AWS re:Inforce

JUNE 13 - 14, 2023 | ANAHEIM, CA

TDR441

How to run security incident response in your Amazon EKS environment

Daniel Begimher

Senior Security Architect,
Global Services Security
AWS

Patrick Gaw

Principal Security Consultant,
Global Services Security
AWS

Purpose and agenda

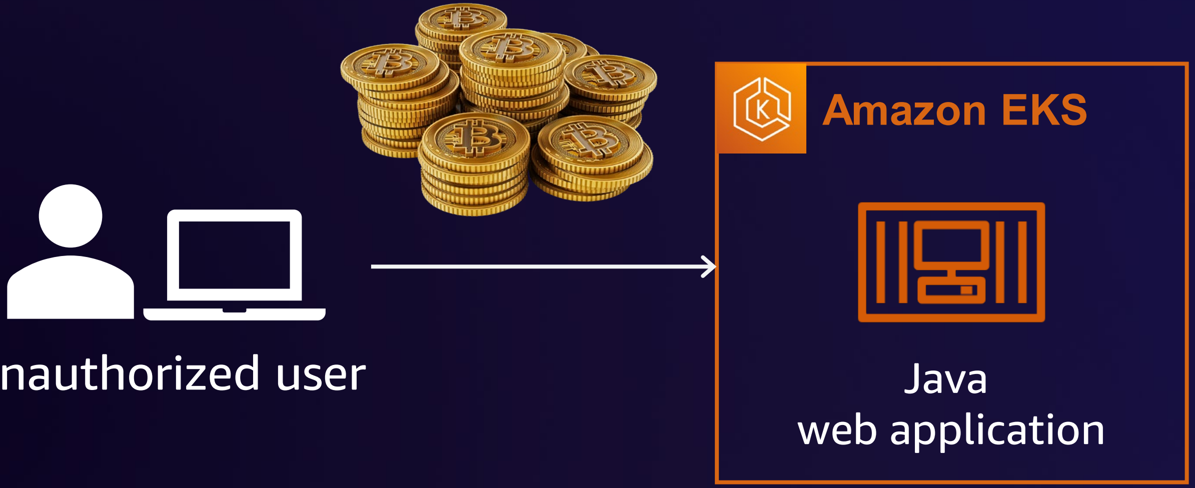
Purpose

Provide insight into how to respond and recover from a security event in Amazon EKS

Agenda

- Scenario overview
- Live demo and coding
- Q&A

Scenario overview: unauthorized user



Unauthorized user

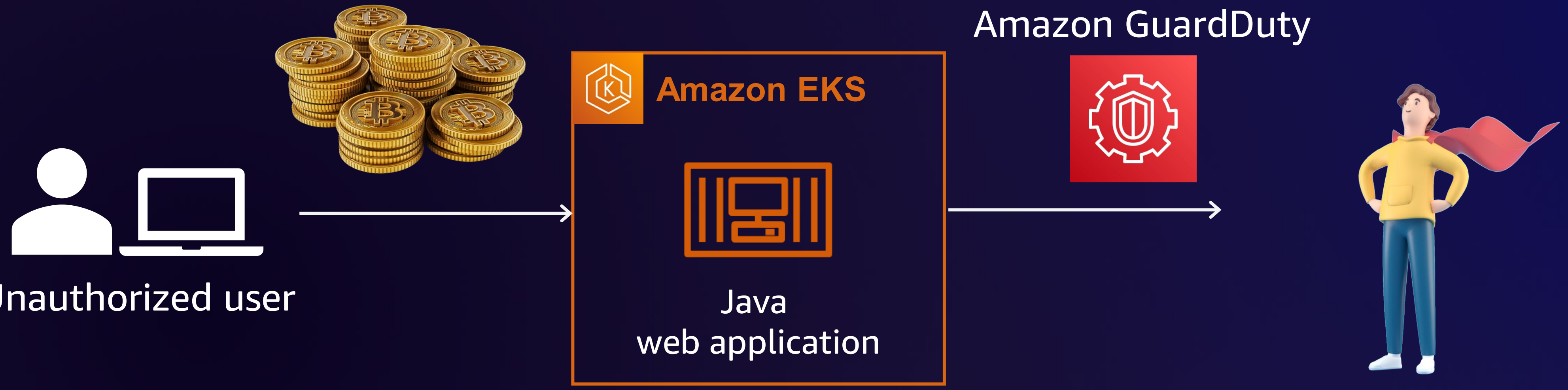
Amazon EKS

Java
web application

The unauthorized user does the following:

- Finds a vulnerability in Banana Corp’s web application
- Delivers an exploit to gain initial access into the running web application
- Determines the application is running on Kubernetes
- Determines that the unauthorized user has privileged access to the Kubernetes API
- Spins up new pods to mine for crypto

Scenario overview: defender



The defender uses his incident response playbook and does the following*:

- Reviews the details of the GuardDuty alerts
- Confirms the security incident based on indicators of compromise
- Checks various other log sources
- Performs containment steps
- Implements forensics and recovery

**Disclaimer:* given the time constraints of this talk, we won't be able to cover every one of these steps in full detail and leave some steps to the exercise of the participants to go and dive deeper on. The detailed steps that follow are aligned to AWS recommended best practices. It's recommended that you tailor your incident response procedures to your organization's specific needs.*

Live demo and coding time!

Discussion:
What could we have done to prevent this from happening?

Thank you!

Please complete the session survey in the mobile app