

2023 REPORT

# Insider Threat



GURUCUL

### INTRODUCTION

The new normal of hybrid work models, access to more cloud apps, and increasing economic uncertainty are driving insider risk to new levels.

The 2023 Insider Threat Report surveyed over 326 cybersecurity professionals to reveal the latest trends and challenges facing organizations in this changing environment. The report explores how IT and cybersecurity professionals adapt to better deal with risky insiders and how organizations are preparing to better protect their critical data and IT infrastructure.

#### Key findings include:

- · 74% of organizations say insider attacks have become more frequent
- · 74% of organizations say they are at least moderately vulnerable or worse to insider threats
- · More than half of organizations have experienced an insider threat in the last year, and 8% have experienced more than 20
- 68% of respondents are concerned or very concerned about insider risk as their organizations return to the office or transition to hybrid work; only 3% are not concerned
- 53% say detecting insider attacks is harder in the cloud

The 2023 Insider Threat Report has been produced by Cybersecurity Insiders, the 600,000-member online community for information security professionals to explore how organizations respond to the evolving security threats in the cloud. We would like to thank Gurucul for supporting this unique research.

We hope you find this report informative and helpful as you continue your efforts in protecting your IT environments against insider threats.

Thank you,

Holger Schulze



**Holger Schulze** CEO and Founder Cybersecurity Insiders

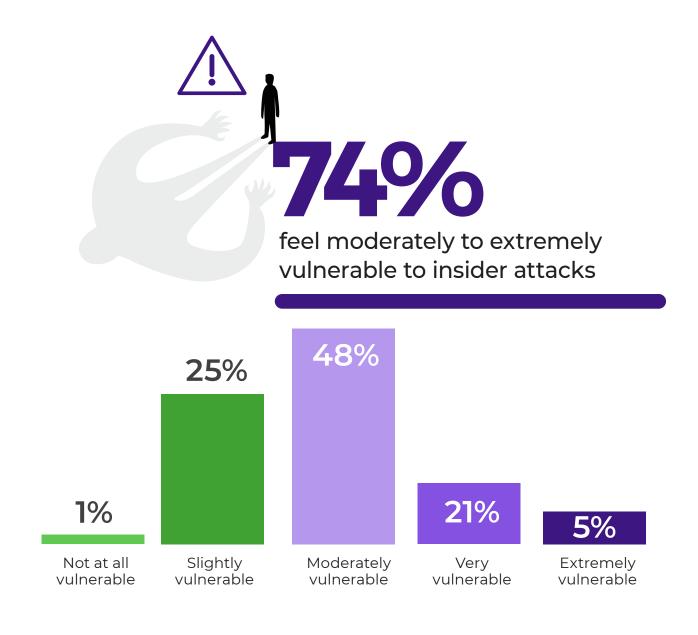
Cybersecurity

2

## **INSIDER VULNERABILITY**

Organizations have never felt more vulnerable to insider threats. Three quarters of survey respondents (74%) say they feel moderately to extremely vulnerable - a significant rise of 8 percentage points compared to our previous survey.

How vulnerable is your organization to insider threats?

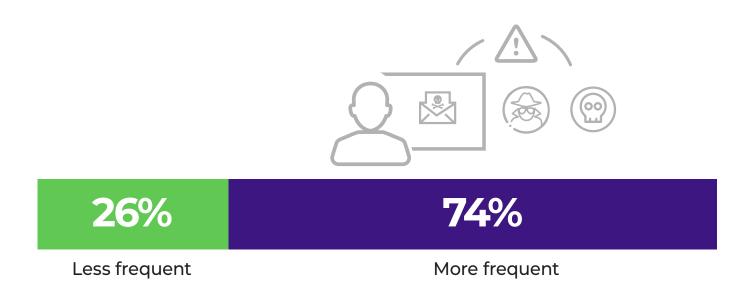


3

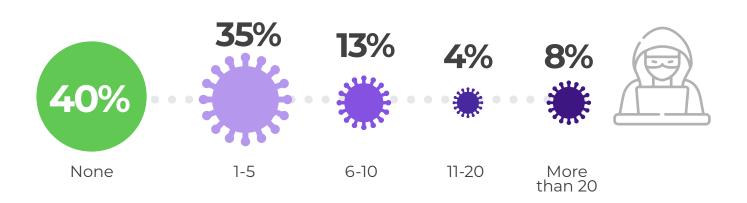
## **RISE OF INSIDER ATTACKS**

The rise in perceived vulnerability coincides with a significant increase in insider attacks. Seventy-four percent of organizations report that attacks have become more frequent, compared to only 68% who said the same in the 2021 survey.

Have insider attacks become more or less frequent over the last 12 months?



▶ How many insider attacks did your organization experience in the last 12 months?



### **INSIDER THREAT IMPACT**

Insider attacks can cause a wide range of negative impacts on affected organizations. When we asked cybersecurity professionals in our survey to prioritize the most critical effects of insider attacks, loss of critical data remained the top issue (45%, up from 40% in 2021). This is followed by brand damage, rising to the second most critical issue (43%, almost doubling from 26% in 2021), and operational disruption or outage (41%, up from 33% in 2021).

#### What impacts have insider threats had on your organization?

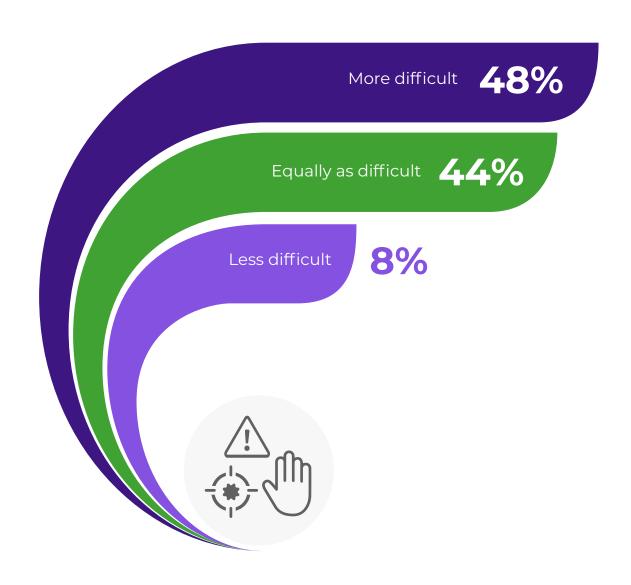
Loss of critical data	45%
Brand damage	43%
Operational disruption or outage	41%
Loss in revenue	26%
Legal liabilities	24%
Loss in competitive edge	23%
Non-compliance with regulations	22%
Expenditure remediating successful intrusions	19%
Loss in market valuation	18%

No impact 16%

### **INTERNAL VS. EXTERNAL ATTACKS**

How difficult is it to detect and prevent insider attacks compared to external cyber attacks? According to our survey, the largest percentage of cybersecurity professionals report that internal attacks are more difficult to detect and prevent than external cyber attacks. Because trusted insiders have approved access privileges, it is challenging to distinguish legitimate use cases from malicious attacks.

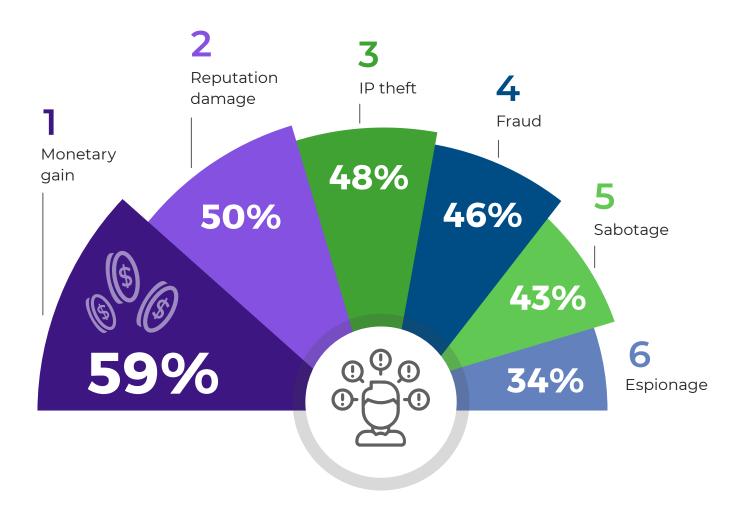
How difficult is it to detect and prevent insider attacks compared to external cyber attacks?



## **MOTIVATIONS FOR INSIDER ATTACKS**

Monetary gain is the top malicious motivation for an insider threat (59%) that concerns security professionals, closely followed by a range of drivers, including reputation damage (50%), theft of intellectual property (48%), and fraud (46%). The ideal insider threat solution uses all these vectors as indicators that a person is at risk or already an active insider threat.

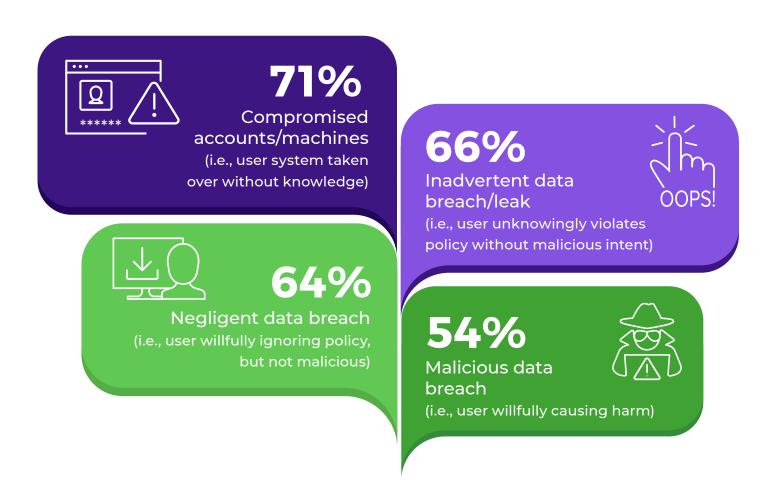
What motivations for malicious insider threats are you most concerned about?



### **TYPES OF INSIDER THREATS**

At its core, insider risk is a data protection problem. Security professionals agree, and 71% are most concerned about compromised accounts/machines. This is followed by inadvertent data breaches/leaks (66%), negligent data breaches (64%), and malicious data breaches (54%).

What type of insider threats are you most concerned about?



8

#### **DETECTION AND PREVENTION**

A number of factors make timely detection and prevention of insider attacks quite difficult for cybersecurity teams. First, trusted insiders already have credentialed access to apps, networks, and services (54%). Add to that the increased use of SaaS apps that can leak data (44%) and an increase in personal device use with access to corporate resources (42%), and it's easy to lose control of sensitive data and systems to malicious insiders.

What makes the detection and prevention of insider attacks increasingly difficult?



Insiders already have credentialed access to the network and services



Increased use of applications that can leak data (e.g., Web email, DropBox, social media)



Personal device access to corporate resources



More end-user devices capable of theft



Insiders are more sophisticated



Difficult to prove malicious intent on part of the employee



Lack of integrated security that protects data consistently across SaaS, laaS, on-prem apps, the web, and all devices

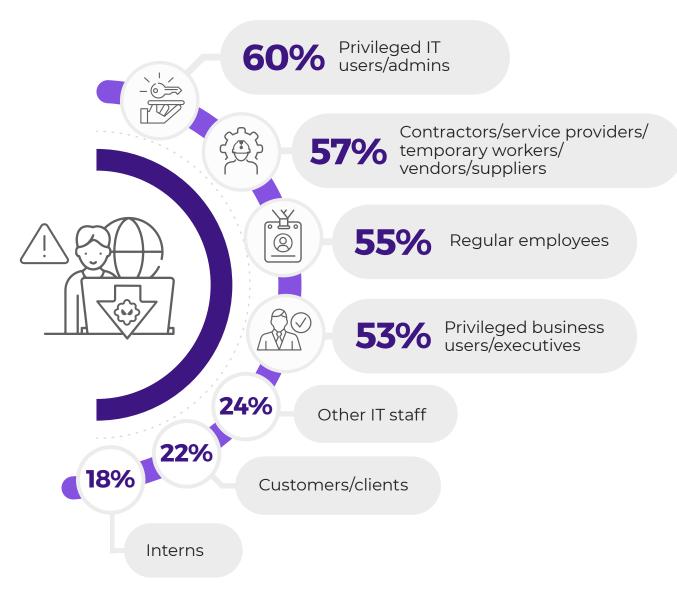
Increased amount of data that leaves protected boundary/perimeter 25% | Challenges related to the management of disjointed and disparate security tools 25% | Migration of sensitive data to the cloud along with adoption of cloud apps 24% | Difficulty in detecting roque devices introduced into the network or systems 20% | Absence of an Information Security Governance Program 18% | Lack of relevant cloud security tools 18% | Other/not sure 12%

9

#### **RISKY INSIDERS**

Among all potential insiders, cybersecurity professionals are most concerned about IT users and admins with far-reaching access privileges that potentially allow them undetected access to even the most sensitive data, apps, and systems (60%). This is closely followed by third-party contractors and service providers who may have less loyalty to the organization and more opportunities to access critical systems (57%). Regular employees (55%) and privileged business users (53%) also pose security risks – and they are by far the largest group of users in any organization with access to sensitive apps.

#### What type(s) of insiders pose the biggest security risk to organizations?

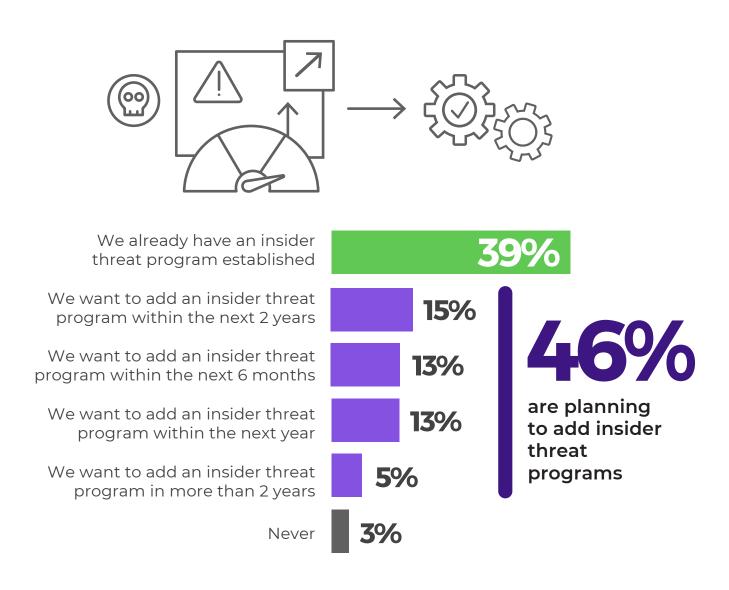


Other 5%

#### INSIDER THREAT PROGRAM ADOPTION

The rising threat of insider attacks is a strong driver for organizations to implement formal insider risk programs. Thirty-nine percent of organizations already have an insider threat program in place. Another 46% are planning to add insider threat programs in the future – a rise of 5 percentage points since our 2021 survey.

Do you have an insider threat program or plan to establish one?

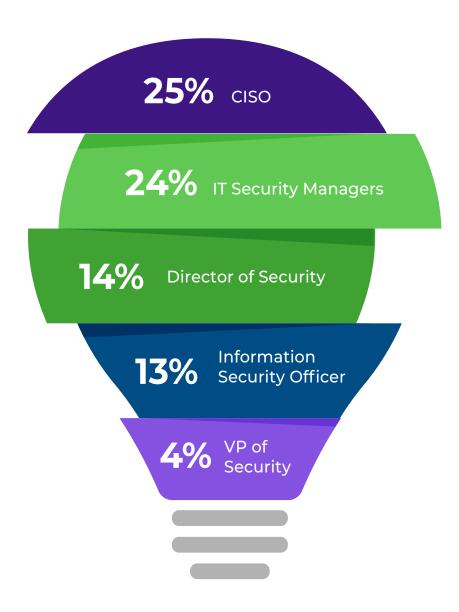


Not sure 12%

## **PROGRAM OVERSIGHT**

Because insider threats are a critical security risk and often deeply embedded in an organization, formal responsibility for insider risk programs often lies with the head of security/CISO (25%), followed by IT security managers (24%) and the director of security (14%).

Who oversees programs for preventing, detecting, and mitigating insider threats at your organization?

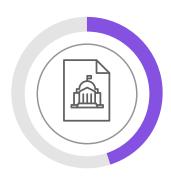


Not sure/other 20%

#### **PROGRAM DRIVERS**

What is driving the creation of corporate insider threat programs? The largest percentage of organizations in our survey report that their insider threat program is part of the overall information security governance program (45%). This is closely followed by programs driven by proactive security team initiatives (44%) and regulatory compliance mandates (40%).

What are the primary drivers of your insider threat program?



45%

Information security governance programs



44%

Proactive security team initiatives



40%

Regulatory compliance



Proactive IT team initiative



Incident(s) that impacted peers or relevant industry



Suspected incident



Previously confirmed incident



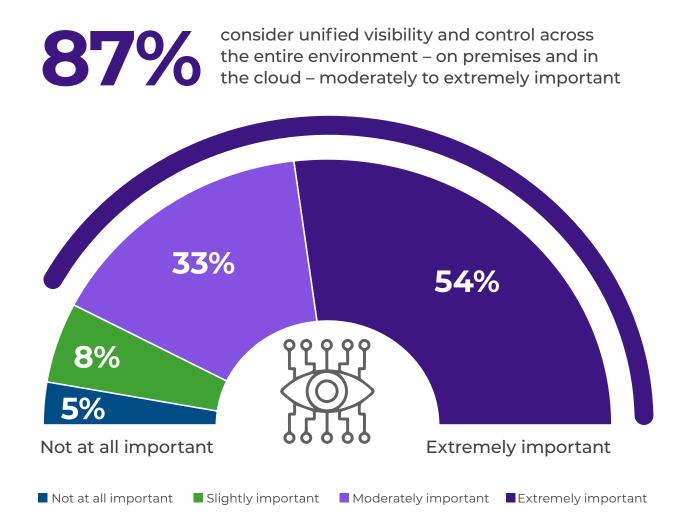
Directive from the executive management team

Directive from the board of directors 12% | We do not have an insider threat program 10% | Other 5%

### **UNIFIED VISIBILITY**

Visibility and control are paramount in preventing insider attacks. Almost all organizations (87%) consider unified visibility and control across all apps, devices, web destinations, on-premises resources, and infrastructure to be moderately to extremely important.

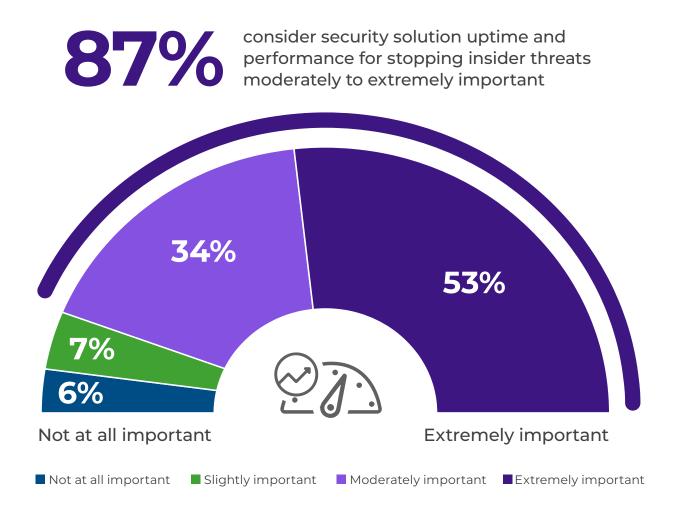
When it comes to insider threats, how important is unified visibility and control across your entire environment – on premises and in the cloud?



#### SECURITY UPTIME AND PERFORMANCE

Uptime and performance of security solutions is critical in protecting against insider threats. Eighty-seven percent of organizations consider this factor moderately to extremely important.

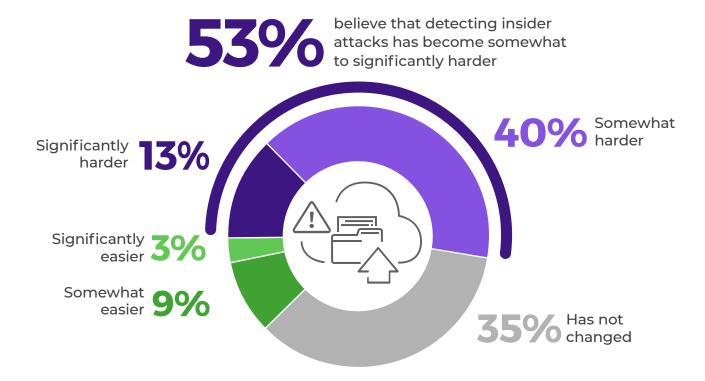
How important is security solution uptime and performance for stopping insider threats in the cloud (for SASE, CASB, SWG, etc.)?



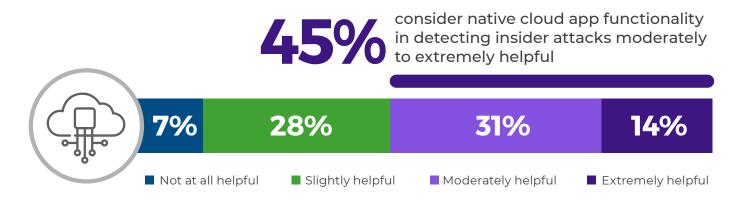
## IMPACT OF NATIVE CLOUD FUNCTIONALITY

The shift to the cloud makes detecting insider attacks more difficult, as confirmed by most cybersecurity professionals (53%). Only 45% consider native cloud app functionality moderately to extremely helpful for detecting insider attacks.

Since migrating to the cloud, detecting insider attacks is:



▶ How important is native cloud application functionality in detecting insider attacks?

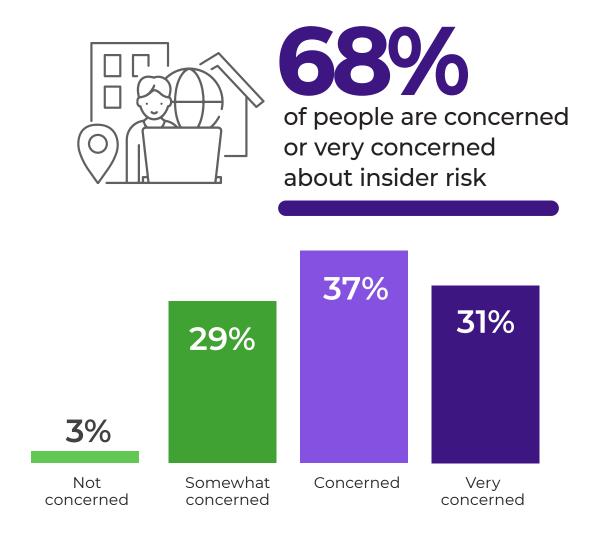


We don't rely upon native cloud app functionality for detecting insider threats 8% | Not sure 12%

#### **HYBRID WORKFORCE RISKS**

The rapid shift to remote and hybrid workforces over the last few years only further aggravated insider risks. Most organizations (68%) are concerned or very concerned about insider risk.

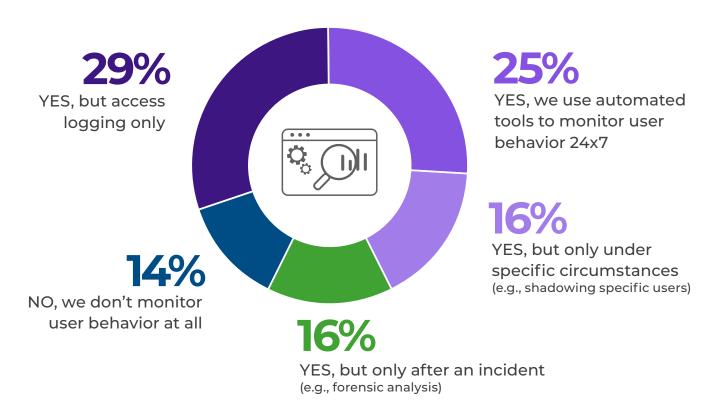
With a post-COVID return to the office imminent, or a new trend of a more hybrid workforce being likely, how concerned are you about insider risk?



### **USER BEHAVIOR MONITORING**

Cybersecurity teams are increasing the use of User Behavior Analytics (UBA) tools to detect, classify, and alert anomalous behavior. Eighty-six percent of organizations monitor user behavior in one way or another. The most common use case is access logging (29%), followed by automated tools to monitor user behavior (25%). Almost half of organizations monitor abnormal user behavior across their cloud footprint (SaaS, IaaS, PaaS) and the web (48%).

#### Do you monitor user behavior?



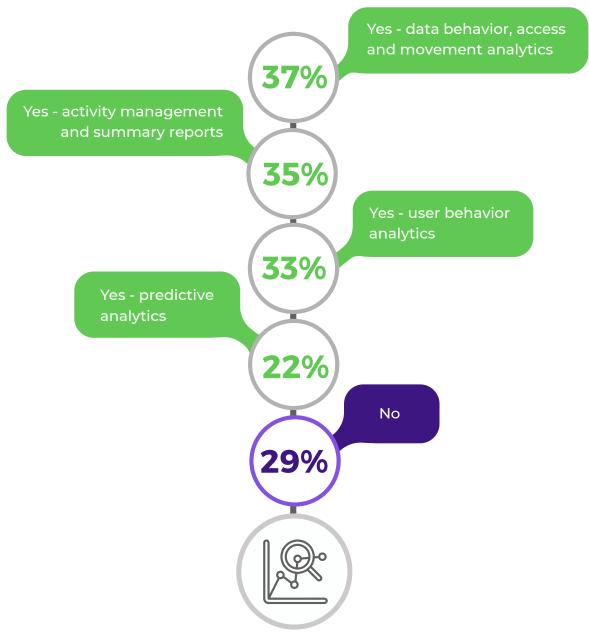
Do you monitor abnormal user behavior across your cloud footprint (SaaS, IaaS, PaaS) and the web?



## **INSIDER THREAT ANALYTICS**

We asked cybersecurity professionals in our survey how they leverage analytics to combat insider threats. The most common use case is the analysis of data behavior, access, and movement (37%). This is followed by activity management summary reports (35%) and user behavior analytics (33%).

Does your organization leverage analytics to determine insider threats?

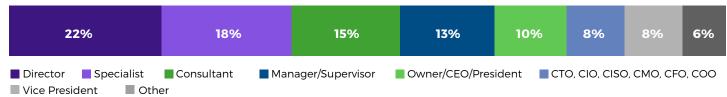


Not sure 9%

## **METHODOLOGY & DEMOGRAPHICS**

This Insider Threat Report is based on the results of a comprehensive online survey of 326 cybersecurity professionals, conducted in December 2022, to gain deep insight into the latest trends, key challenges, and solutions for insider threat management. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

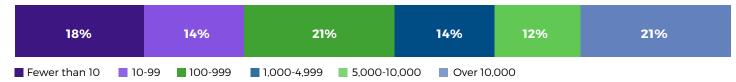
#### CAREER LEVEL



#### DEPARTMENT



#### COMPANY SIZE



#### **INDUSTRY**



## GURUCUL

Gurucul is a global cyber security company that is changing the way organizations protect their most valuable assets, data and information from insider and external threats both on-premises and in the cloud. Gurucul's real-time Cloud-native Security Analytics and Operations Platform provides customers with Next-Gen SIEM, Open XDR, UEBA, and Identity & Access Analytics. It combines machine learning behavior profiling with predictive risk-scoring algorithms to detect and prevent breaches.

Gurucul technology is used by Global 1000 companies and government agencies to fight cybercrimes, IP theft, insider threat and account compromise as well as for log aggregation, compliance and risk-based security orchestration and automation for real-time extended detection and response. The company is based in Los Angeles.

To learn more, visit gurucul.com and follow us on LinkedIn and Twitter.

## Cybersecurity INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with <u>unique marketing opportunities</u> to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com