An Introduction to Detection Engineering

Author: Nils Kannengiesser, Germany

Abstract:

Effective cyberattack detection requires more than collecting logs and deploying monitoring tools. Security teams need to translate relevant threat scenarios into observable events, identify suitable data sources, and maintain detection rules as systems and attacker behaviour change. Detection engineering provides a systematic approach to connecting these tasks and supporting continuous improvement in security operations.

This presentation introduces the detection engineering lifecycle, from the identification of detection requirements and suitable telemetry to the development, testing, and refinement of detection rules. Using Wazuh as a practical example of a security information and event management (SIEM) platform, it examines how agents collect events, how decoders extract relevant fields from log data, and how rules use this information to generate security alerts. Particular attention is given to the relationship between threat scenarios, available telemetry, and detection logic, as well as the distinction between an observed event, an alert, and a confirmed security incident. Feedback from security operations teams is considered an essential input for reducing false positives and adapting detections to operational requirements.

The presentation also explores the role of artificial intelligence (AI) in supporting detection engineering, including assistance with decoder and rule configuration and the enrichment of alerts with additional context. These applications are discussed alongside their limitations, including unreliable assessments, the exposure of sensitive data, and prompt injection through untrusted input. The discussion emphasises the importance of validating generated configurations and checking automated assessments against the available evidence before using them to inform security decisions.

By connecting threat analysis, technical implementation, and operational feedback, the presentation provides a structured introduction to developing and maintaining detection capabilities. It establishes a basis for understanding the detection engineering lifecycle and assessing where AI assistance can contribute to security operations and where human expertise remains essential.

Keywords:

Detection Engineering, Security Monitoring, SIEM, Wazuh, Threat Detection, Artificial Intelligence.