DATA SHEET

Artificial Intelligence for Insider Threat Management in the Public Sector

Insider threats arise when employees and other trusted parties abuse their access to the organization's network infrastructure to steal, modify or delete data. Such events are particularly damaging when insiders have privileged knowledge of your organization's high-value information assets.

Security Information and Event Management (SIEM) tools that collect data describing system events from logs of firewalls, networks, and other infrastructure components are an invaluable resource to security professionals. However, to counter threats from within, department-wide security controls must be complemented with user behavior and anomaly detection analytics.

AI TO ANALYZE USER BEHAVIOR

Creating tight security requires that departments understand individual's normal patterns of data access and use this as a baseline. Metrics to analyze include: start and end times of daily activity; regular patterns of email activity, including recipients of attachments; use of the Internet; and transfers of data. AI continuously compares current use to this baseline and to behaviors typical of co-working peers to detect emerging changes to the pattern. Investigators should test for false positives, as departures from an individual's baseline may be attributable to new work assignments or a change in role and responsibility.

AI TO DETECT ANOMALIES

By creating a profile of regular access patterns to networks and information assets, departments can deploy AI as an active defense to detect unusual and anomalous activity.

DataRobot has enabled insider threat protection in the following ways:

Data Misuse. Using DataRobot, a federal agency uses previous information policy violations to create AI that detects and proactively blocks emerging potential threats as individuals attempt to: misuse the internet; improperly handle documents; and violate security controls in attempts to access computer hardware.

Insider Threat Detection. With DataRobot, organizations leverage their enterprise usage policies and data on individual employees to develop, model, and deploy algorithms that detect security breaches and violations of clearance responsibilities and report theft or misuse of information assets.

Exfiltration Detection. With DataRobot, a defense cyber security agency checks for indications of data exfiltration (and other noisy attacks) that currently take months to detect with other network defense technologies.

Contact the Public Sector sales team at DataRobot to learn more: public-sector@datarobot.com.

With DataRobot, agencies can detect and prevent insider threats to information assets by building and deploying the right model in minutes rather than months. Our AI solution complements existing security controls to harden defenses against cybercrime.

Contact Us

DataRobot
1775 Tysons Blvd., 5th Floor
McLean, VA 22102

www.datarobot.com
info@datarobot.com

powered by aws