"The Superpowered SOC: How AI Can Drive Agencies to the Next Level of Cyber Defense"

Submitted by grigby1 on Wed, 04/07/2021 - 3:11pm

Cybersecurity incidents faced by federal agencies are continuing to increase in volume, complexity, and impact. The massive SolarWinds hack that impacted the Departments of Treasury, Justice, Commerce, and others further indicates the growing sophistication and success of threat actors. Although investments in diverse cloud and Internet of Things (IoT) environments are intended to improve productivity at federal agencies, the expanding complexity and scale of their digital infrastructures are creating additional challenges for Security Operations Center (SOC) teams. The constant emergence of advanced threats is also making it increasingly difficult for understaffed and overworked SOC teams to be efficient and effective. Triaging alerts and responding to incidents have also become more challenging for SOC teams due to the overwhelming generation of alerts. The integration of self-learning Artificial Intelligence (AI) solutions into existing government technologies will help elevate the performance level of human security team members. Self-learning AI and automation will help security professionals better sort through the noise and focus on dangerous incidents. AI can bring SOC teams to the next level of cyber defense as the technology can enable full-range detection, accurate threat management, and more. This article continues to discuss the challenges faced by government cybersecurity teams and how self-learning AI can help SOC teams improve their effectiveness and efficiency.

GCN reports "The Superpowered SOC: How AI Can Drive Agencies to the Next Level of Cyber Defense"