Technica™
Innovation In Action

BROCHURE
10.2023

AIOps for DCO

Artificial Intelligence for IT Operations (AIOps) for Defensive Cyber Operations (DCO)

INTRODUCTION

AIOps (Artificial Intelligence for IT Operations) offers several benefits for Defensive Cyber Operations (DCO) which involve protecting an organization's digital assets and system from cyber threats and attacks. By leveraging artificial intelligence and machine learning. AIOps enhances and automates the ability to detect, respond to, and mitigate cybersecurity threats with unmatched speed and accuracy. Its proactive vulnerability and threat detection capabilities allow for the identification of anomalies and potential threats in real-time, while automation streamlines incident response and remediation, reducing the critical time gap between detection and mitigation.

AIOps also contributes to predictive analysis, helping organizations preemptively address vulnerabilities and threats before they can be exploited. By integrating with network sensors, Security Information and Event Management (SIEM) systems, and threat intelligence feeds, AIOps provides a comprehensive, up-to-the-minute view of security events and threat vectors, facilitating quicker responses and informed decision-making. Moreover, it offers the potential for continuous improvement through resource optimization and insights into the effectiveness of security measures, ensuring organizations can adapt to evolving cyber threats with greater efficiency and precision.

By leveraging AIOps for DCO, organizations can not only improve their ability to detect and respond to cyber threats but also reduce operational costs by automating routine security tasks and optimizing resource allocation.

See How →

HOW AIOPS CAN BE APPLIED TO DCO

Threat Detection and Analysis

AIOps can enhance threat detection by analyzing vast amounts of data from various sources, including logs, network traffic, and system behavior, in real-time to detect anomalies and potential security threats. Machine learning algorithms can identify patterns that may be indicative of cyberattacks.

Incident Response Automation

AIOps can automate incident response processes. When a potential security incident is detected, AIOps can trigger predefined responses, such as isolating compromised systems, blocking malicious IP addresses, and notifying security teams.

User and Entity Behavior Analytics (UEBA)

AIOps can monitor user and entity behavior and identify unusual or suspicious activities. It can correlate user behavior with threat indicators and alert security teams when deviations from the norm are detected.

Predictive Analytics

AIOps can use predictive analytics to identify potential cyber threats before they manifest. It can analyze historical data and current network conditions to make predictions about future attacks.

Security Information & Event Management (SIEM)

AIOps can enhance SIEM systems by providing real-time analysis of security events and automating the response to known threats.

Dynamic Threat Intelligence

AIOps can ingest threat intelligence feeds and dynamically update security policies and rules to protect against emerging threats.

Vulnerability Management

AIOps can help identify vulnerabilities by continuously scanning systems and correlating them with known threats, allowing for timely patching or mitigation.

Security Orchestration and Automation

AIOps can orchestrate and automate security workflows, allowing for rapid responses to security incidents and reducing the workload on security teams.

Baseline and Anomaly Detection

AIOps can establish baselines for normal network and system behavior and then identify anomalies that may indicate security breaches or operational issues.

Continuous Monitoring

AIOps integrates network operations data with cybersecurity policies that provides an event-driven capability for continuous monitoring of the IT environment, allowing for immediate detection and response to security issues due to configuration changes and drift.

Capacity Planning for Security Resources

AIOps can help organizations allocate resources for DCO more effectively by analyzing trends in security events and traffic.

Reducing False Positives

AIOps can help reduce false positive alerts by learning from historical data, understanding system and mission context, and filtering out noise to refine alerting and detection, allowing security teams to focus on genuine threats.

Natural Language Processing (NLP) for Threat Intelligence

AIOps can process and analyze unstructured threat intelligence data, such as text reports and social media, using NLP to extract relevant information and assess potential threats.

To effectively **implement AIOps for DCO**,organizations should:

1. **Invest in advanced AIOps platforms and technologies that integrate with existing security solutions.**
2. **Train cybersecurity personnel to work alongside AIOps systems and understand the insights provided.**
3. **Continuously update and fine-tune AIOps models and algorithms to adapt to evolving threats.**
4. **Collaborate with threat intelligence providers and share information to improve AIOps threat detection.**