Best practice for detecting and protecting against insider threats

Sam Hector
IBM Security Channel Leader, UKI

IBM **Security**

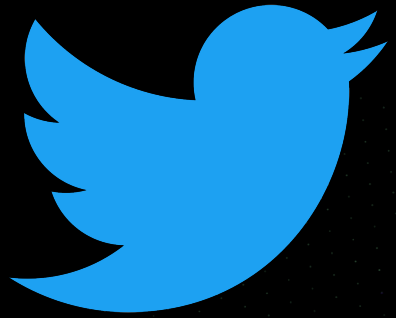
IBM

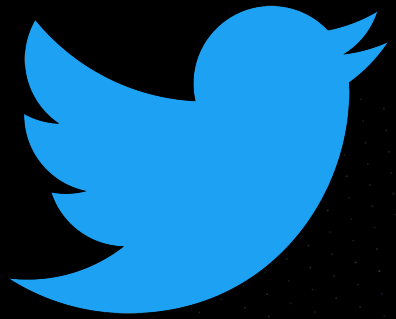
“Insider threats are users with legitimate access to company assets who use that access, whether maliciously or unintentionally, to cause harm to the business.”

“Insider threats are users with **legitimate access** to company assets who use that access, whether maliciously or unintentionally, to cause harm to the business.”

Profiles of employees that can act as malicious insiders

- Lone wolf
- Collaborator
- Goof
- Pawn





“Ideally, automated systems would have identified which Twitter reps were changing all those email addresses in such a short amount of time. But a former Twitter security employee says the company had been slow to invest in that kind of early warning technology and that a culture of trust had blinkered it to potential internal threats.”

Wired (24th September 2020) - How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One

How should insurers protect themselves from insider threat?

Raise awareness and educate staff

How should insurers protect themselves from insider threat?

Raise awareness and educate staff

Design internal policies and IT systems in a way that deters malicious activity

How should insurers protect themselves from insider threat?

Raise awareness and educate staff

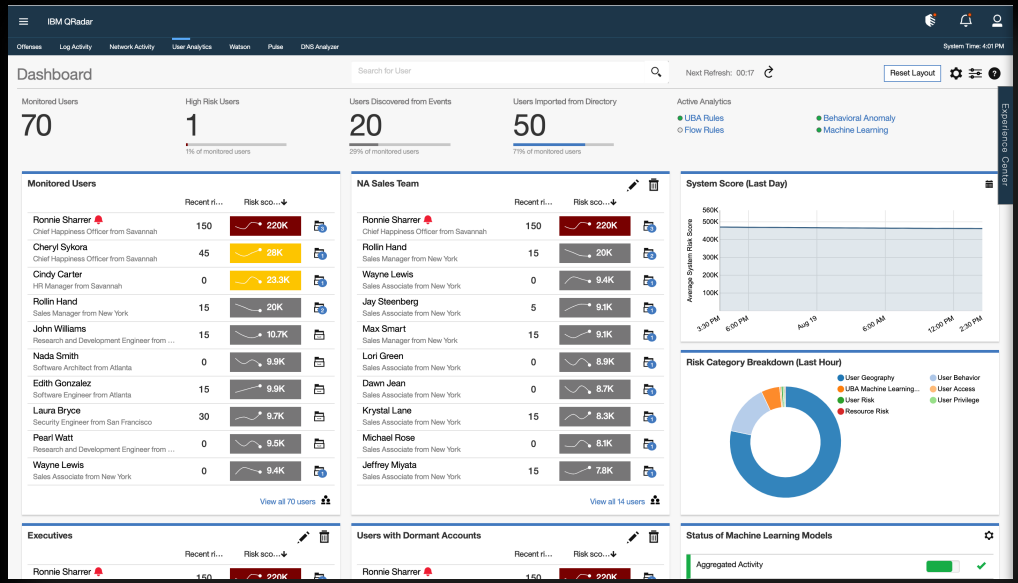
Design internal policies and IT systems in a way that deters malicious activity

Put Security tools in place to detect, alert against, and block insider threats

IBM QRadar User Behavior Analytics

Powerful machine learning driven use cases addressing 3 major insider threat vectors

- Compromised or Stolen Credentials
- Careless or Malicious Insiders
- Malware takeover of user accounts



IBM Security Verify Privilege Vault

End User Served	IT & Security Admins
Capabilities	Vaulting, Auditing & Privileged Access Control
Delivery Method	On-Premises Cloud

Discover, manage, protect and audit privileged accounts across your organization.

Establish a Secure Vault
Store privileged credentials in an encrypted, centralized vault

Discover Privileges
Identify all service, application, administrator, and root accounts to curb sprawl and gain full view of your privileged access.

Manage Secrets
Ensure password complexity and automatically rotate credentials.

Delegate Access
Set up RBAC, workflow for access requests, and approvals for third parties.

Control Sessions
Implement session launching, proxies, monitoring, and recording.

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions