Scalable Incident Response with Automation, Orchestration, and AI/ML

NANOG 88 – Seattle, WA

Introduction

- Highlight the growing complexity and scale of cyber attacks
- The need for efficient, accurate, and rapid incident response
- We’ll explore the role of automation and orchestration including AI/ML and SOAR based approaches to incident response

Challenge

- Better network telemetry has increased volume and lowered signal to noise ratio
- We now have too much data for human operators to analyze efficiently
- Multi-vendor tools that don’t talk to each other – no integrated end-to-end tool chain

Legacy tools

- Security Orchestration, Automation, and Response (SOAR)

- Security Information and Event Management (SIEM)

- Endpoint Detection and Response (EDR/XDR)

AI/ML to the rescue!

- No, ChatGPT cannot solve this problem for you (yet!)
- AIOps – leveraging big data and ML
- Reduced response times via AI-driven data analysis and event correlation
- Continuous learning algorithms = smart(er) anomaly detection
- Automated workflows and root cause analysis

AI/ML + SOAR

- AI/ML is focused on analyzing big data sets to efficiently find the signal in the noise
- SOAR is focused on automating and orchestrating incident response
- The integration of AI/ML and SOAR enables efficient, automated responses 24/7

Best practices

- Automate high-impact, low-risk tasks first
- Develop and refine automation playbooks that work for your environment, policies, toolkits
- Push vendors to work together via open standards to enable seamless tool-chain integration

Relevant Standards

- OpenC2 - a standardized language for the command and control of technologies that provide or support cyber defenses
- TAXII - a free and open transport mechanism that standardizes the automated exchange of cyber threat information
- STIX - a language and serialization format used to exchange cyber threat intelligence (CTI)
- OpenAPI (OAS)

Real World Example:

- Will document a real world scenario and how AI/ML and SOAR work together to automate incident response
- Will reference Fortinet tools including FortiAIOps and FortiSOAR, but the concepts will apply to any tools
- This will not be a live demo, but rather a discussion of how these tools work together to solve a real world incident response

Thank you

14 June 2023

NANOG™