
Security Assurance through
UberMonitoring™

Security Assurance through UberMonitoring™

UberMonitoring is our answer to the challenge of maintaining a secure environment for the AIMS Platform's critical operations. Our continuous 24/7/365 monitor and audit regimen takes the worry away from your staff and gives you confidence that your important assets are safe and secure. But it goes beyond just safety and security. We constantly monitor the installations to ensure that all processes and systems are operating at peak efficiency, which improves system performance and reduces your overall costs. More importantly, UberOps has the security experts that are the brains behind the technology's power.

Monitoring

Discovering your Network

One of the Core functions of UberMonitoring is the automation of the discovery and monitoring of all components throughout the IS lifecycle This is done using a framework of tools like the NIST Cybersecurity Framework, the Collective Intelligence Framework (CIF), Puppet, Saner, AlienVault, Ansible and AWS SDK. All of these tools are tied together by the UberMonitoring API.

Auditing

Continuous Compliance

Auditing each component of the customer's network on a continuous cycle in order to maintain CIS Cybersecurity standards as well as any customer required FISMA, NIST, DoD, or other regulatory compliance. This provides a real time view into the compliance posture of the customer's environment as well as reporting for auditing and regulatory purposes.

Self-Remediation

Self-healing

UberMonitoring participates in, and uses, the NIST Cybersecurity Framework, the Collective Intelligence Framework (CIF), and AlienVault's Open Threat Exchange (OTX) to obtain up-to-date information regarding threat updates, news releases, and customer specific intelligence. This provides a continuously updating set of remediation profiles which reacts to intrusion attempts and continuously monitors/remediates any non-compliant systems.

Protecting

Threat Management

UberMonitoring participates in, and uses, the NIST Cybersecurity Framework, the Collective Intelligence Framework (CIF), and AlienVault's Open Threat Exchange (OTX) to obtain up-to-date information regarding threat updates, news releases, and customer specific intelligence. This provides a continuously updating set of remediation profiles which reacts to intrusion attempts and continuously monitors/remediates any non-compliant systems.

Optimization

Efficient and Effective Processing

With our constant monitoring and tooling, we are always coming up with new ways to save you money, employ the latest advances in technologies, and optimize your environment.

Tooling

Automation

Whenever appropriate, we write automation scripts that help streamline workflow in your environment. Seamlessly integrated, we make the complicated easy!