X-Force

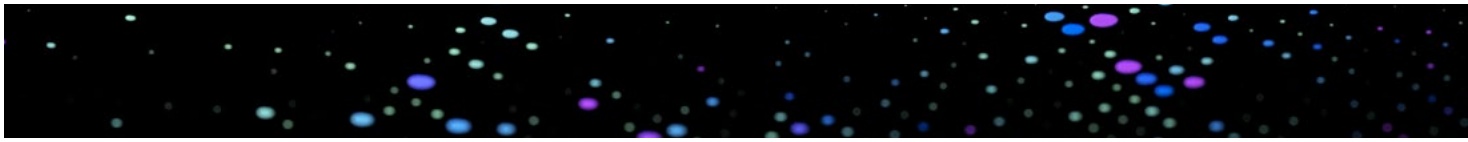
2021 IBM Security X-Force Insider Threat Report

IBM Security X-Force Threat Intelligence

Special Intelligence Report Q2 2021

IBM

Table of contents



Introduction

The cyber threat landscape is constantly changing as attackers and defenders alike innovate with new technologies and processes. Organizations spend a collective approximate of $60 billion dollars per year to defend their assets and recruit talent to prevent and respond to attacks, as security spend rises another 10% in 2021.[1]

While much of an organization's security focus and spend is dedicated to thwarting attacks that come from outside of the company itself, often overlooked are insider threats: those that come from within the organization. Insider threats, many of which turn out to be non-malicious or accidental, have the potential to cause devastating harm in the form of data theft, financial loss, theft of intellectual property, and reputational damage. In a 2020 survey, the Ponemon Institute estimated organizations spend on average $644,852 to recover from an insider threat incident, regardless of incident source.[2] This includes the cost of monitoring and investigating suspected insider events and the incident response, containment, eradication, and remediation of an insider incident.

In the context of this paper, IBM Security X-Force defines an insider as:

— The accidental insider: a negligent employee, or third-party vendor/contractor.[3]

— The malicious insider: a criminal or malicious employee or third-party vendor/contractor.

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. A negligent insider is defined as an insider who accidentally causes an incident impacting the confidentiality, integrity or availability of data or systems within an organization. This does not include phishing/social engineering incidents.

Using exclusive proprietary data gleaned from actual incident response investigations, X-Force analyzed suspected insider threat incidents—both accidental and malicious—that affected organizations from 2018 to 2020. Coupled with open-source reporting of the most prominent insider threat attacks, this paper will examine critical discoveries from that data, including:

— How most insider attacks are discovered.

— The role access level plays in insider attacks.

— Best practices for mitigating insider threats.

Key research findings

40% of incidents were detected through alerts generated via an internal monitoring tool.

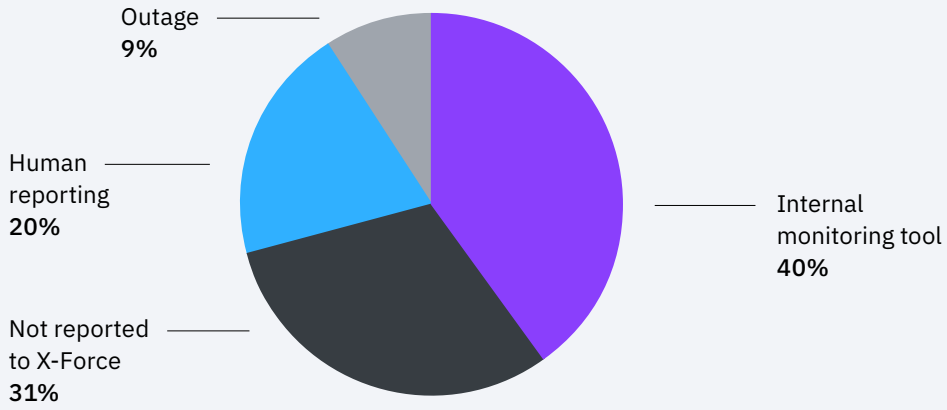
40% of incidents involved an employee with privileged access to company assets.

In 100% of the incidents where the insider was confirmed or likely had administrative access, this elevated access played a role in the incident itself.

How insider threat attacks are discovered

Insider threats are generally defined as attacks where legitimate users who have some level of access to enterprise assets leverage that access, either maliciously or accidentally, and ultimately cause harm to the organization. This threat can come from a current or former employee or from a third-party contractor or vendor who maintains access to serve a designated business function.

How the insider attack was discovered



An analysis of insider threats to which X-Force has responded to since 2018 reveals that 40% of these incidents were detected through alerts generated via an internal monitoring tool. Human reporting—such as employees alerting their organization to anomalous activity—accounted for 20% of the detections, and a system outage alerted security teams in 9% of the cases.

In the 2020 Cost of Insider Threats: Global Report by the Ponemon Institute, sponsored by ObserveIT and IBM, tools like User Behavior Analytics (UBA), Privilieged Access Management (PAM), Security information and event management (SIEMs) and programs like threat intelligence sharing and user training and awareness were estimated to save organizations an average of $3 million in terms of reducing or eliminating insider risks.[4]

Cost savings of $3 million

Tools like UBA, PAM, SIEMs and programs like threat intelligence sharing and user training and awareness were estimated to save organizations an average of $3 million in terms of reducing or eliminating insider risks.[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

Lack of evidence and unknowns in X-Force research

Regarding insider incidents where the discovery method was “not reported to X-Force” or “lack of evidence,” X-Force incident response teams were not provided enough information to make a determination about discovery. This is often because many organizations lack visibility into what their baseline environment looks like and how it operates. In order to detect anomalous activity inside any system, it is critical to understand what normal activity looks like so that outliers can be more easily spotted with confidence. In 2019, IBM sponsored a SANS report[5] looking at the landscape for advanced threats to organizations. This research showed that:

— 48% of organizations considered lack of visibility into their infrastructure as the top gap in security.

— 35% felt that they lacked the ability to detect misuse by company insiders.

— 47% of organizations admitted to lacking the ability to understand what normal baseline activity looked like inside their networks.

5. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39989

Privileged versus administrative access

X-Force classified two different types of users when analyzing insider threat incidents.

A **privileged user** is defined as someone within the organization that has access to sensitive data. This data might be intellectual property, customer data, or HR information. These users could also be those with access to sensitive business information like mergers & acquisition data or other legal information.

Users with **administrative access**, also known as administrators or admins, are defined as people with elevated access to IT systems within the network. In theory this type of access should not overlap. However, X-Force discovered that end users may often be overprovisioned in their IT environments.

Insiders with administrative access differ from those with sensitive access to a corporate environment. These include employees, contractors/vendors with access to the organization's IT environment and present a unique risk to an organization based on their elevated network privileges.

Example roles with privileged access

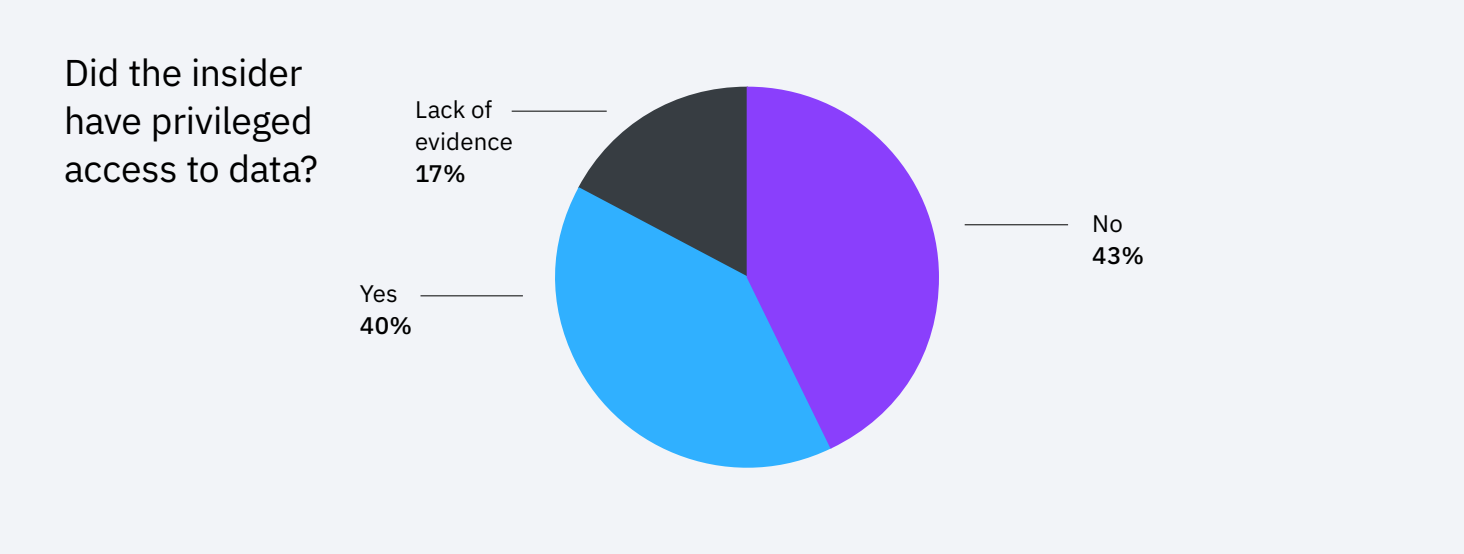
- HR roles
- Senior executives
- Finance roles
- Legal roles
- Research positions
- Other roles with access to an organization's intellectual property or "crown jewels" or customer data

Example roles with administrative access

- Server administrators
- IT administrators
- Help Desk
- Third party IT vendors
- Other roles that are able to modify configurations/ settings on IT systems

Who is watching the watchers?

Do insiders who cause incidents typically have privileged access? The short answer is yes.



Analysis of X-Force data shows that 40% of insider-provoked incidents involved an employee with privileged access to sensitive company assets. For this research, X-Force classified privileged access as those who work in areas including the IT department, human resources, finance, security, or executive positions.

In an additional 17% of the data it was unclear whether or not the insider had privileged access to sensitive data, which means the number of incidents caused by privileged access users could be substantially higher.

Individuals with elevated access to critical assets, such as network shares, security appliances, email systems, employee- or client personally identifiable information (PII), intellectual property, or financial data, can pose a significantly higher risk than those with more limited privilege.

It makes sense then that incidents caused by accidental insiders with privileged access end up costing organizations more than those caused by accidental insiders with a lesser degree of access. Incidents involving malicious insiders with higher degrees of privileged access carry an even heavier price tag, and attacks involving these users can escalate to a full-scale data breach. For example, in 2018, an Australian real estate agent working for a high-profile local agency was found guilty of accessing confidential databases prior to leaving the agency. The agent manipulated the state of prospective sales in the system by downgrading the interest of the prospective clients. Additionally, the agent admitted to taking over 200 client records to solicit business at a new agency. This insider attack was estimated to have cost the impacted agency $30 million in potential property sales.[6]

One of the best methods for preventing access-level-related insider incidents is to adhere to least privilege principles and ensure that users have the lowest level of access needed to carry out their duties for the organization. This can come in the form of a privileged access management (PAM) solution which may build around a zero-trust model.[7,8] In this model, the goal is for everyone with a user account to be granted the least amount of privilege as possible, lowering the chances that an insider will gain unintended access to data or assets. This concept becomes even more critical in the cloud where more data resides and both human and non-human requestors must access it to operate.

The 2020 Cost of Insider Threats: Global Report showed that only 39% of organizations have adopted some form of privileged access management in their organizations.[9] Additionally, it shows that the adoption of a PAM has resulted in a cost savings of $3.1 million, highlighting the effectiveness of these measures.

39%

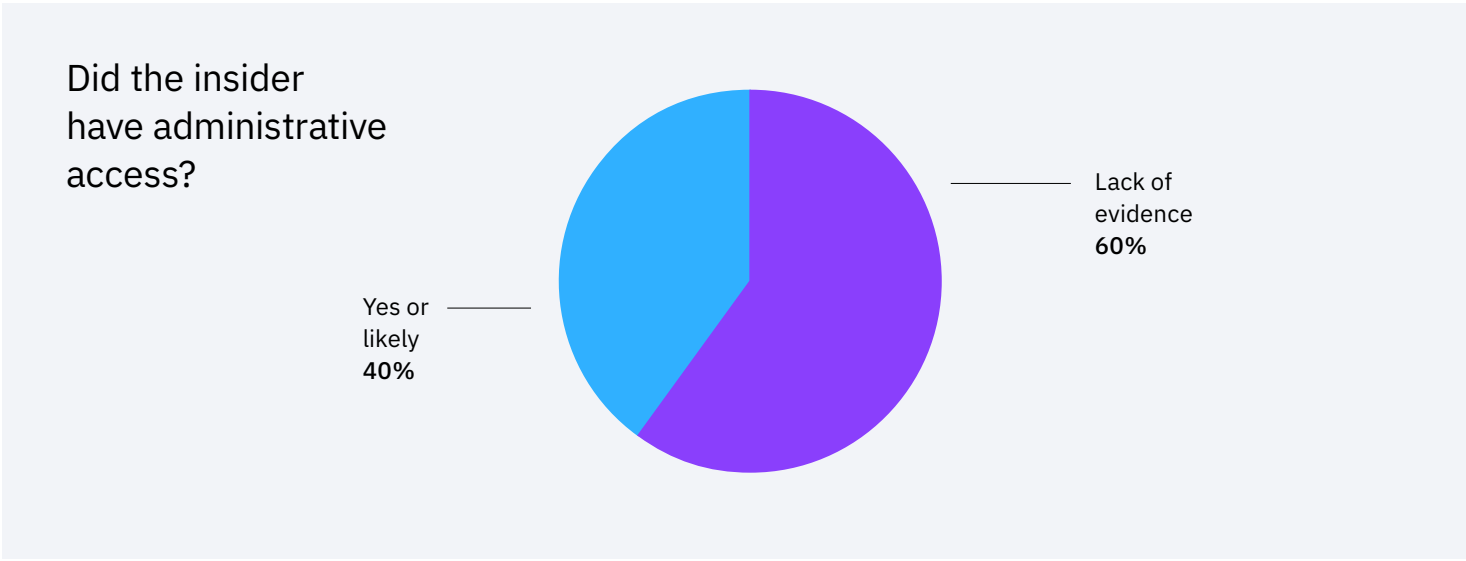
39% of organizations have adopted some form of PAM in their organizations.[9] This adoption has resulted in a cost savings of $3.1 million.

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

Administrative access abuse is a costly matter

There have been numerous public instances of insiders abusing their power as admins at organizations for nefarious purposes, including revenge, monetary gain, or other maligned intent. In February 2020, former Microsoft engineer, Volodymyr Kvashuk, was found guilty of using his privileged access to steal over $10 million in digital assets from the company.[10] The theft was enabled by Kvashuk's administrative access on the retail sales platform he was responsible for managing.[11] Specifically, Kvashuk used his colleagues' email addresses and valid test accounts on the system to obfuscate their activity, including exfiltrating digital gift cards. These and other assets stolen were resold on the internet for personal profit which the engineer later used to buy a $1.6 million home and a $160,000 Tesla vehicle.[12]

Administrative access abuse by the numbers

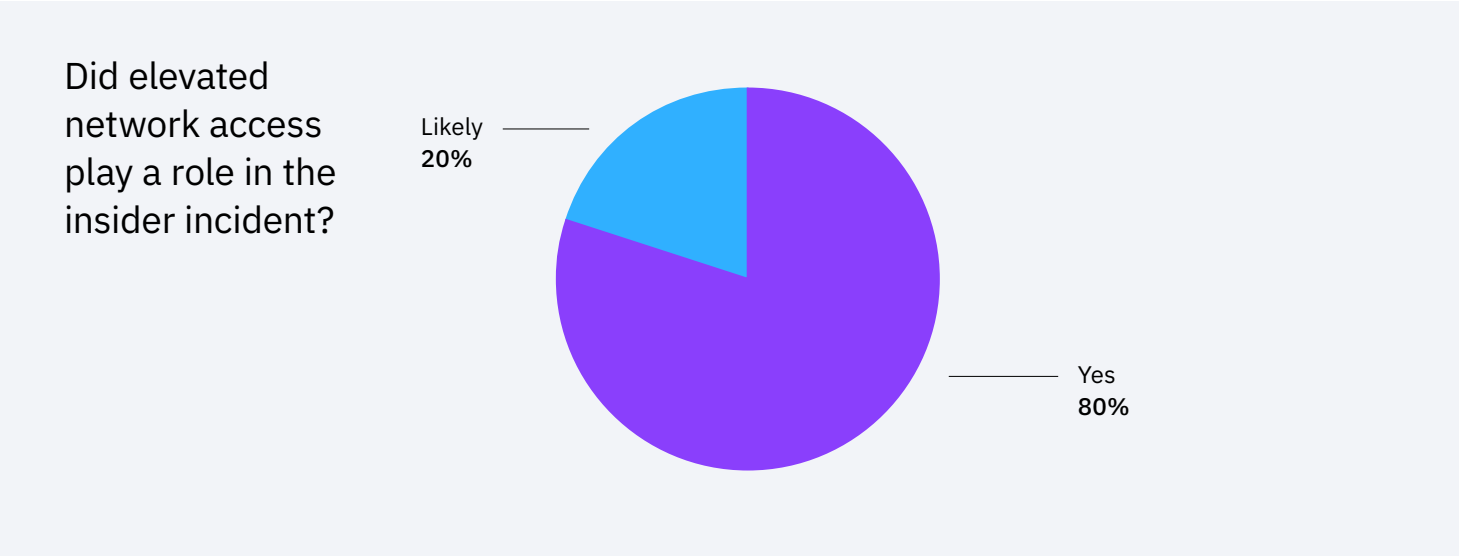


In 40% of the incidents X-Force responded to from 2018 through 2020, the insider was confirmed or likely had administrative access to the network. X-Force analysts determined the type of insider access based on the details of the incident when the specific role of the user was not provided by the client.

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

These incidents involved data exfiltration, exposure and deletion of sensitive data, and installation of unauthorized software, among others. Specifically, some organizations lost petabytes of logs deleted from servers, endured intentional source code leaks, or suffered costly outages at the hands of an insider with administrative access.

More interestingly, in 100% of the incidents where the insider was confirmed or likely had administrative access, this elevated access played a role in the incident itself. (See chart below)



To explain this point differently, if the insider did not have administrative access, it is likely the incident would have had much less impact to the organization, or in many cases, may not have occurred at all. X-Force has responded to several insider incidents where critical databases and logs were deleted from servers. Had the insider not had administrative access to those systems, the event would not have taken place.

Recommendations

X-Force believes the amount of insider incidents is underrepresented in third-party data. There are likely many more incidents of this nature handled inhouse by organizations and likely not publicized due to fear of liability or reputational damage to the organization.[13]

X-Force research and data highlight the need for potential insider threats to be a prominent component of an information security program based on the impact these incidents may have on an organization. Specifically, IBM Security recommends the following regarding insider threats:

Defense-in-depth strategies work well to detect insider threats.

Traditionally a multilayered approach to the technologies and processes implemented by organizations is thought to address external threats. However, X-Force research indicates that many of these tools, including security information and event management (SIEM) solutions, were crucial in detecting insider threat activity as well.

Understand what is normal in your environment.

The best way to detect suspicious activity from any type of attacker is to understand what type of activity is considered normal inside your network. Building a strong understanding of baseline activity makes it easier to detect and respond to anomalous behavior promptly and effectively. A robust user behavior analytics (UBA) solution can provide this functionality and adapt to changes in your environment over time.

Review administrative access on a regular basis.

X-Force found several insider incidents involving administrators were likely due to overprivileged users. Stringent change and process control should be implemented around administrative access, particularly on mission critical servers. Consider technology solutions that log and grant temporary administrative access to sensitive systems and functions.

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

Separate your information security and IT administrative teams.

X-Force experience has demonstrated that a balanced approach to managing the independence and governance of security and administrative teams helps enable better security. It also allows the administrative teams to have the flexibility and creativity necessary to optimize their exploration and discovery of threats while providing the enterprise with sufficient supervision and oversight to minimize risks within the team.

Build risk profiles for sensitive organizational roles.

Because elevated access played a role in many of the insider incidents X-Force responded to, we recommend organizations consider building risk profiles for positions within the organization that have sensitive or administrative access to systems or data. The implementation of a privileged access management (PAM) solution which builds around a zero-trust model creates least privilege access for users and could minimize the impact of insider incidents.

Update your Incident Response playbook to include insider threats.

General training is not enough for these incidents. While most incident response playbooks account for attacks from external adversaries, organizations should consider adding scenarios to include accidental or malicious insider threat scenarios. Consider a partner who can help you develop Incident Response Plans and attack-specific playbooks to better prepare and respond to cyberattack.

Keep training your employees.

Ethical business practices are included in numerous organizations' annual training programs alongside social engineering training. Many of the insider incidents X-Force responded to were discovered by other employees and not technology. Organizations should include how to report a suspected insider incident in annual business ethics or social engineering training efforts. Also, role-based training for employees with privileged access can help them remain conscious of tell-tale signs that something around them is going awry.

Leverage reputable Threat Intelligence Services.

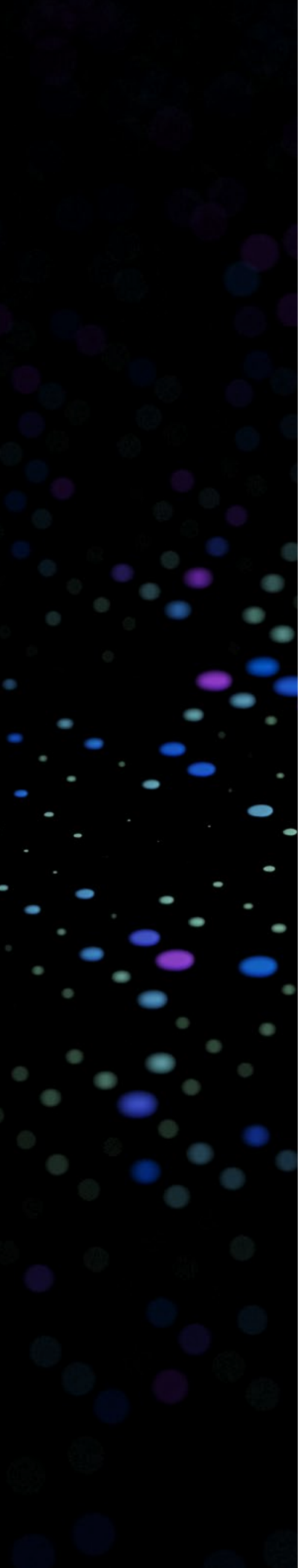
Often clients are challenged by creating, managing and operationalizing threat intelligence. Look for a solution that provides the aggregation, automation, and integrations required to operationalize threat intelligence at scale.

Managed Detection and Response services provide around the clock protection.

Managed Detection and Response (MDR) security services are essential for providing prevention, detection and fast response to insider threats. Solutions that extend beyond traditional prevention by using next-gen AV for behavior-based blocking, investigations, and continuous policy management are key.

Find out how IBM Security helps customers secure the most complex and critical environments from external and internal threats.

Learn more about IBM Security



IBM Security

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
May 2021

IBM