

Best practice for detecting and protecting against insider threats

Sam Hector

IBM Security Channel Leader, UKI

“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



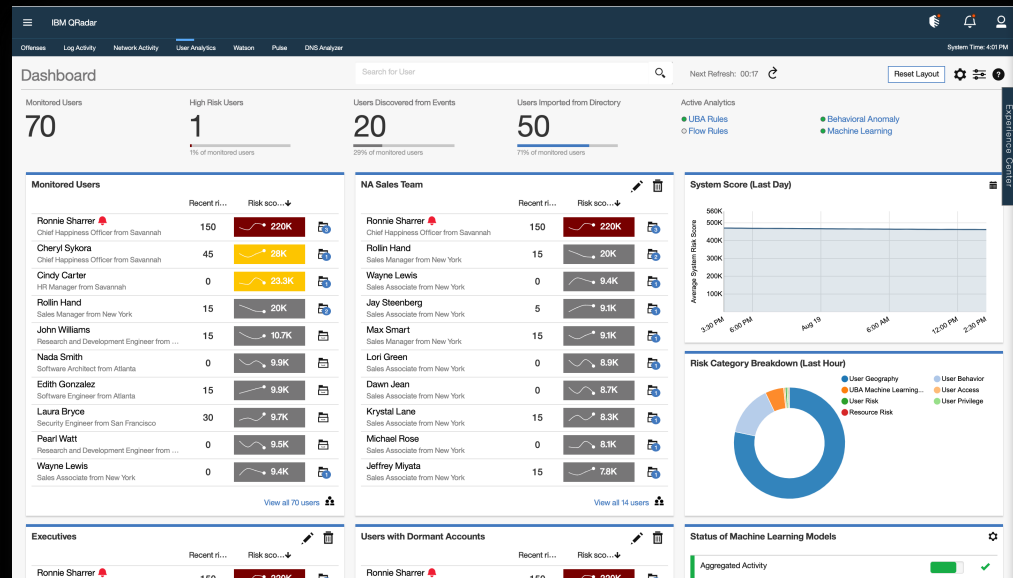
Compromised or Stolen Credentials



Careless or Malicious Insiders



Malware takeover of user accounts



IBM Security Verify Privilege Vault



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

End User Served

IT & Security Admins

Capabilities

Vaulting, Auditing & Privileged Access Control

Delivery Method

On-Premises
Cloud

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](https://twitter.com/ibmsecurity)

youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM Security



The image features the classic IBM logo, which consists of the letters 'IBM' in a bold, sans-serif font. Each letter is formed by eight horizontal white stripes of equal thickness, set against a dark blue background that transitions from a lighter shade at the top to a darker shade at the bottom.