SECURONIX™

2020 Securonix Insider Threat Report

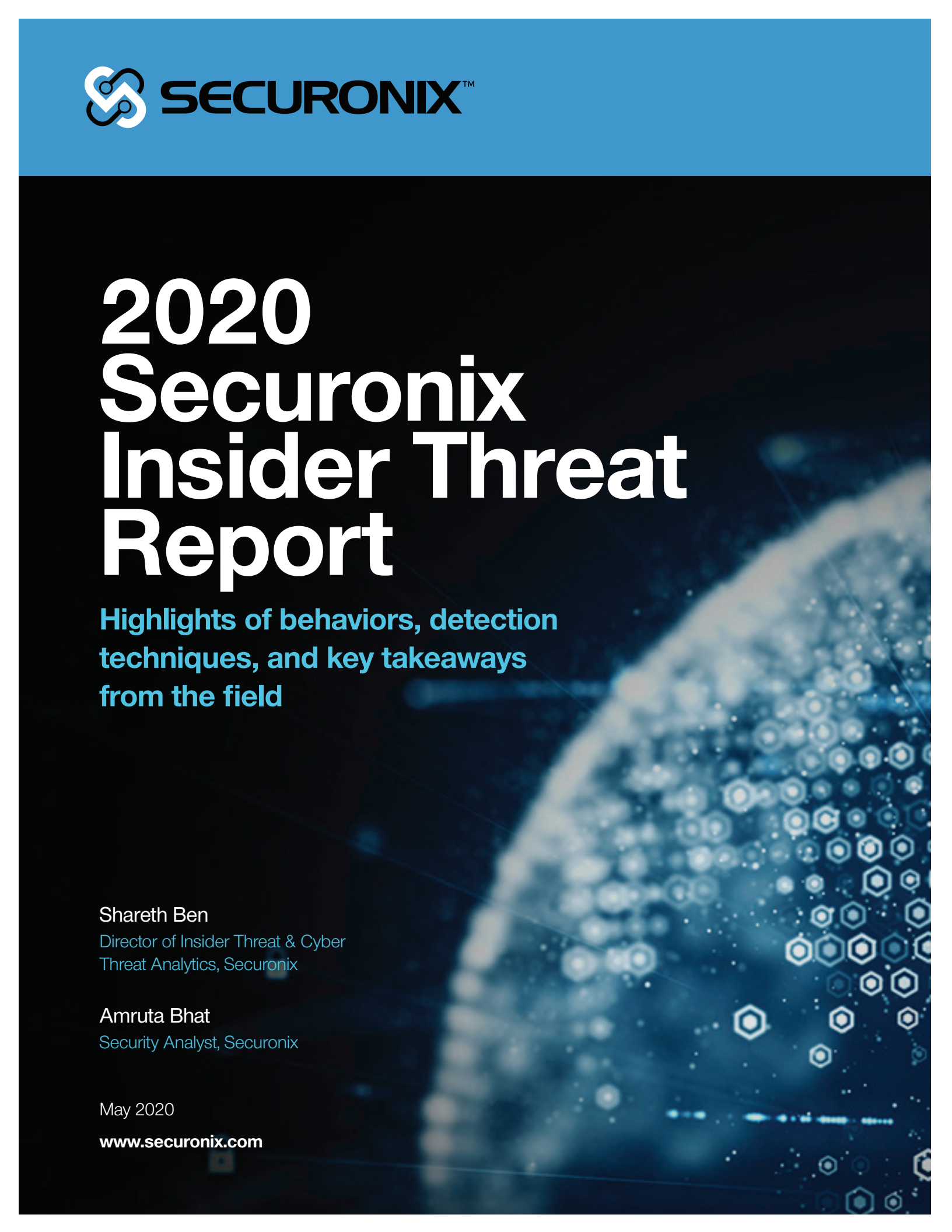
Highlights of behaviors, detection techniques, and key takeaways from the field

Shareth Ben
Director of Insider Threat & Cyber Threat Analytics, Securonix

Amruta Bhat
Security Analyst, Securonix

May 2020

www.securonix.com



Executive Summary

- The exfiltration of data deemed sensitive continues to be the most common insider threat caused by employees and contractors, followed by privileged account abuse, in several organizations.
- The exfiltration of sensitive data over email continues to be the #1 egress vector, followed by web uploads to cloud storage sites.
- An employee or contractor had been identified as a flight risk in about 60% of the incidents detected.

What is a flight risk?

An employee who is about to terminate their employment with a company for various reasons. These employees typically show flight risk behavior patterns when their browsing behavior and email behavior indicate they are leaving the company. This behavior is pertinent to insider threats because over 80% of flight risk employees tend to take data with them, anywhere from 2 weeks to 2 months prior to their termination date.

- Data aggregation and snooping of sensitive data is still prominent in most organizations, however tools to detect such behavior still lag behind. This is primarily due to organizations struggling to classify data that is deemed sensitive, combined with data being vastly distributed across networks and systems.
- Using cloud collaboration tools like Box and Dropbox, sharing data outside the organization has become prominent as companies make the shift to embrace cloud infrastructure and applications for end users. In addition, the ease with which cloud collaboration tools allow for sharing documents with non-business accounts presents an elevated challenge to IT security operations teams.
- The circumvention of IT controls is prevalent across all organizations. IT security operations teams, especially ones from large enterprises, are finding it difficult to draw conclusions about such incidents mostly due to lack of, or differences between, policies and procedures for each line of business.
- Account sharing continues to be a huge problem for organizations, resulting in compliance, security hygiene issues, and, in some severe cases, leading to account compromise.

- For effective insider threat mitigation, product vendors are forced to be precise in applying purpose-built algorithms to curated use cases in order to derive the desired outcomes.
- The work from home situation due to the recent COVID-19 pandemic has exacerbated the problem pertinent to data leaving the enterprise perimeter, which continues to become more porous.

Introduction

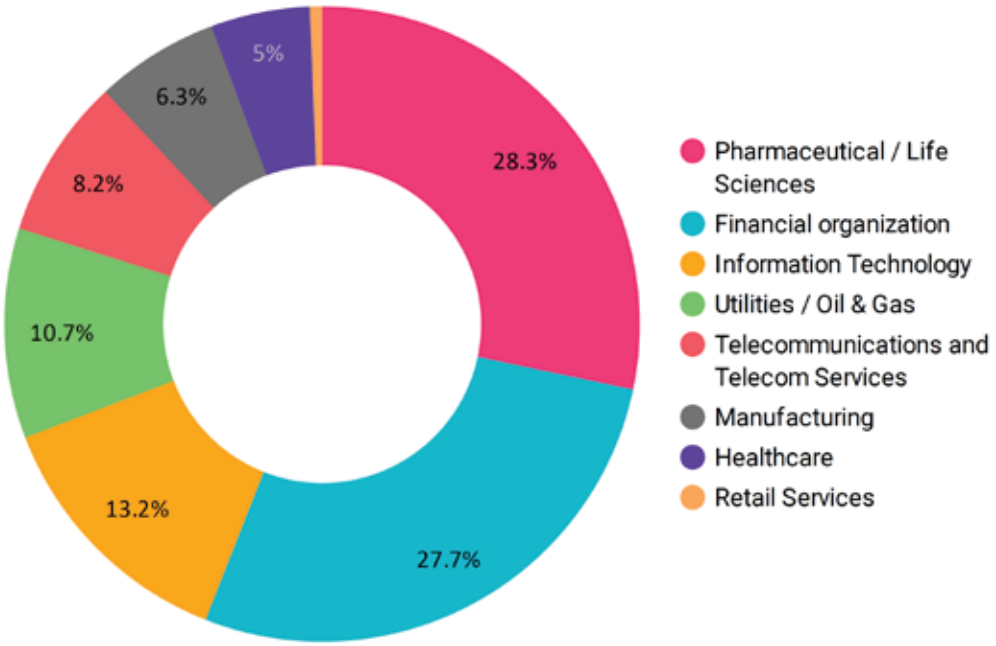
Insider threat continues to be a problem for organizations, regardless of size or industry. Companies are trying to mitigate this risk by continuously investing in tools, people, and processes. The Securonix Threat Research Team has analyzed hundreds of incidents across several industry verticals in order to understand the various behavior patterns that impose risk to organizations. In this report we take a closer look at such behaviors by examining real-life incidents across number of dimensions such as motive and type of risks against industry verticals. The objective of this report is to expose the various types of behaviors that have been observed in the field and the detection techniques that have worked to detect such behaviors. We believe insider threat programs can benefit from such insights in order to make improvements or instill new initiatives that can benefit the organization as a whole.

What is an insider threat?

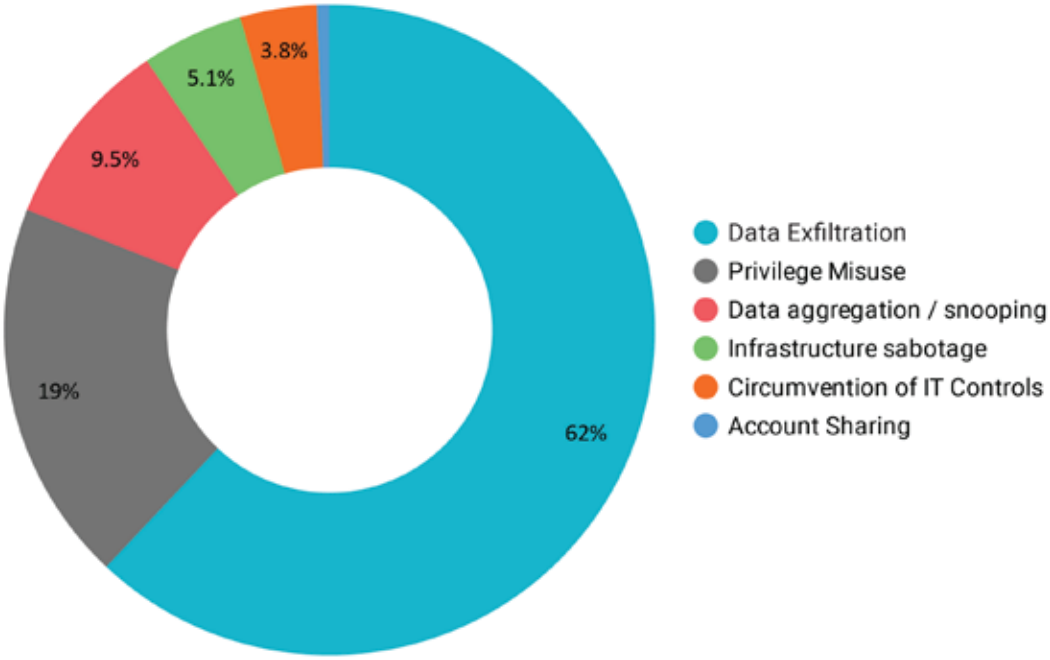
An insider threat is the risk posed by employees or contractors regarding the theft of sensitive data, misuse of their access privileges, or fraudulent activity that puts the organization's reputation and brand at risk. The insider's behavior can be malicious, complacent, or ignorant, which in turn can amplify the impact to the organization resulting in monetary and reputational loss.

Data Profile

The following industries were taken into consideration for this threat analysis. Over 300 confirmed incidents were reviewed across 8 different industry verticals.



The following categories of threat were detected across the industry verticals.



Key Takeaways

The highest number of data exfiltration incidents was observed in pharmaceutical companies, followed very closely by financial organizations. Intellectual property continues to be of high value for nation state and corporate espionage, given the monetary gains and acceleration of replicated drugs to market.

Even those organizations who are mature with their data loss prevention (DLP) technology – the primary tool for detecting data theft – are looking to compensate for its blind spots by deploying additional monitoring controls like user and entity behavior analytics (UEBA).

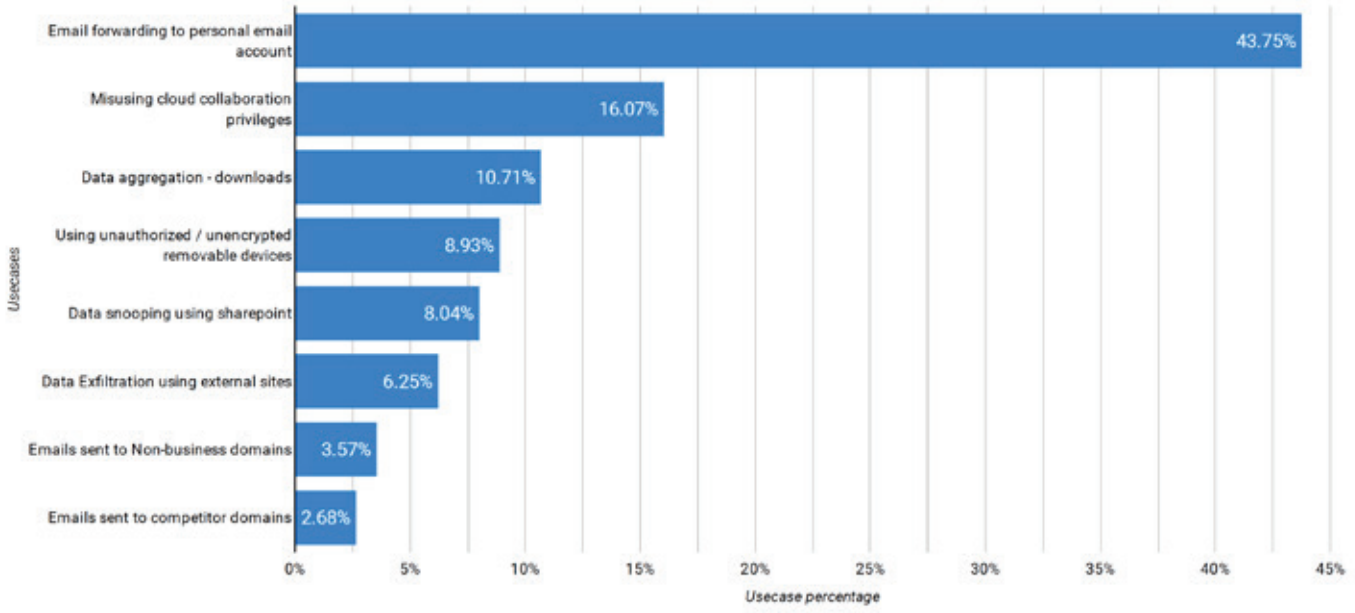
With the increased adoption of cloud-based resources and applications, some aspects of security have been compromised. As they evolve, the business units within an organization need cloud-based third-party tools and platforms to stay competitive. This poses several challenges for security operation teams as they are forced to rely on the third-party's security controls and resiliency. The culmination of a complacent or ignorant insider's actions combined with a third-party vulnerability poses security breach risks to an organization.

Circumvention of IT controls was observed across all types of organizations but was more pronounced in organizations with a lower security posture maturity. The large IT spends on identity and access management (IAM) and identity and access governance (IAG) initiatives have started to bear fruit with financial organizations where high privilege access was observed to be tightly controlled and monitored.

Landspeed violations leading to credential sharing seems to be prevalent amongst all organizations, which causes security hygiene issues and poses credential compromise threats. These indicators, combined with other atomic indicators such as suspicious authentication anomalies and self-escalation of privileges, are proving to be effective ways of detecting insider threats.

Exfiltration of Sensitive Data Detection - Observations

The following chart represents the most common behaviors that were observed when users attempted to, and in many cases were able to successfully, exfiltrate data which was considered sensitive or business critical.



Key Takeaway

The exfiltration of data over email continues to be the #1 exfiltration method, followed by cloud uploads, which continue to be a blind spot for many organizations. We predict that there will be an increase in cloud-based exfiltration attempts and incidents in 2021 as cloud adoption continues to grow.

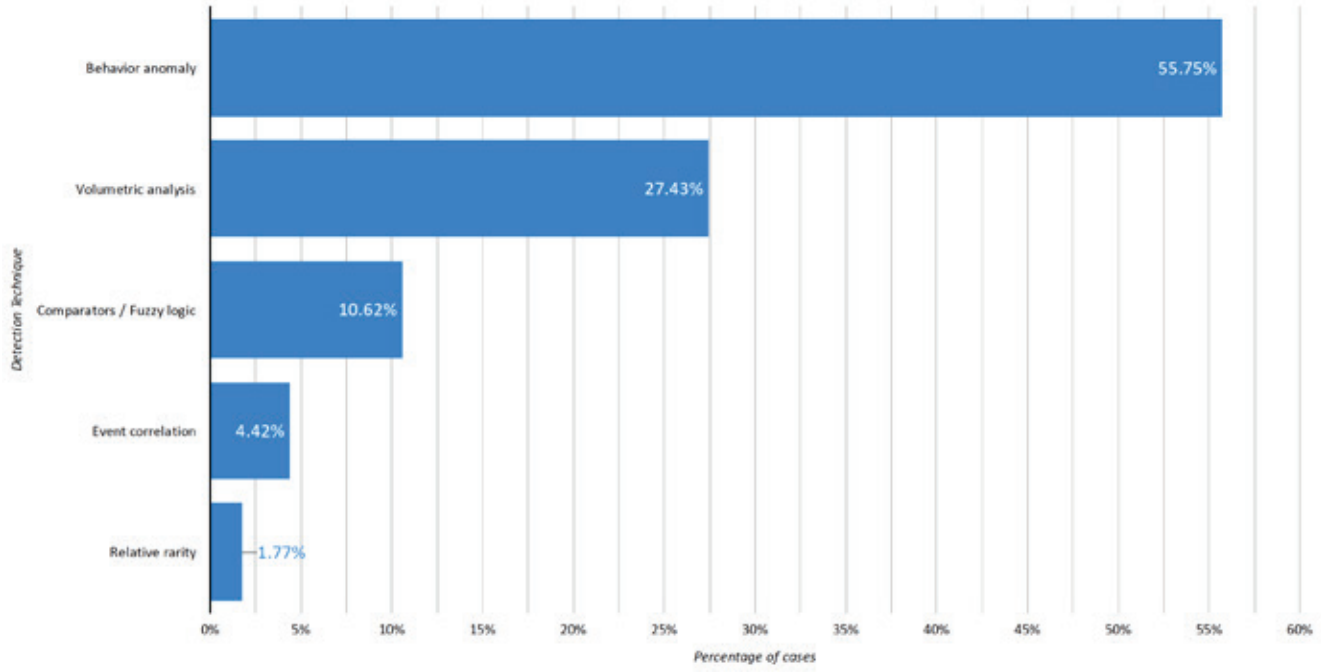
Most organizations continue to find it difficult to classify data deemed sensitive (confidential or business critical) and DLP technologies are always playing catch up. Also, due to the decentralized manner in which organizations store, process, and consume data, nefarious data snooping activities are generally hard to detect. This is where connecting related events using threat chains helps. Typically, an exfiltration attempt is preceded by a data snooping activity, which increases the probability of the user being detected for an infraction.

The number of incidents tied to data exfiltrated using USB continues to decline due to two main reasons – organizations either completely blocking USB usage or heavily restricting it, combined with the increased adoption of cloud-based collaboration tools and applications being used to move data.

A spike in print activity was observed across all industry verticals recently as organizations loosen restrictions on print from home privileges. This is, without a doubt, rushing companies to elevate their monitoring and deploy additional controls like preventing cloud-based e-print which makes it easy to bypass DLP controls.

Detection Techniques Utilized by the Platform

The following detection techniques, powered by a purpose-built algorithm, were deployed in order to detect and predict the exfiltration of data considered sensitive or business critical. The following chart lists the top 5 detection techniques used:



Key Takeaway

Employee behavior may seem normal when they send data over email or copy data to USB, but when they deviate from daily baselined “normal” activity in terms of number of emails they send or quantity of attachments they send, that represents an anomaly in that user’s behavior, which can lead to elevated attention. In most cases, it is a combination of such anomalies that lead to a violation.

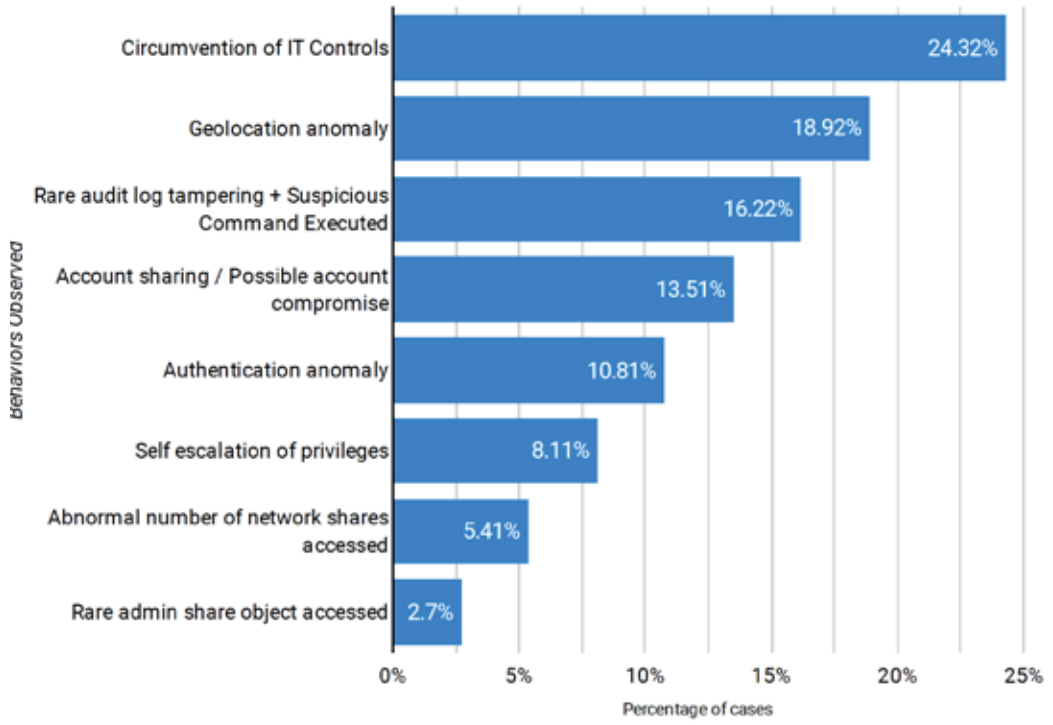
One of the frequently used behavior anomaly algorithms using min/max clustering applies unsupervised machine learning techniques to baseline normal activity and then measures large deviations from that normal activity on a daily basis. This has proven to be successful in detecting nefarious insider threat behaviors.

Volumetric analysis is similar to behavior anomaly where it detects deviations from normal behavior in terms of size or volume. The use cases tied to this algorithm very often trigger when an employee moves or uploads large volumes of data as compared to their past behavior.

Comparators/fuzzy logic in conjunction with relative rarity algorithm is used to detect a first time occurrence of users sending emails to an unknown, non-business email account or to a competitor's email domain, indicating a nefarious data exfiltration attempt.

Detection of (Privileged) Account Misuse Behavior Leading to Possible IT Sabotage - Observations

The following behaviors were observed with privileged account misuse that could lead to IT sabotage-type incidents.



Key Takeaway

Circumvention of IT control violations are often observed in large and mid-size organizations where policies and procedures are not followed because they are either not defined clearly or because users are complacent. Examples observed include employees running powershell with no proper business justification, a spike in undocumented account creation, and misuse of service accounts, where explicit credentials were used to run non-business approved programs.

Another common behavior observed is landspeed violations, which consisted of employees – mostly contractors – sharing administrative credentials to certain business applications, subjecting organizations to risk both from a compliance and a hygiene perspective. In one scenario, a contractor was found logging in from 2 rare countries specific to that organization, indicating a compromised account.

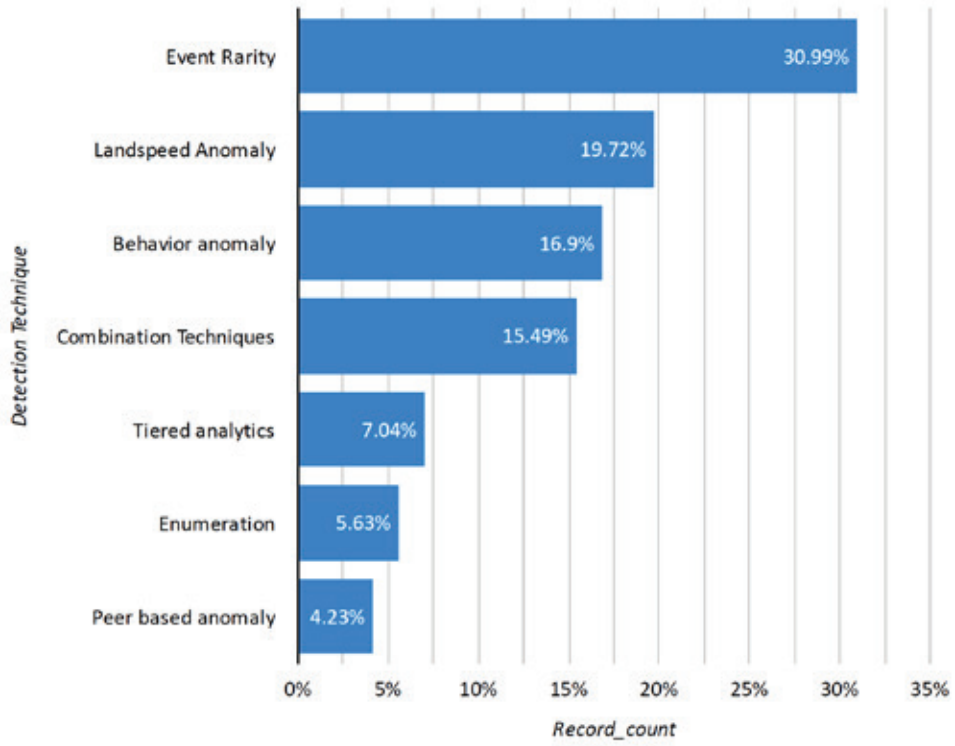
Other scenarios include geolocation-based violations where a service account was used to login to a critical business application using two different source addresses from two different countries (India and China) within an hour. Of the incidents analyzed, contractors were more prone to committing these types of violations.

Authentication anomalies include the misuse of a service account to log in interactively, followed by running a program as multiple target accounts; multiple login failures to cloud collaboration applications from 7-9 countries within a 7 day timeframe; and a rare log in from an undocumented service account.

Network share drives typically hold business-specific data, and security operations is typically sensitive to any anomalies observed in how it gets accessed. An incident involving an undocumented account accessing a network share drive for the first time, followed by that account accessing more than 3,700 objects in the span of 2 days, is an anomaly. This same account was then observed clearing audit logs and changing the auditing setting of an object.

Detection Techniques Utilized by the Platform

The following detection techniques, powered by a purpose-built algorithm, were deployed in order to detect privileged access abuse. The following chart lists the most effective detection techniques used.



Key Takeaway

An event rarity algorithm is effective at detecting anomalies that have happened for the first time, such as an account logging in from a geolocation never seen before, an undocumented account accessing network share objects for the first time, or a non-privileged account running a certain suspicious command which happens to be relatively rare for that account.

The behavioral anomaly technique is effective at detecting abnormal account or system behavior. It does this by comparing current behavior to what is considered normal, based on the past behavior of that entity or by comparing the entity's behavior to its peers. Using this technique, an account was identified as using a scheduled job on a critical server to delete data. The reason ended up being intentional IT sabotage. The irregular frequency of the cronjob that involved the removal of data from a directory was detected using the behavioral anomaly technique.

In order to address the large volume of alerts that are generated from infrastructure logs such as web servers, databases, and endpoints, the tiered analytics technique is essential to filter the noise and highlight events of interest to analysts. Simply put, this technique applies multiple layers of filtering to reduce the number of events of interest to a manageable size, which can then be used for further analysis.

The enumeration technique is particularly useful in detecting a behavior where an account is trying to brute force access to unauthorized systems by attempting to log in to multiple servers within a specified period of time.

Peer-based anomaly detection techniques are powerful in detecting outliers within a peer group – such as a department, division, or a job function – performing an activity that is a deviation from the rest of the peer group's activity as a whole. For example, the Securonix threat research team found cases where a member of a security-enabled group was self-escalating their privileges to run certain DML commands on a critical database.

Conclusion

Using traditional technologies – such as DLP tools, privileged access management (PAM) solutions, and other point solutions – is not sufficient to detect insider threat behavior today. The adoption of cloud systems presents a complex threat fabric which requires advanced security analytics that utilize purpose-built algorithms to detect specific outcomes. In addition, it is essential to stitch these indicators together to form a threat chain that represents a holistic threat, which allows for effective response and threat mitigation.

In order to detect privileged access abuse, which is an important insider threat for companies to combat, by applying a curated multi-stage detection, which combines a rare occurrence of an event in conjunction with anomalies that indicate suspicious or abnormal usage, is proving to be effective since it combines deviations from what is deemed as "normal" behavior for accounts, users, and systems.

We hope this report has been insightful in surfacing specific insider threat behaviors that are affecting organizations today, as well as the approaches that are effective in detecting such infractions.

ABOUT SECURONIX

The Securonix platform automates security operations while our analytics capabilities reduce noise, fine tune alerts, and identify threats both inside and outside your enterprise.

The Securonix platform includes Securonix SaaS SIEM, the #1 cloud-based, next-generation, quadrant-leading SIEM solution. Securonix provides fast time to value through its analytics capability, cloud strategy, and integrated SOAR feature set.

Big data driven, Securonix scales from small startups to S&P 100 global enterprises, providing fast security ROI and predictable cost. It automates security operations, allowing your security analysts to focus on threats, not infrastructure.

CONTACT SECURONIX

www.securonix.com
info@securonix.com | (310) 641-1000

0520


SECURONIX™