November 7, 2022

CrowdStrike EDR Deployment to CMS HIDS Multi-tenant Account

Planned Actions: The Cloud Support Team will be deploying CrowdStrike Endpoint Detection and Response (EDR) agent to the FAXCOM Windows instances for the Production Lifecycle that currently do not have CrowdStrike EDR agent deployed as part of AMI.

Note: This effort is mandatory for all Elastic Compute Cloud (EC2) instances running in AWS. The CrowdStrike agent has already been integrated into all the HIDS GOLD AMIs (Amazon Machine Images).

CrowdStrike Falcon:

CrowdStrike's expanded endpoint security solution suite leverages cloud-scale Artificial Intelligence (AI) and deep link analytics to deliver best-in-class Extended Detection and Response (XDR), EDR, Next-Gen Anti-Virus (AV), device control, and firewall management.

Features Included:

- **Falcon Prevent:** Next-gen AV – Protects against malware and malware-free attacks.
- **Falcon Insight:** Endpoint detection & response – Delivers continuous and comprehensive endpoint visibility across detection, response, and forensics.

- **Falcon Discover:** IT hygiene – Identifies unauthorized systems and applications which alerts in real time to the use of privileged credentials in the environment.
- **Falcon X:** Integrated threat intelligence – Integrates threat intelligence into endpoint protection, automating incident investigations, and speeding breach response.
- **Falcon Overwatch:** Threat hunting service – Identifies attacks and stops breaches 24/7 with an elite team of experts who proactively hunt, investigate, and advise on threat activity in the environment.

If you have any questions or concerns, please feel free to reach out to the Cloud Support team on Slack **#hids-clouddevops-support**

Impacted Lines of Business (LOBs):

- FAXCOM

Planned Downtime for AWS Account CMS HIDS Multi-tenant 150370869210 by environment:

- November 8, 8 p.m. ET
- Estimate ~2 hours to complete the agent installations and instance reboots.

What To Expect: A reboot is required to install the agent. The FAXCOM Team is on standby to restart their services and to confirm functionality once the effort is completed.

Center for Clinical Standards and Quality (CCSQ)