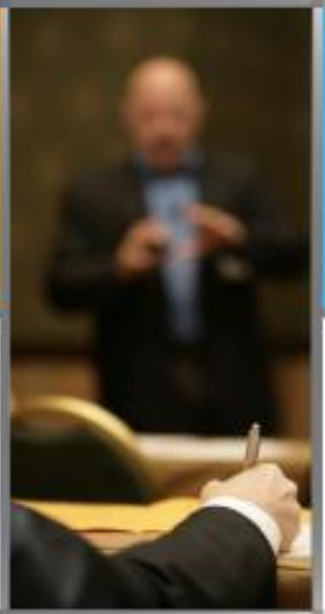
@CSOevents
#CSO50

CSO50 CONFERENCE+AWARDS

Aligning Proactive Security with Modern Threats



May 1-3, 2017

The Scottsdale Resort
Scottsdale, Arizona

PRODUCED BY
CSO
FROM IDG

CSO 50 CONFERENCE +AWARDS

Minimizing Insider Threats Through Behavior Analytics and Machine Learning

Jennifer Darwin

Director, Identity and Access Management

Sallie Mae

Project Background

Internal threats are becoming increasingly concerning every day.

Below are some Identity and Access Management top items that could be enhanced to provide more insight:

- Least Privileged Access
- Segregation of Duties
- User Access Certifications
- Job Roles
- Anomalous Activity

Use Cases

My next main objective was to outline use cases and determine what tool would best suit our needs. Below were my main objectives:

- Disgruntled Employees
- Cyberattacks Focusing on Users with Privileged Access
- Excessive Access
- Anomalous Activity

Project Execution

Next Steps:

- Identified the appropriate product
- Turned on specific event IDs in Windows, Oracle, and SQL
- Turned on audit logs for SharePoint and OneDrive
- Reconciled the log data
- Engaged the vendor to parse the data into the tool
- Reconciled the data in the tool is accurate
- Built business processes around the reports and the dashboard notifications

How are We Benefiting?

- Disgruntled Employees-
  - Developed a potential bad actor watch list
  - Terminated users attempting to log into the network
- Cyberattacks Focusing on Users with Privileged Access-
  - Anomalous activity alerts based on high & privileged entitlements
- Excessive Access-
  - Business friendly data for access outliers
- Anomalous Activity-

  Activity outside the U.S.
  Abnormal failed login attempts
  Abnormal password changes
  Privileged access group modifications
  Unusual downloads
  Abnormal file modifications
  Login during weekend/after hours
  Unusual access

Takeaways

Lessons Learned/Potential Challenges:

- Event IDs are key
- Log Management System is pertinent along with appropriate knowledge of the tool
- Parsing of the data can be time consuming and challenging
- Know your use cases and audit requirements
- Define your reconciliation process
- Clearly know your business processes

Next Steps

- Continue to add application logs to the system to broaden our insight to activities around anomalies and dormant access or accounts
- Currently working with the business on the access outliers
- Exceptions outside of the role should be approved and flagged as a known exception.
- Provide the business the ability to view to their direct reports access and access outliers on demand
- Enhance our access certification processes
- Add an API for vendor integration
- Continue to improve business processes and efficiency around the data