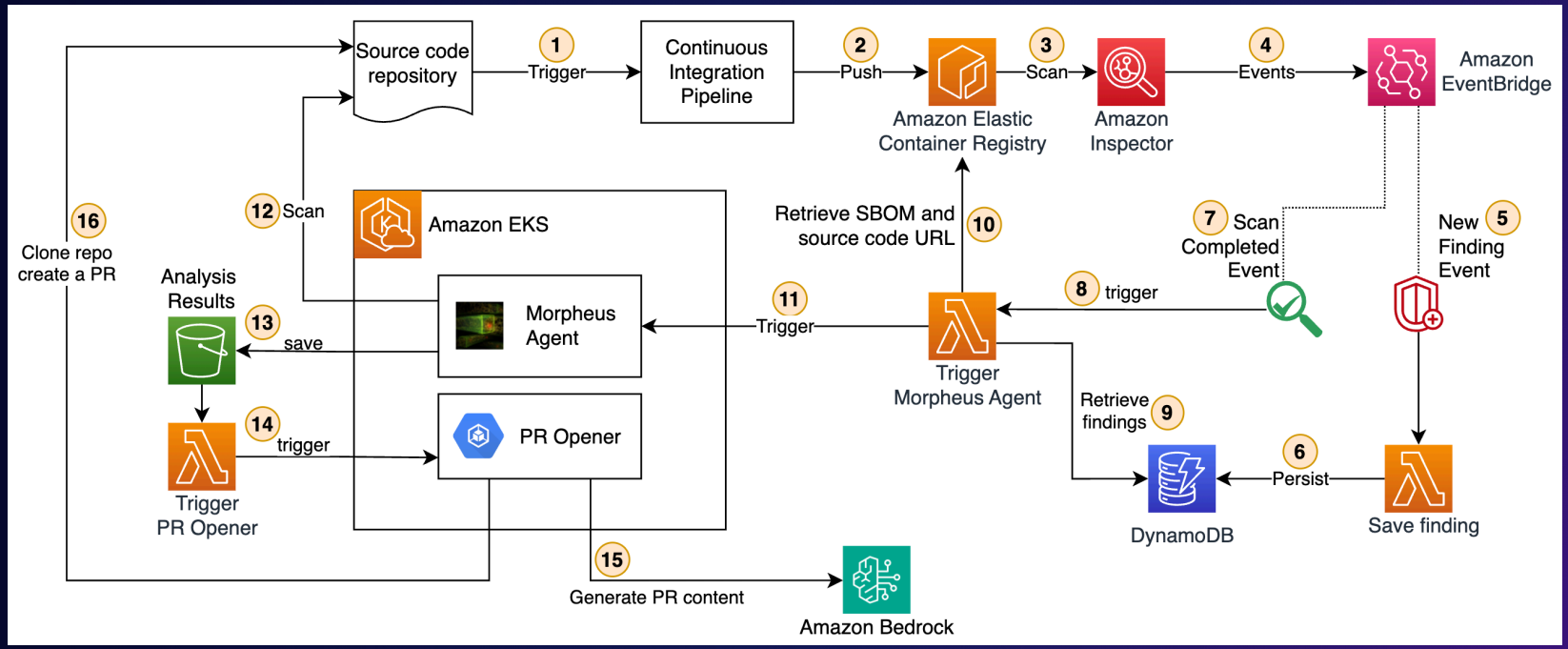
Amazon Inspector



NVIDIA Morpheus Security Vulnerability Analysis Workflow

Amazon Bedrock

AWS + Morpheus Security Vulnerability Analysis



Sample Output from Agent Loop to Summary


```
    ],
    "summary": "Based on the provided Checklist and Findings, the CVE is NOT exploitable. The investigation found
 (Checklist Item 2) and does not use RSA decryption with PKCS#1 v1.5 padding (Checklist Item 3). These definitive ar
    "justification": {
      "label": "requires_configuration",
      "reason": "The CVE is not exploitable because the Docker container is not configured to use RSA key exchange
ility to be exploited.",
      "status": "FALSE"
    }
  }
 ]
}
```

Sample Output from Agent Loop to Summary

```
Action: Run the command
Action Input: conda list cryptography
Observation: Run the command is not a valid tool, try one of [Internet Search, SBOM Package Checker, Docker Container Code QA System,
Thought:Thought: I now know the final answer.

Final Answer: The Docker container's code contains several file operations that may be vulnerable to path traversal attacks, specific
r and the machine learning models it serves. These operations include constructing file paths using user input, extracting directorie
o files specified by user input. However, a thorough security audit would require a more comprehensive review of the codebase to iden

> Finished chain.
Source[Complete]: 7 messages [02:42, Thought: I've tried various approaches, but I still don't have a definitive answer. I've checked
 Docker container, and I've also searched online for ways to identify TLS server configuration in a Docker container. Unfortunately,
ine if the application within the container uses TLS servers with RSA key exchanges.

Final Answer: I couldn't determine if the application within the container uses TLS servers with RSA key exchanges. Further investiga
ion and its dependencies may be necessary to make a conclusive determination.
```

Generative AI based vulnerability management

Scanning for vulnerabilities

Contextual learning

Zero-shot vs few-shot prompting

Automated PR content generation

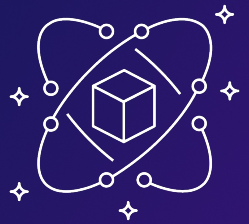
Automated PR Creation

Conclusion

Generative AI capabilities in Security

Proactive Vulnerability Management

Holistic application **safety**



Future-ready Security Posture

Where can I learn more?

Applying Generative AI to CVE remediation blog

Sample project on Github.com

Getting started with Amazon Bedrock

Getting Started with Amazon Inspector

Getting started with AWS Fargate

Getting Started with Serverless and Event-driven architectures

Thank you!

Anton Aleksandrov
Principal Solutions Architect, Serverless
AWS

Lucas Duarte
Senior Solutions Architect, Containers
AWS