# Ongoing Monitoring of CI/CD: Automatically Finding Threats

## Introduction

In our last reading about cybersecurity incident detection methods, you explored ways to discover threats. ...

## Automation for Finding Threats

CI/CD pipelines help you release software faster, but they can also open up new vulnerabilities...

## Common Indicators of Compromise (IoCs) in CI/CD Pipelines

Understanding common CI/CD IoCs helps you monitor effectively and quickly find security incidents...

## Proactive Security Through Monitoring for IoCs

Ongoing monitoring of CI/CD pipelines, focusing on automated anomaly detection...

## Using Automation to Find Anomalies and IoCs

To monitor CI/CD pipelines and automatically find threats, you can use these methods:

## Comprehensive Logging and Auditing

Detailed logs are the bases of monitoring...

## Security Information and Event Management (SIEM) Integration

Connecting your CI/CD logs to a SIEM tool can help automatically find anomalies...

## Real-time Alerting and Notifications

Automated alerts make sure security teams are notified right away about unusual activity...

## Performance Monitoring to Find IoAs and Discover IoCs

Performance monitoring, while mainly used to make sure things are running smoothly...

## Continuous Vulnerability Scanning

Regularly checking the CI/CD infrastructure for weaknesses can proactively find vulnerable parts...

## Key Takeaways

Using automation to monitor your CI/CD pipelines, you can find unusual activity and identify important Indicators of Compromise...

## Resources

1. Optimizing logs for a more effective CI/CD pipeline: https://coralogix.com/blog/optimizing-logs-for-a-more-effective-ci-cd-pipeline/  
2. Streamline Your CI/CD: https://www.latesttechinsights.com/2024/04/streamline-your-cicd-hands-on-anomaly.html  
3. What is CI/CD? https://www.threatintelligence.com/blog/continuous-integration-continuous-delivery  
4. CI/CD & DevOps Pipelines: https://www.splunk.com/en\_us/blog/learn/ci-cd-devops-pipeline.html