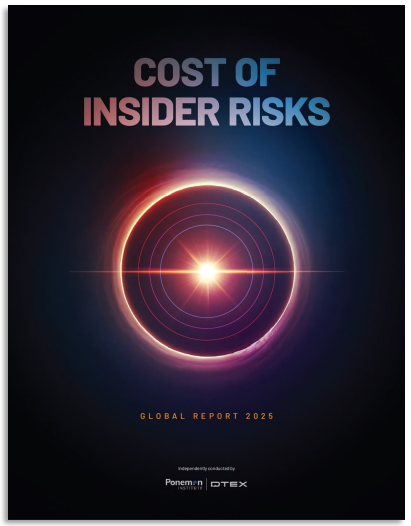
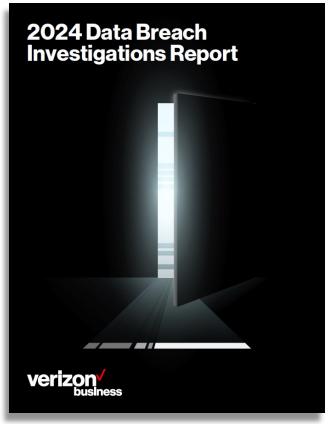

black hat
BRIEFINGS
DECEMBER 10-11, 2025
EXCEL LONDON / UNITED KINGDOM
Understanding Trends & Patterns In Insider Threat
Analysis Of 1,000+ Cases
Michael Robinson
#BHEU @BlackHatEvents

Investigating insider threat cases is challenging.

industry publications

- Built primarily on surveys of executives/managers.
- Insider Threat is a growing problem.
- Provide no actionable information for Digital Forensic Incident Response (DFIR) teams.





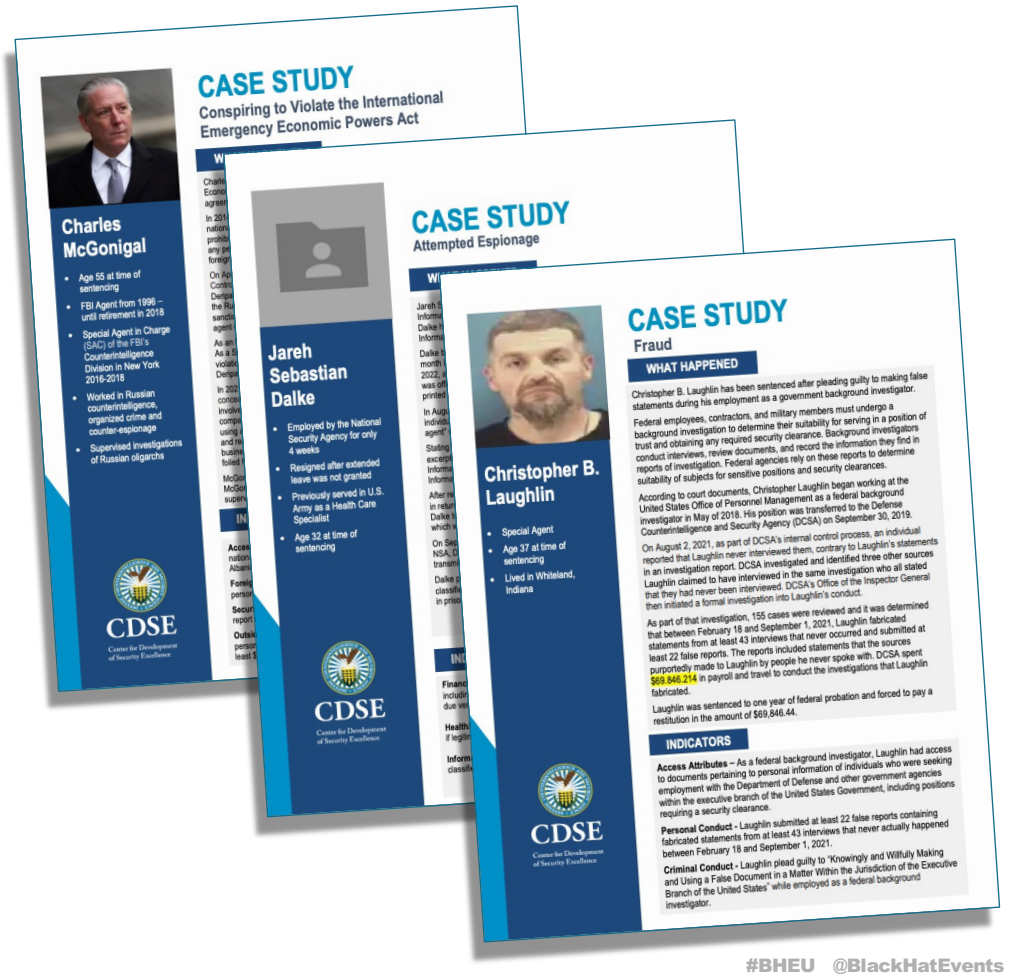
Ponemon Institute. (2025). Cost of Insider Risks: Global Report 2025
Gurucul. (2024). 2024 Report: Insider Threat.
Veriato. (2019). Insider Threat Program Maturity Model.
Verizon. (2024). Data Breach Investigations Report.

"Baseball Cards:"

- Anecdotal stories call attention to the issue.
- Provide no actionable information for digital forensic incident response (DFIR) teams.

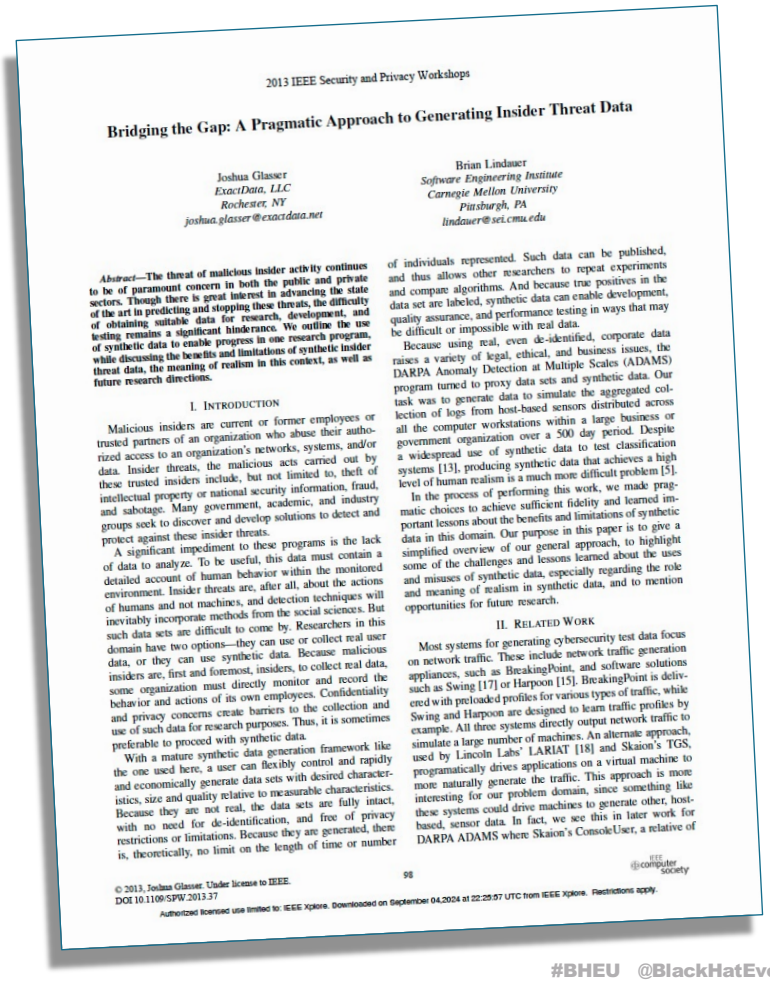
Carnegie Mellon's Software Engineering Institute:

- Periodic posts on the analysis of small datasets.
- Library of cases is private.



Center for Development of Security Excellence.

- Testing is being performed using synthetic datasets.
- Most popular synthetic dataset was released by Carnegie Mellon in 2013. Coincides with the movement of User and Entity Behavior Analytics in 2010.
- Freely available.
- Does not account for changes in TTPs.



2013 IEEE Security and Privacy Workshops

Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data

Joshua Glasser
ExactData, LLC
Rochester, NY
joshua.glasser@exactdata.net

Brian Lindauer
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA
lindauer@sei.cmu.edu

***Abstract*—The threat of malicious insider activity continues to be of paramount concern in both the public and private sectors. Though there is great interest in advancing the state of the art in predicting and stopping these threats, the difficulty of obtaining suitable data for research, development, and testing remains a significant hinderance. We outline the use of synthetic data to enable progress in one research program, while discussing the benefits and limitations of synthetic insider threat data, the meaning of realism in this context, as well as future research directions.**

I. Introduction

Malicious insiders are current or former employees or trusted partners of an organization who abuse their authorized access to an organization's networks, systems, and/or data. Insider threats, the malicious acts carried out by these trusted insiders include, but not limited to, theft of intellectual property or national security information, fraud, and sabotage. Many government, academic, and industry groups seek to discover and develop solutions to detect and protect against these insider threats.

A significant impediment to these programs is the lack of data to analyze. To be useful, this data must contain a detailed account of human behavior within the monitored environment. Insider threats are, after all, about the actions of humans and not machines, and detection techniques will inevitably incorporate methods from the social sciences. But such data sets are difficult to come by. Researchers in this domain have two options—they can use or collect real user data, or they can use synthetic data. Because malicious insiders are, first and foremost, insiders, to collect real data, some organization must directly monitor and record the behavior and actions of its own employees. Confidentiality and privacy concerns create barriers to the collection and use of such data for research purposes. Thus, it is sometimes preferable to proceed with synthetic data.

With a mature synthetic data generation framework like the one used here, a user can flexibly control and rapidly and economically generate data sets with desired characteristics, size and quality relative to measurable characteristics. Because they are not real, the data sets are fully intact, with no need for de-identification, and free of privacy restrictions or limitations. Because they are generated, there is, theoretically, no limit on the length of time or number of individuals represented. Such data can be published, and thus allows other researchers to repeat experiments and compare algorithms. And because true positives in the data set are labeled, synthetic data can enable development, quality assurance, and performance testing in ways that may be difficult or impossible with real data.

Because using real, even de-identified, corporate data raises a variety of legal, ethical, and business issues, the DARPA Anomaly Detection at Multiple Scales (ADAMS) program turned to proxy data sets and synthetic data. Our task was to generate data to simulate the aggregated collection of logs from host-based sensors distributed across all the computer workstations within a large business or government organization over a 500 day period. Despite a widespread use of synthetic data to test classification systems [13], producing synthetic data that achieves a high level of human realism is a much more difficult problem [5].

In the process of performing this work, we made pragmatic choices to achieve sufficient fidelity and learned important lessons about the benefits and limitations of synthetic data in this domain. Our purpose in this paper is to give a simplified overview of our general approach, to highlight some of the challenges and lessons learned about the uses and misuses of synthetic data, especially regarding the role and meaning of realism in synthetic data, and to mention opportunities for future research.

II. Related Work

Most systems for generating cybersecurity test data focus on network traffic. These include network traffic generation appliances, such as BreakingPoint, and software solutions such as Swing [17] or Harpoon [15]. BreakingPoint is delivered with preloaded profiles for various types of traffic, while Swing and Harpoon are designed to learn traffic profiles by example. All three systems directly output network traffic to simulate a large number of machines. An alternate approach, used by Lincoln Labs' LARIAT [18] and Skaion's TGS, programatically drives applications on a virtual machine to more naturally generate the traffic. This approach is more interesting for our problem domain, since something like these systems could drive machines to generate other, host-based, sensor data. In fact, we see this in later work for DARPA ADAMS where Skaion's ConsoleUser, a relative of

DOI 10.1109/SPW.2013.37

Glasser, J. & Lindauer, B. (2013). Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data. *2013 IEEE Security and Privacy Workshops.* DOI 10.1109/SPW.2013.37

- Substantial amount of research performed in the domain of psychology and behavioral sciences.
- Shaw et al.: the Critical Pathway to Insider Risk (CPIR) Model.
- Most fall outside of digital forensics purview. Under the CPIR, the insider's maladaptive responses and concerning behavior may fall into digital forensics.

Internal Security and Counterintelligence

Application of the Critical-Path Method to Evaluate Insider Risks

Eric Shaw and Laura Sellers

But when [past] cases are reviewed in depth, it becomes clear that a lack of appreciation exists for the factors that increase the risk that insiders will undertake hostile acts against their organizations.

Introduction

Governments and institutions of many kinds have faced the danger of hostile acts by insiders from time immemorial. In the case of the US government, such hostile acts have included betrayals by employees who supplied secrets to hostile powers, committed sabotage, and fatally attacked fellow employees. Relatively recent examples of such activity include the espionage activities of Aldrich Ames, Larry Chin, and Robert Hanssen; the Wikileaks revelations of Bradley Manning; the disclosures of Edward Snowden; and the violent assaults against fellow Americans by Nidal Hassan and Aaron Alexis.[a,1]

After each of these events investigators produced reports which, in 20/20 hindsight, assessed the damage and demonstrated that warnings of risks had been missed. These case-based, "One should have seen the writing on the wall" exercises often produce increased awareness and some revisions in policies and practices in screening, adjudication, and risk assessment. But when these cases are reviewed in depth, it becomes clear that a lack of appreciation exists for the factors that increase the risk that insiders will undertake hostile acts against their organizations.

Our purpose in this article is to draw on the most recent and comprehensive empirical studies of insider hostile acts—ranging from formal academic efforts to collections of in-depth case reports—to demonstrate that there exists a common set of factors and a similar pattern of individual and organizational behavior across the many occurrences during recent years. We will describe these factors and the indicators of heightened risk and place them in the context of a "critical-path" analysis, an approach that has been used in business and medical fields to identify the interrelationships of processes and their most critical and vulnerable points. We will apply this framework to historical cases and discuss the implications for counterintelligence and security personnel, as well as for intelligence officers engaged in recruitment activities focused on the insiders in targeted foreign institutions.[b]

a. We use the DoD definition of "insider" contained in DoD INSTRUCTION 5240.26, 15 October 2013, as "A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities."

b. See Eric D. Shaw and Harely V. Stock for a version of this analysis in *Behavioral Risk*

Lenzenweger, M. F., & Shaw, E. D. (2022). The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions. *Counter-Insider Threat Research and Practice*, *1*(1).

Shaw, E. D., & Sellers, L. (2015, June). Application of the Critical-Path Method to Evaluate Insider Risks. *Studies in Intelligence*. *59*(2).

DFIR personnel and detection folks are on their own,
because the industry does not share details.

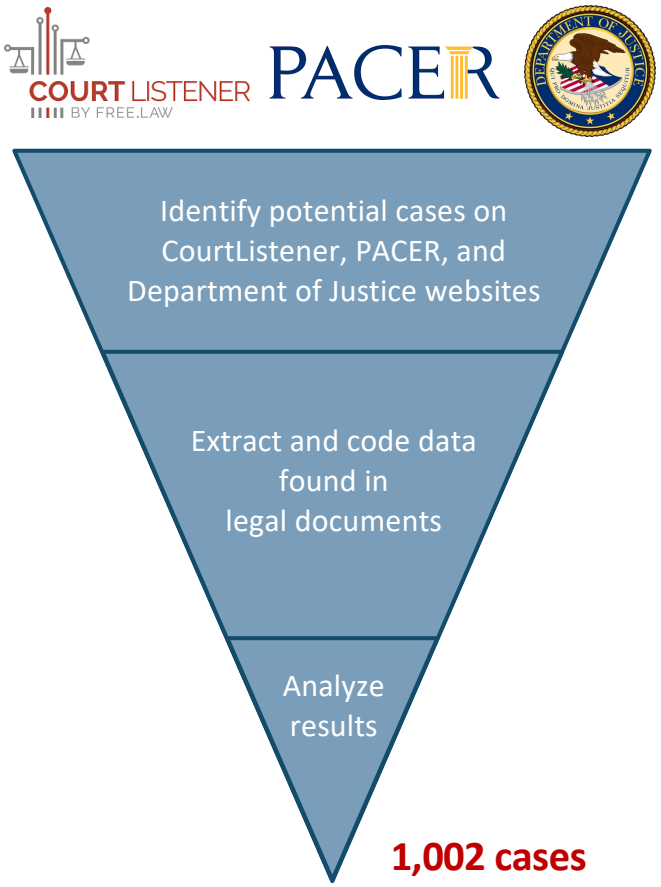
the big question

What are the current trends associated with techniques, tactics, and procedures (TTPs) used by insiders, as identified from real insider threat cases, which can be used to make incident response and forensic examinations more efficient?

Building the Sample

capturing legal documents

Identify and analyze data in U.S. legal documents pertaining to insider threat cases involving computers.



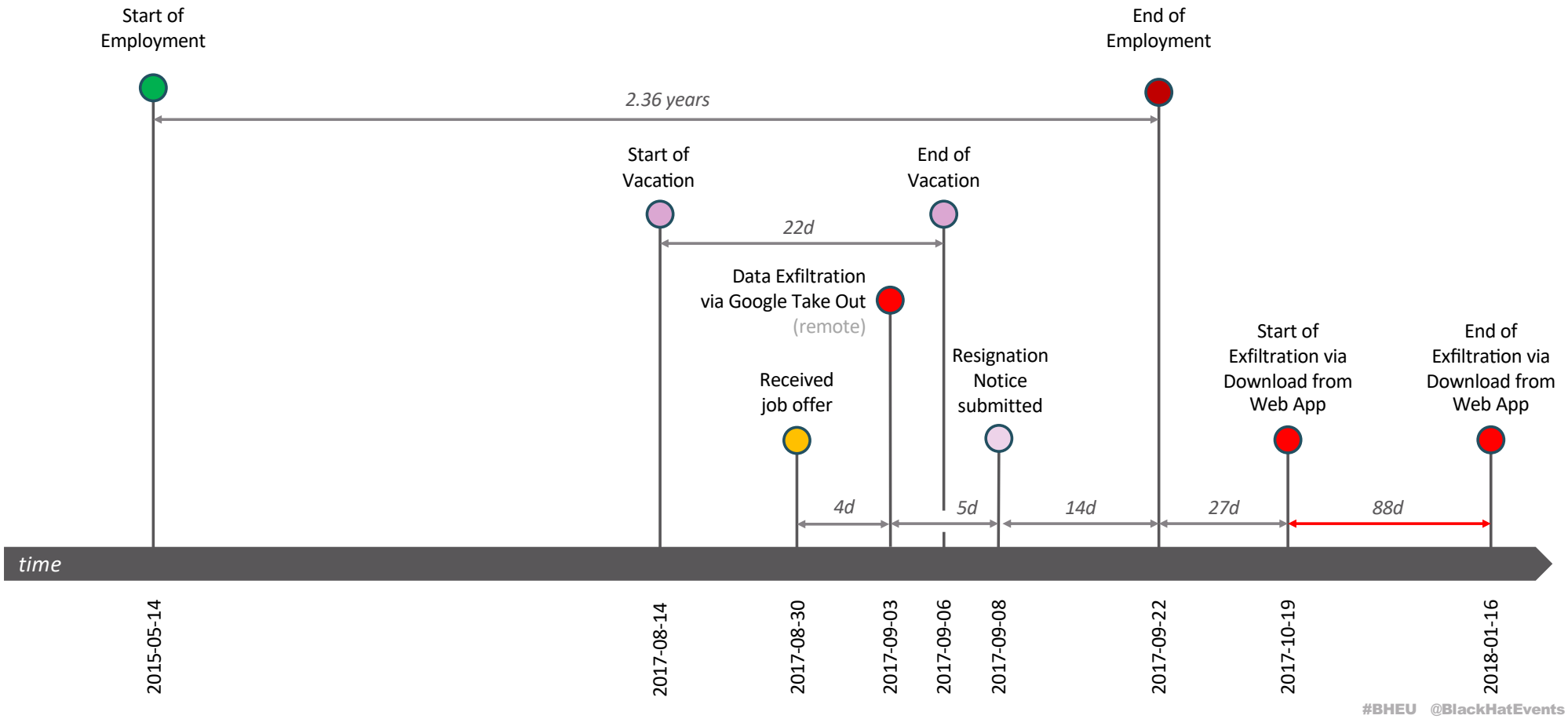
15,000+ cases

1,002 cases

What value would legal documents have?

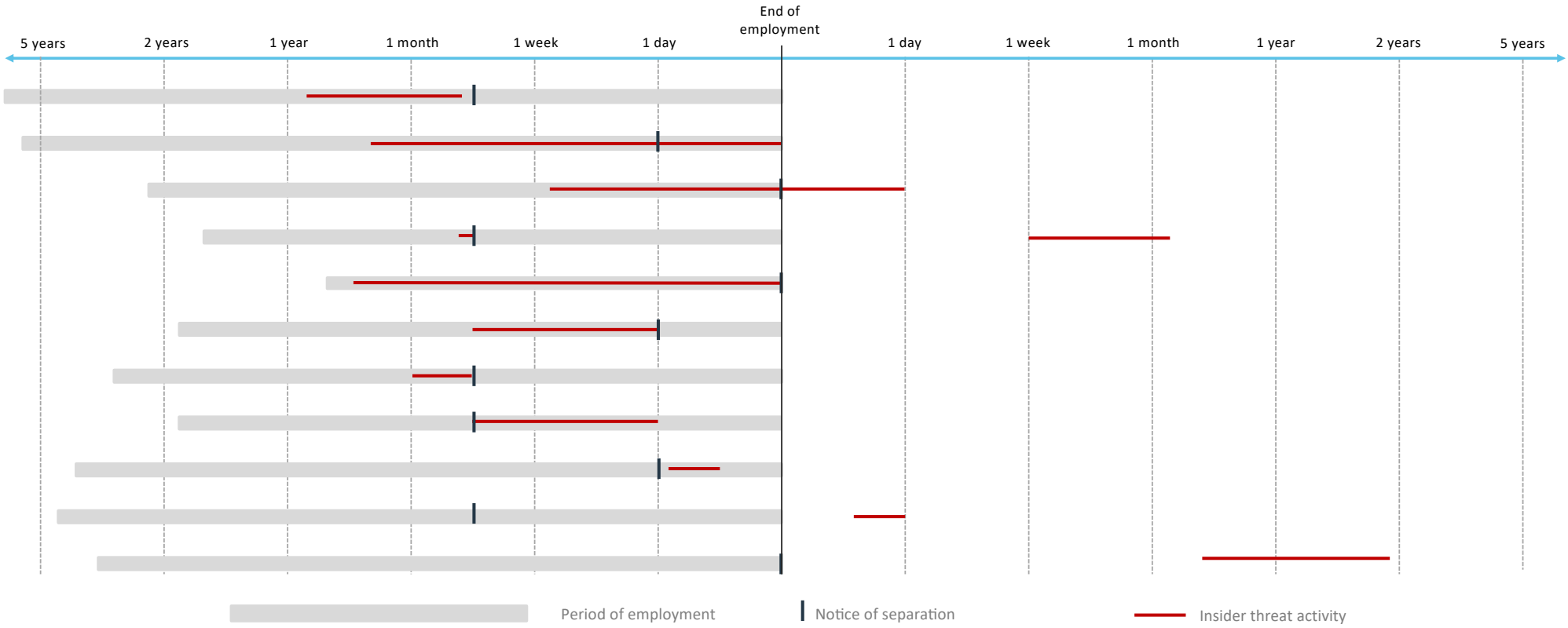
sample case

Business Development Associate, promoted to Account Executive, downloaded 1,000+ documents.



Value comes from aggregating the data.

Timelines from multiple cases



Limitations

limitations of the sample

The universe of insider threat cases is of an unknown size.

Analysis is of a finite sample: 1,002 cases.
1,002 cases may not necessarily be predictive of entire universe.

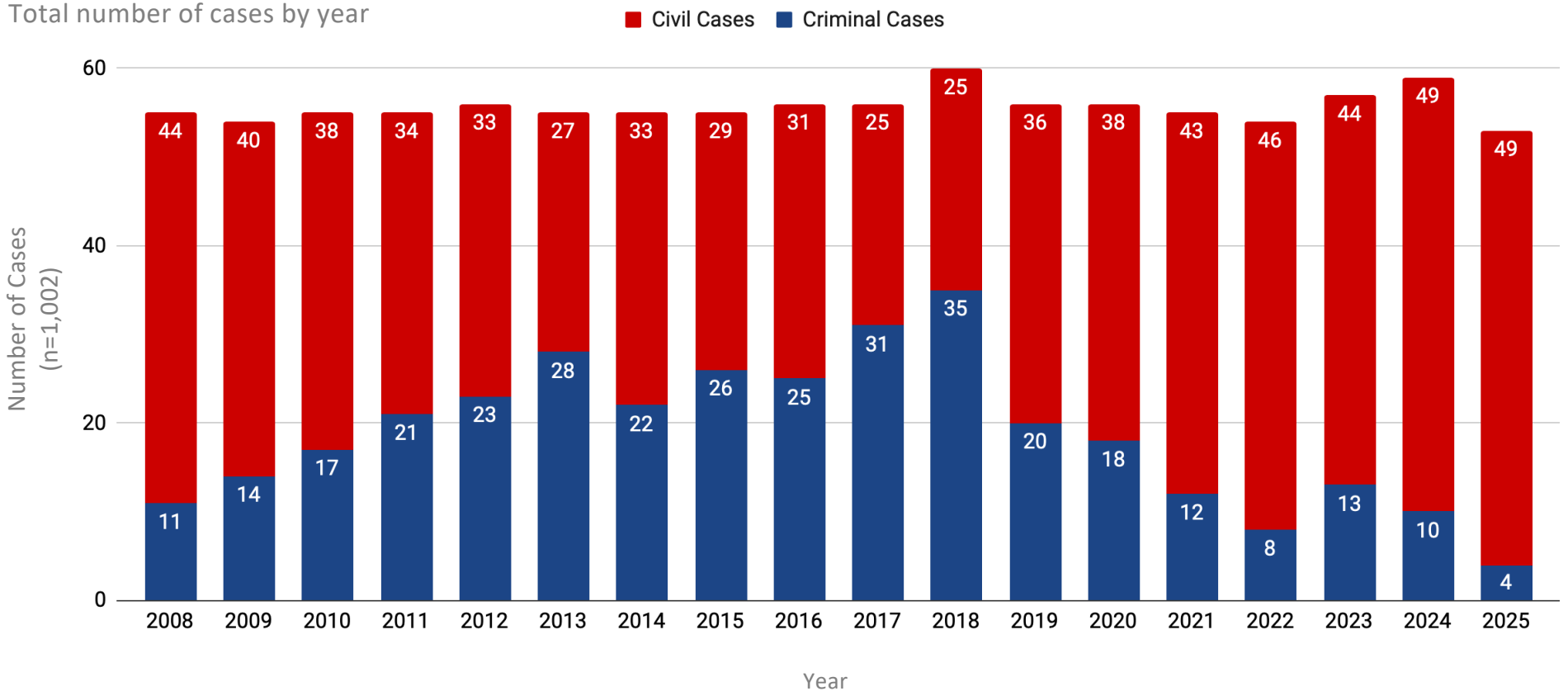
Legal documents tell a story.
Legal documents have holes in them.

Demographics of Sample

demographics

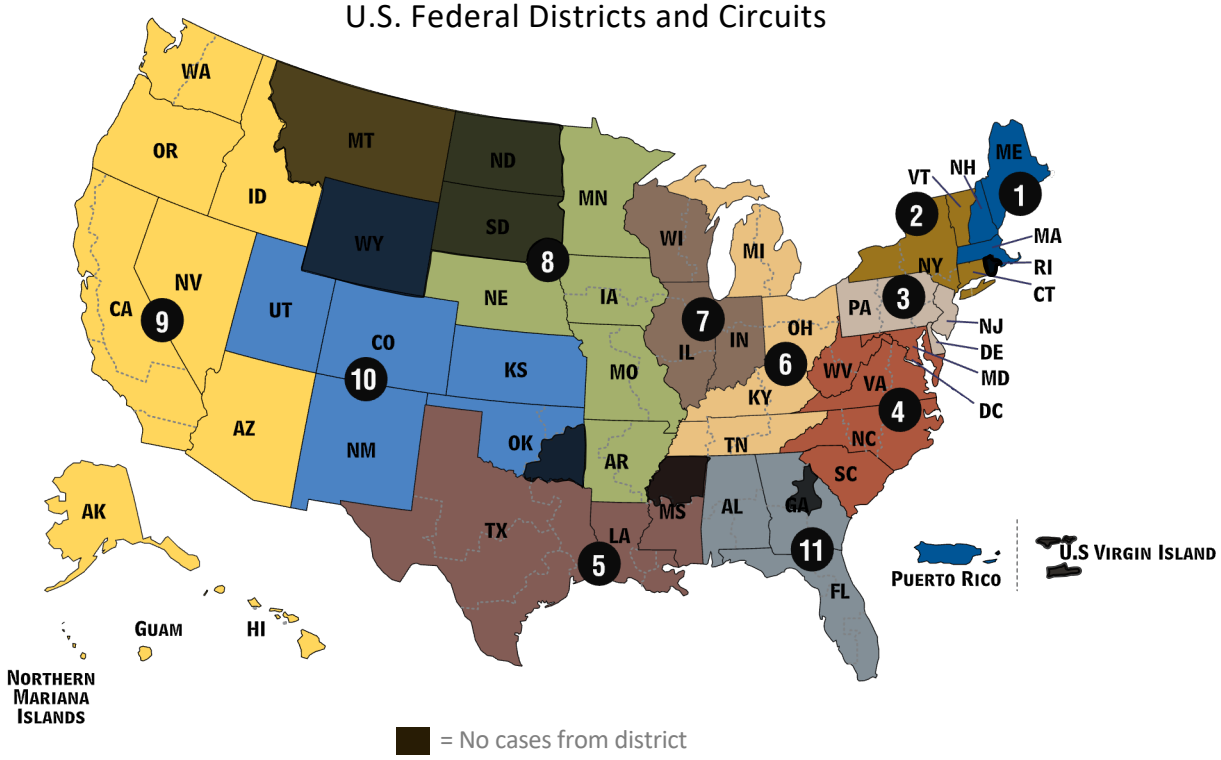
1,002 cases of malicious insider threat activity were analyzed: 664 civil cases; 338 criminal cases

Total number of cases by year



1,002 cases came from all 12 circuits. Cases came from 94 different jurisdictions with 84 of 94 federal districts represented.

U.S. Federal Districts and Circuits



Top Represented Districts

Jurisdiction	Count
Northern District of California	64
Southern District of New York	61
Northern District of Illinois	55
Middle District of Florida	48
Eastern District of Virginia	44
Southern District of Florida	34
District of New Jersey	33
Eastern District of Pennsylvania	33
District of Massachusetts	32
Central District of California	27
District of Colorado	27
District of Maryland	24

demographics

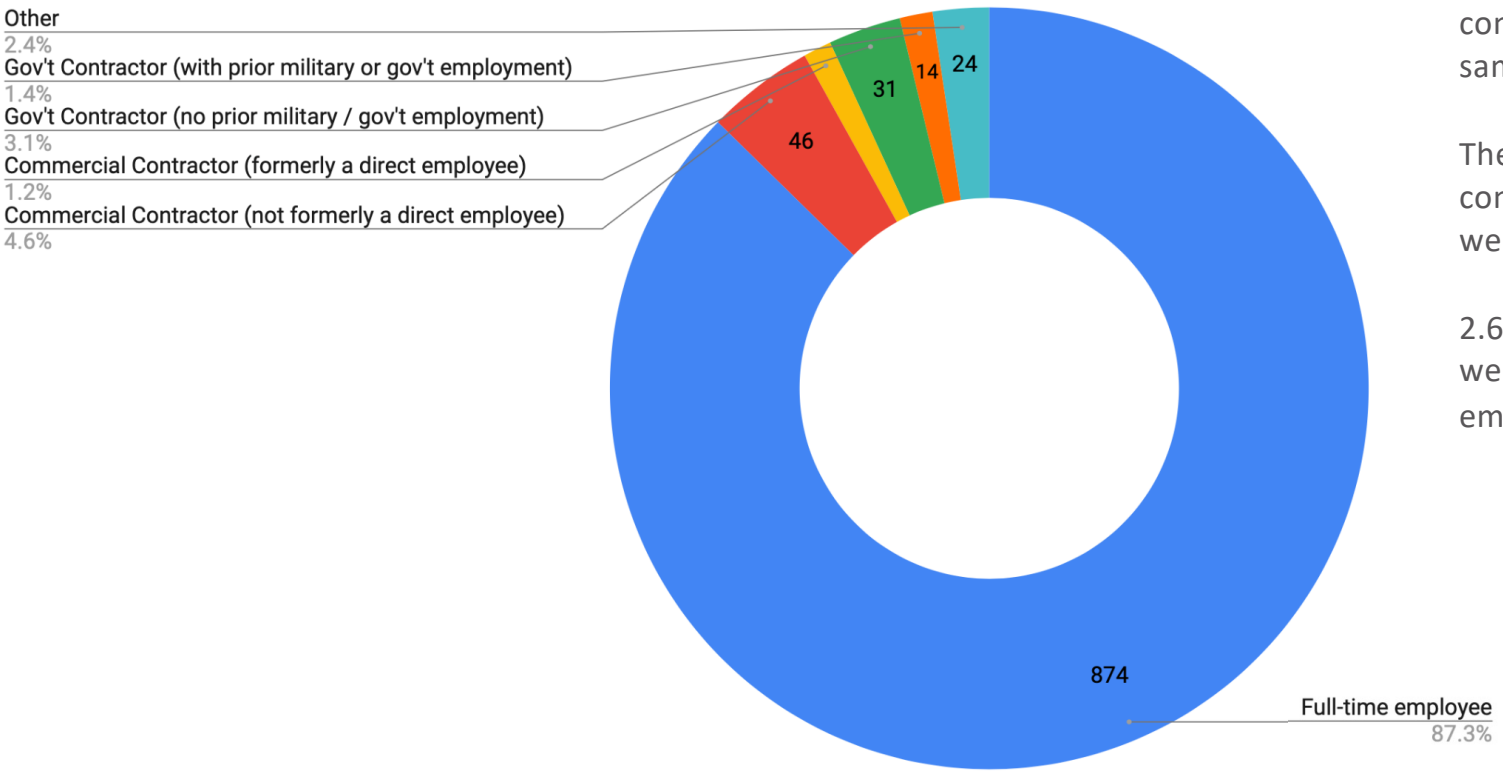
1,002 cases came from 77 different industries.

Top represented industries by count

Industry	Count
IT (not software development)	99
Financial	90
Government	66
Manufacturing	59
Construction	51
Healthcare	45
Automotive	36
Military	35
Energy	33
Software Development	28
Medical Research	28

Demographics of Insiders

874 cases of 1,002 involved full-time employees



Note: A Software Engineering Institute (SEI) blog post in 2010 had a sample of 401 cases where contractors were 15% of the sample.

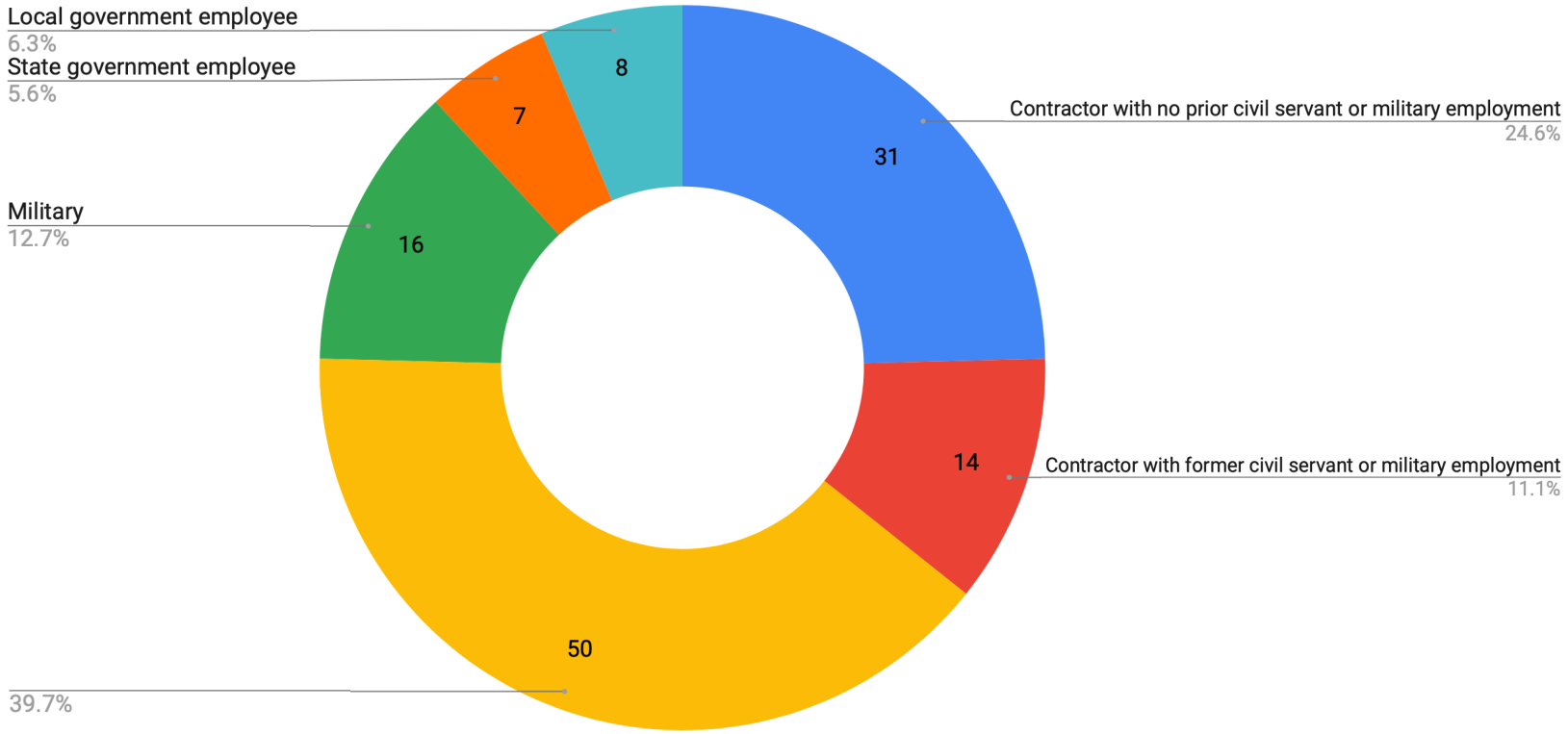
The sample of 1,002 cases contained cases where 10.3% were contractors.

2.6% were “contractors” who were former full-time employees.

demographics

126 cases of 1,002 government or military / defense.

Prior to 2025, the contractors in the U.S. federal workforce outnumbered civil servants 2:1.



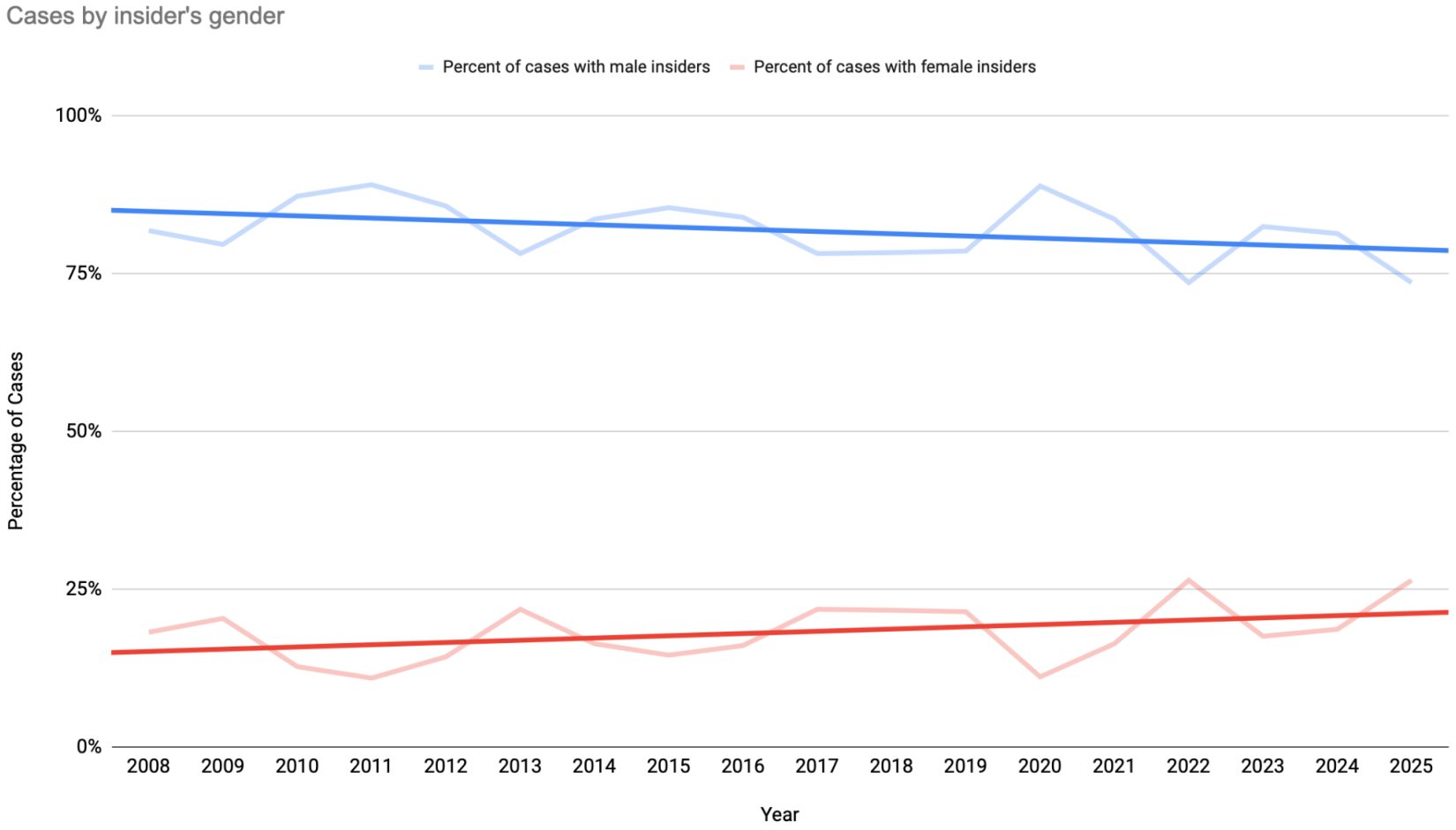
demographics

In this sample, 26% of insiders were at the senior and executive level.
Based on article from *Forbes*, most executive level positions are held by males.

This data appears to align with statistics around STEM jobs.

Gender of Insider	2016 publication from the Software Engineering Institute	This research study
Sample size	820	1,002
Males	517 (63%)	817 (82%)
Females	246 (30%)	181 (18%)
Unknown or other	57 (7%)	4 (< 1%)

demographics

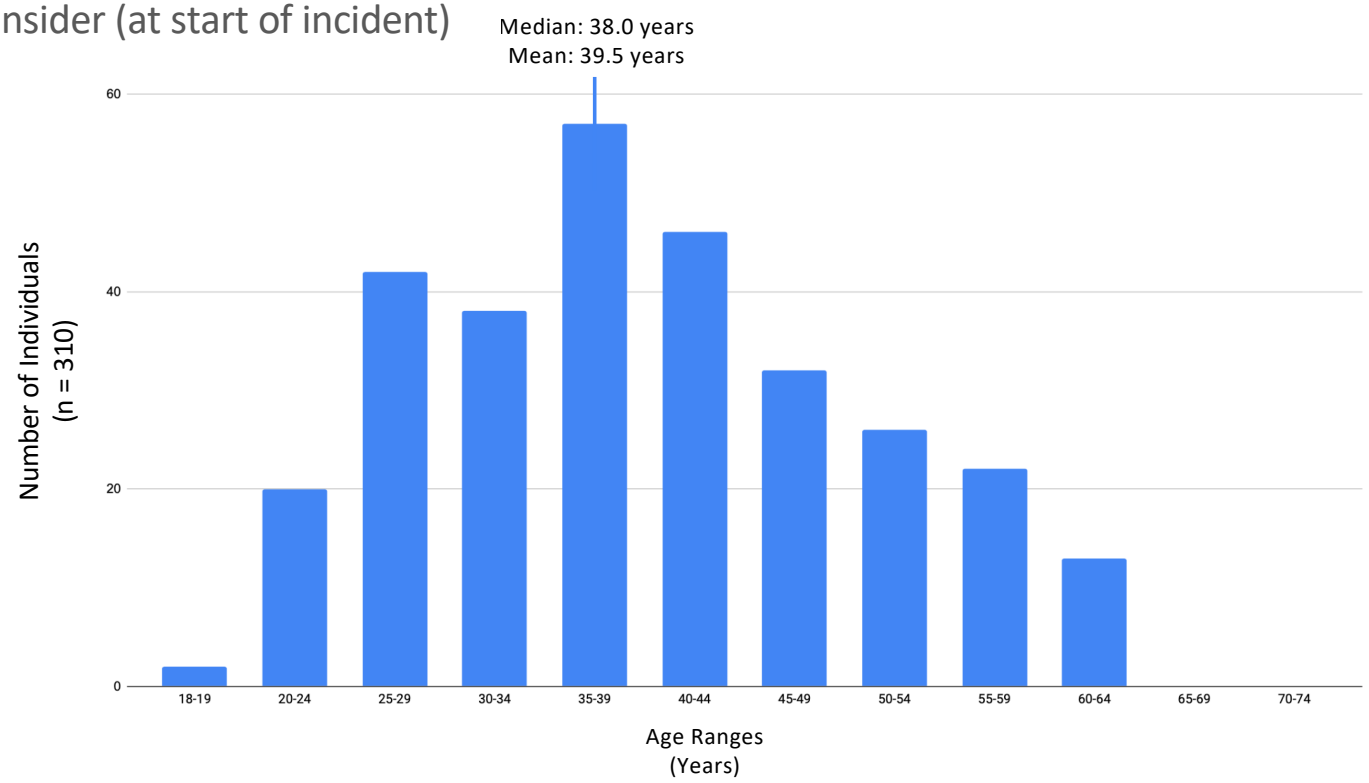


What is the average age of the malicious insider?

demographics

310 of 1,002 cases identified the age of the insider at the start of the incident (mostly criminal cases).
U.S. Bureau of Labor and Statistics (2024): median age of the U.S. worker in 2023 was 41.6 years; in 2013 it was 42.0 years.

Age of Insider (at start of incident)

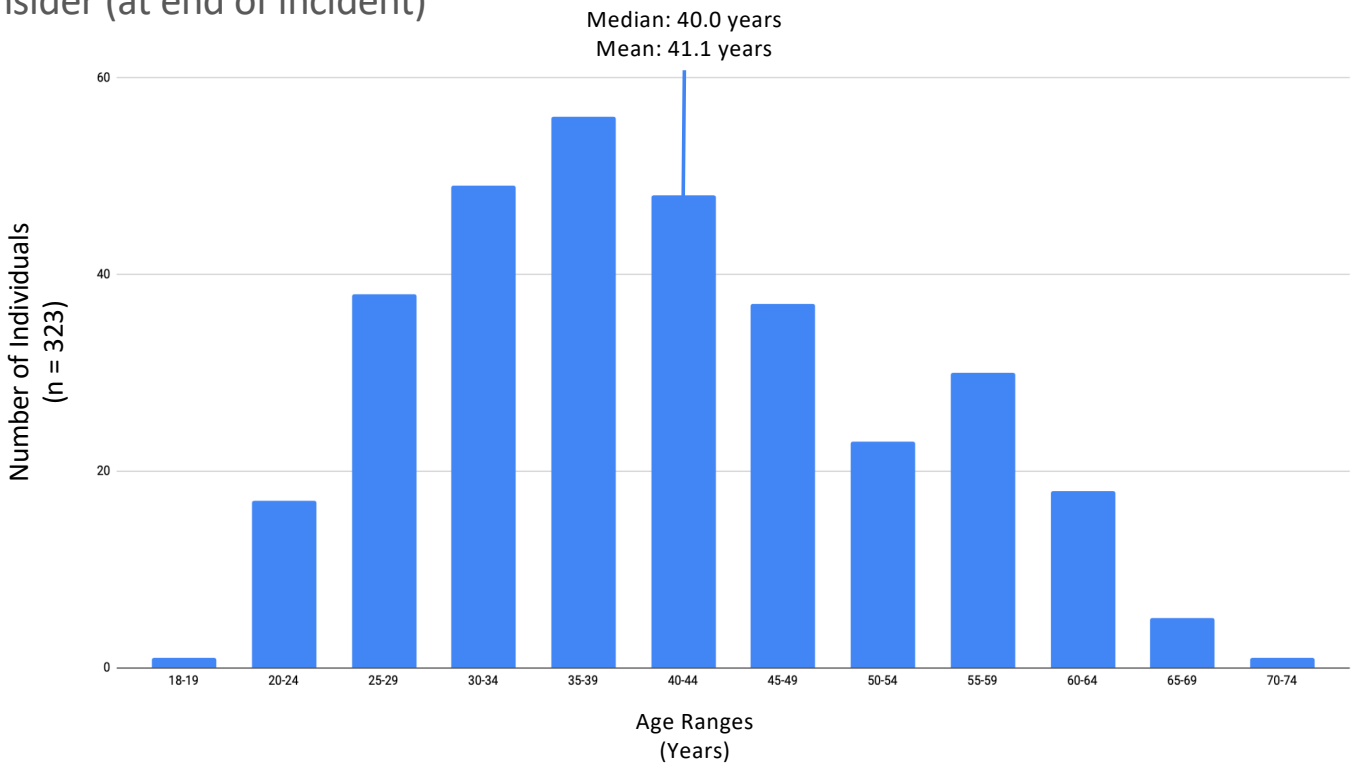


This should be age at time of detection.

demographics

323 of 1,002 cases identified the age of the insider at the end of the incident (mostly criminal cases).
U.S. Bureau of Labor and Statistics (2024): median age of the U.S. worker in 2023 was 41.6 years; in 2013 it was 42.0 years.

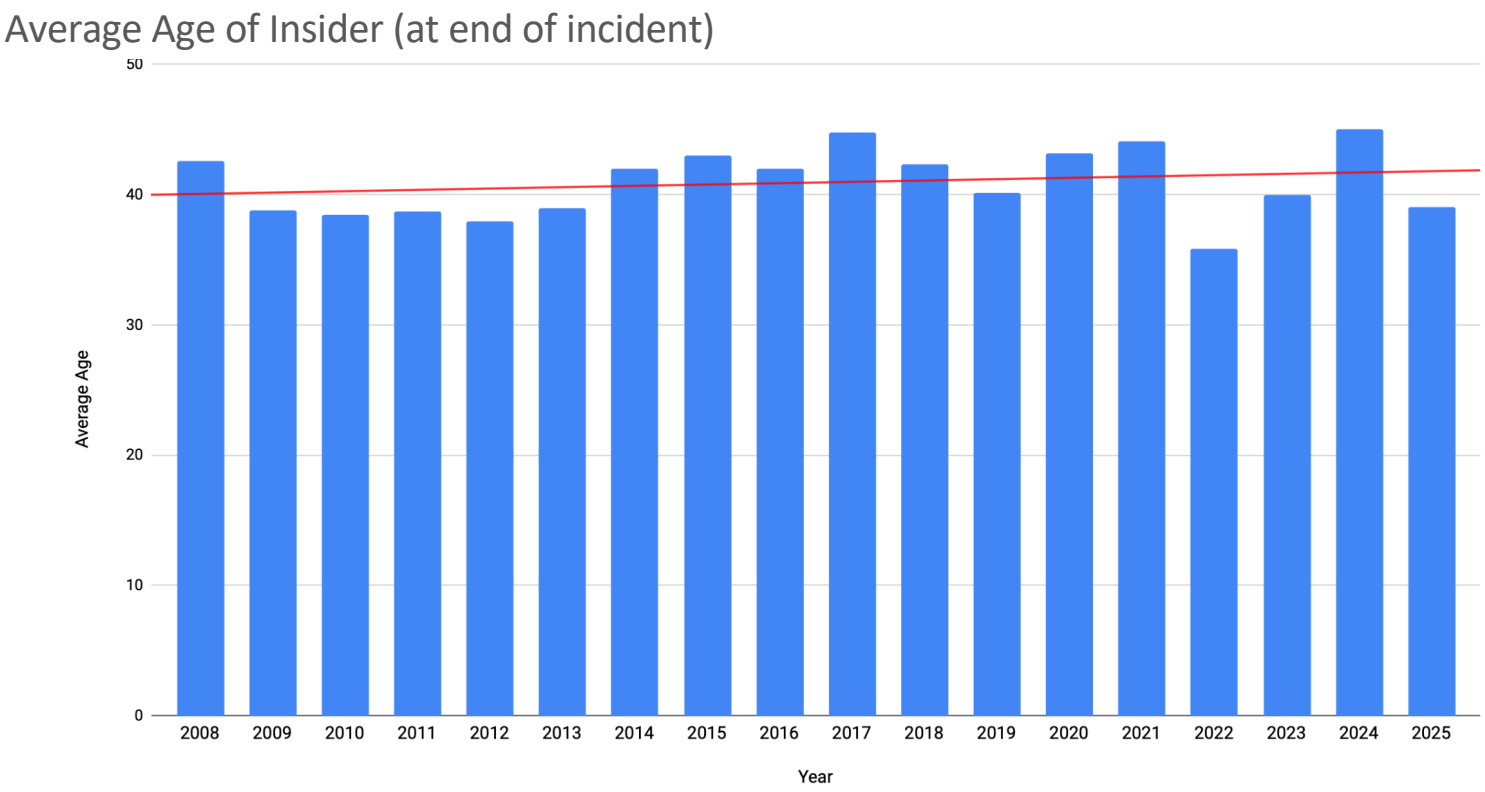
Age of Insider (at end of incident)



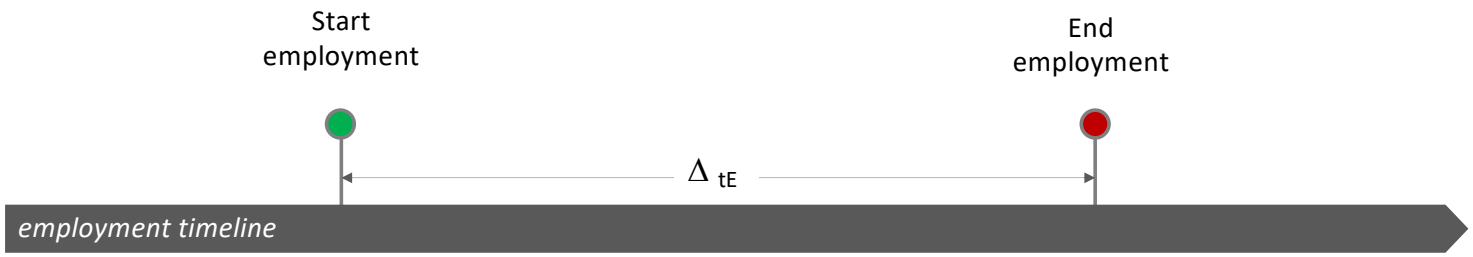
This should be age at time of investigation.

demographics

323 of 1,002 cases identified the age of the insider at the end of the incident (mostly criminal cases).
U.S. Bureau of Labor and Statistics (2024): median age of the U.S. worker in 2023 was 41.6 years; in 2013 it was 42.0 years.



What is the average employment tenure of the malicious insider?

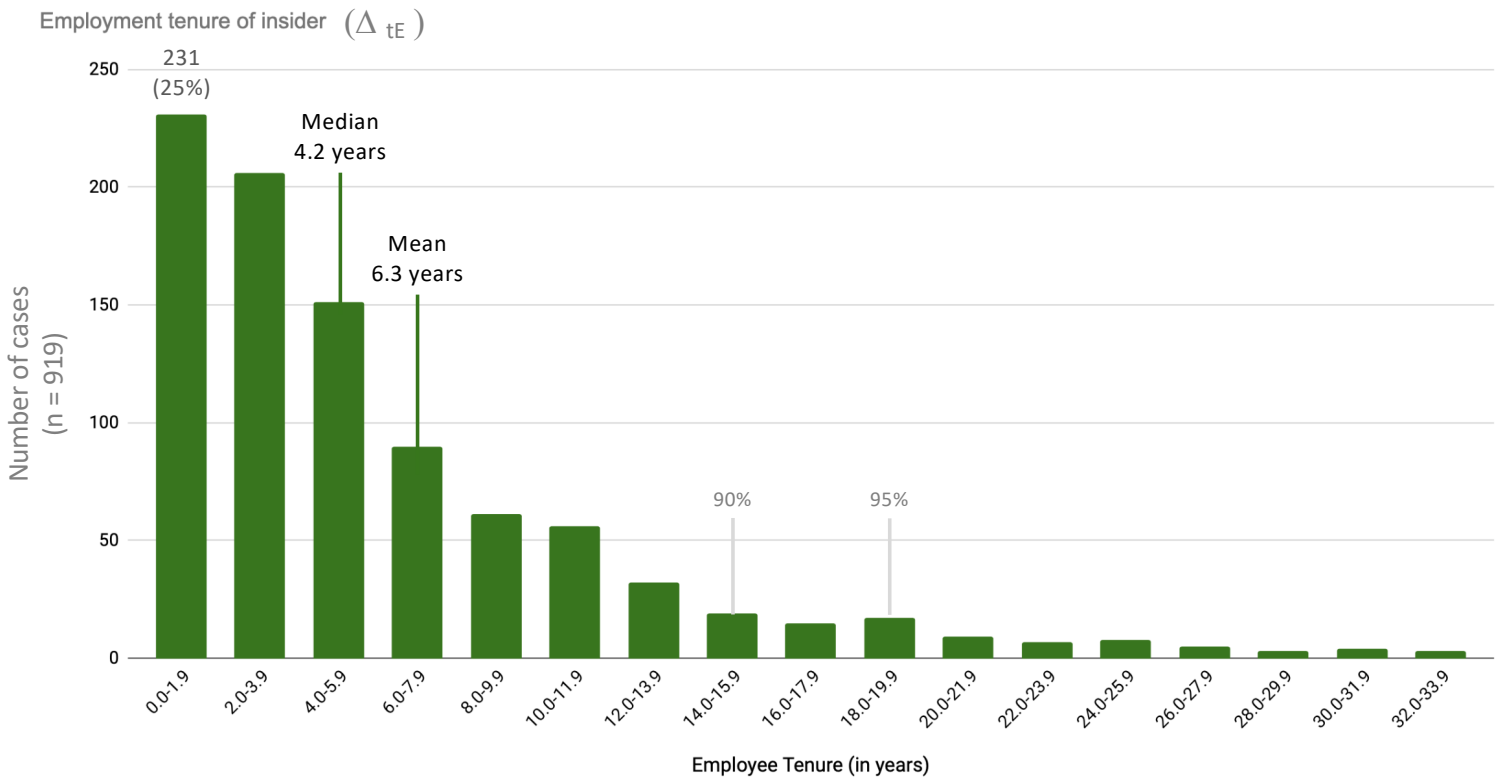


Standard Employee

Δ_{tE} = Employment Tenure

Malicious Insider

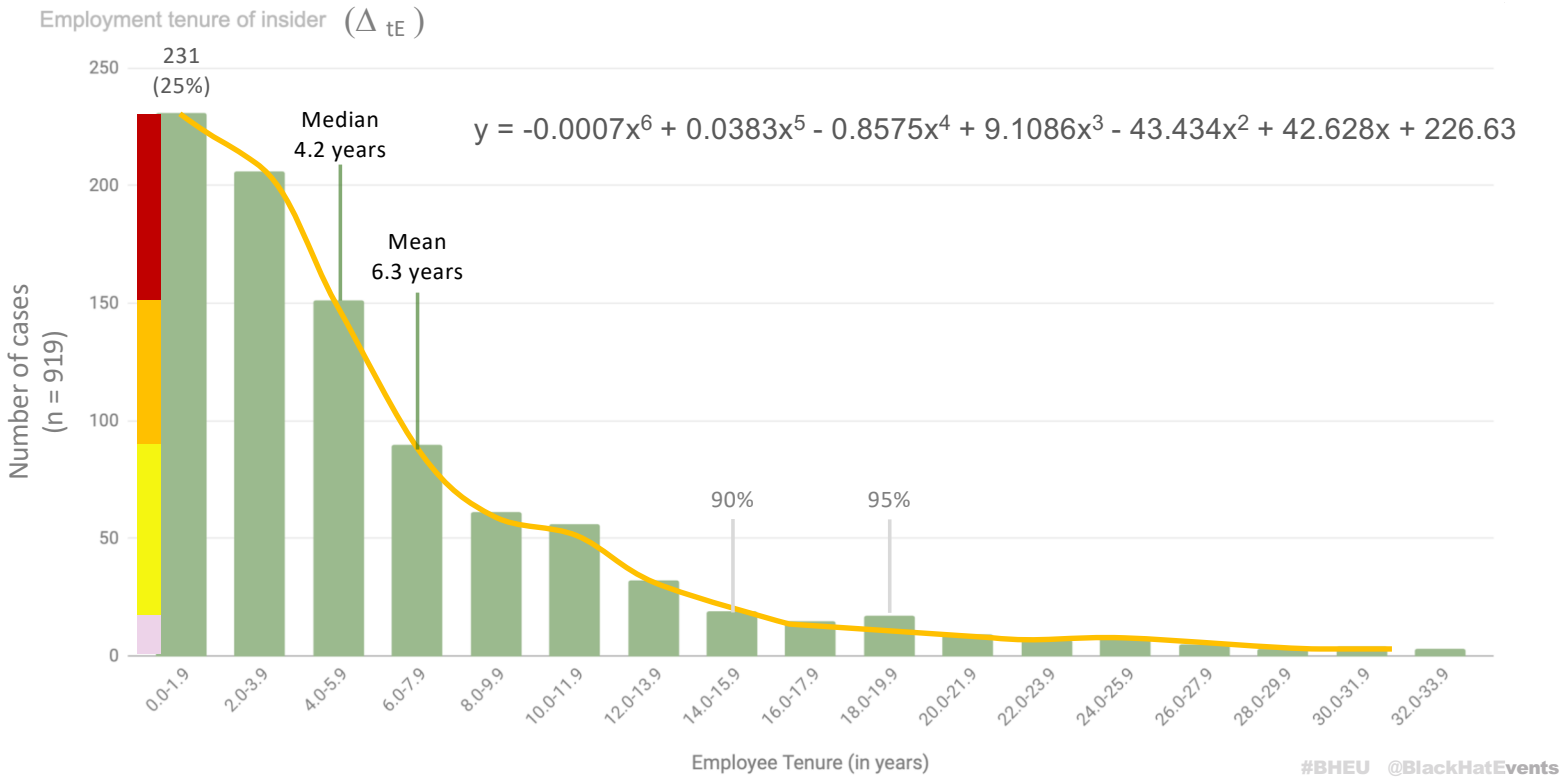
Δ_{tE} = Employment Tenure



Malicious Insider

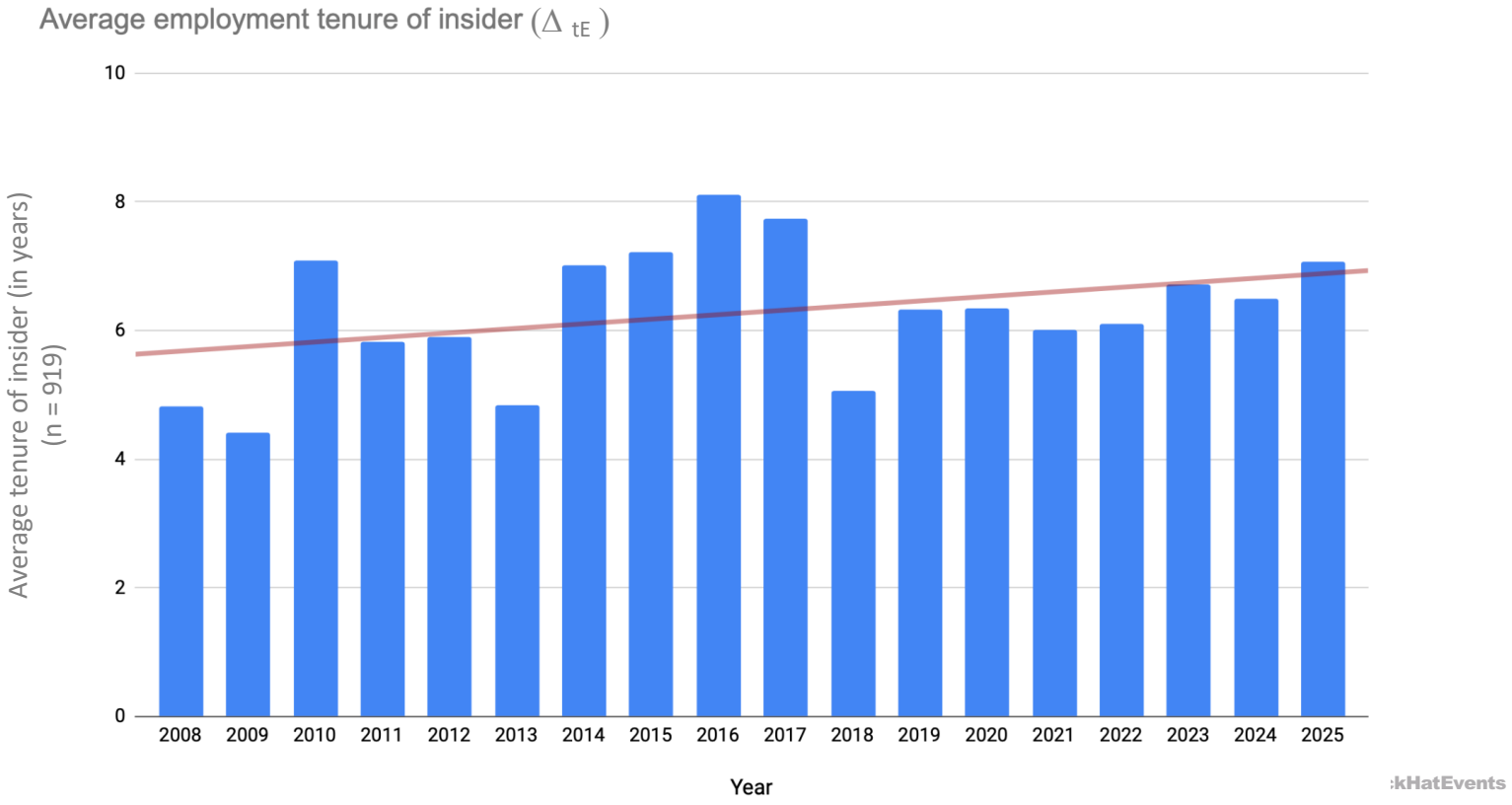
Δ_{tE} = Employment Tenure

Every graph has an equation.



Malicious Insider

Δ_{tE} = Employment Tenure



demographics

Total numbers of cases:	1,002

Performance

Number of actors who were promoted during tenure	197
Number of actors who denied promotions, demoted, PIP	27

Take away: Not all malicious insiders were poor performers. Drift occurs!

demographics

Total numbers of cases:	1,002

Performance

Number of actors who were promoted during tenure	197
Number of actors who denied promotions, demoted, PIP	27

Take away: Not all malicious insiders were poor performers. Drift occurs!

Separation

- Voluntary separation, e.g., resign, retire	507
- Forcible separation, e.g., fired	255
- Contract ended	23
- Layoff / RIF	18
- Separation mechanism not disclosed	196

Take away: The majority of malicious insiders voluntarily separated from their organizations.

demographics

Total numbers of cases:	1,002

Performance

Number of actors who were promoted during tenure	197
Number of actors who denied promotions, demoted, PIP	27

Take away: Not all malicious insiders were poor performers. Drift occurs!

Separation

- Voluntary separation, e.g., resign, retire	507
- Forcible separation, e.g., fired	255
- Contract ended	23
- Layoff / RIF	18
- Separation mechanism not disclosed	196

Take away: The majority of malicious insiders voluntarily separated from their organizations.

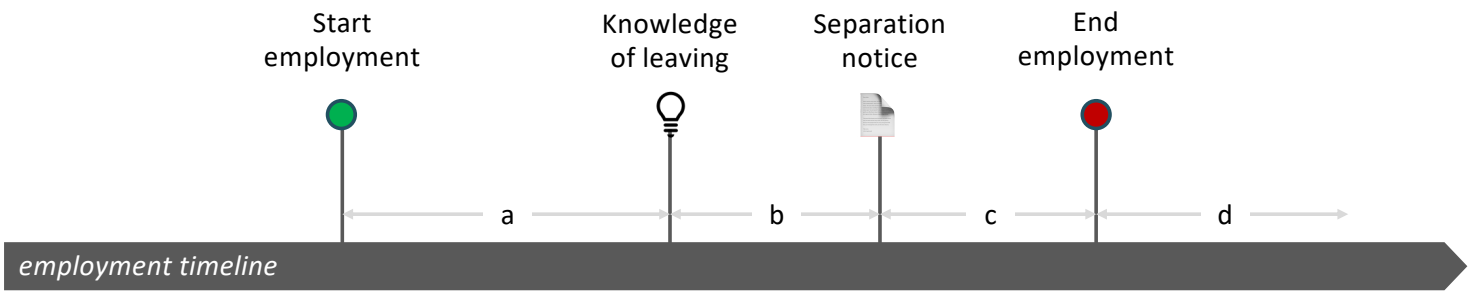
Senior roles within the organization

- Vice President or higher	167
- Directors	95

Take away: ~26% of analyzed cases involved senior leaders engaged in malicious insider threat activity.

Timing of malicious activity


Start
employment
End
employment
employment timeline

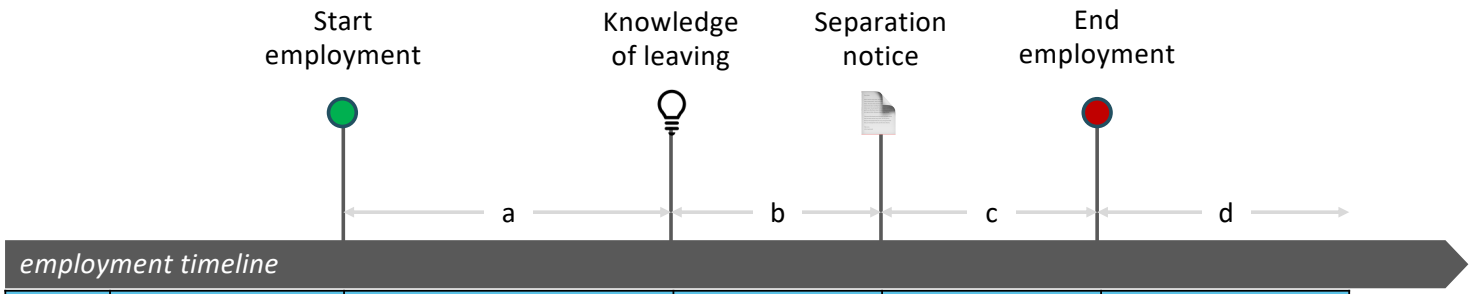


Key elements of employment timeline:
1.) start their employment,
2.) eventually have knowledge that they will separate employment,
3.) generate or receive a separation notice that formally documents the upcoming separation, and
4.) employment ends.

Knowledge of leaving include things such as:
- Job offer from another company
- Founding competing company
- Awareness of a pending termination before official notice
- Awareness of a layoff or RIF before official notice
- Awareness of a contract ending before official notice

Separation notice include things such as:
- Resignation notice, e.g., quitting
- Termination notice, e.g., fired

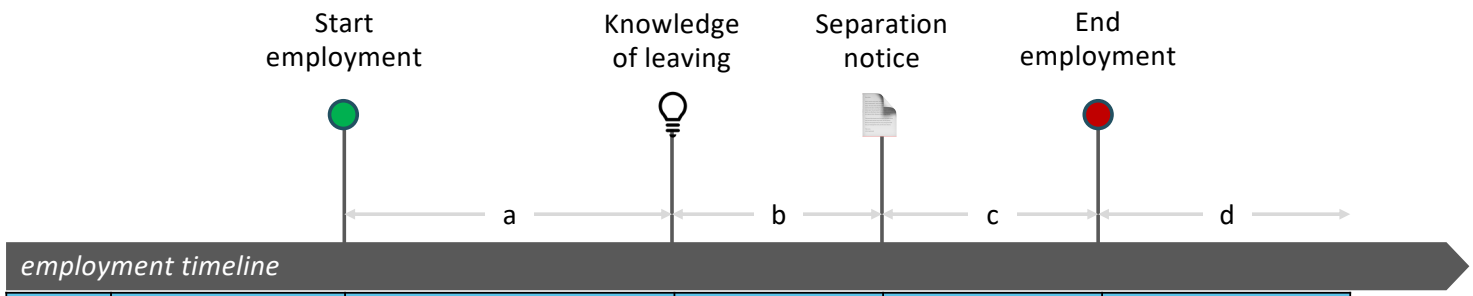
Malicious insider activity has occurred at various stages during the employment lifecycle.



Row	Count	a	b	c	d
1	293	X			
2	162		X		
3	46			X	
4	172				X
5	30		X	X	
6	22	X		X	
7	26	X	X		
8	12	X	X	X	
9	22			X	X
10	61		X		X
11	109	X			X
12	13		X	X	X
13	13	X		X	X
14	14	X	X		X
15	7	X	X	X	X

X = Malicious activity occurred

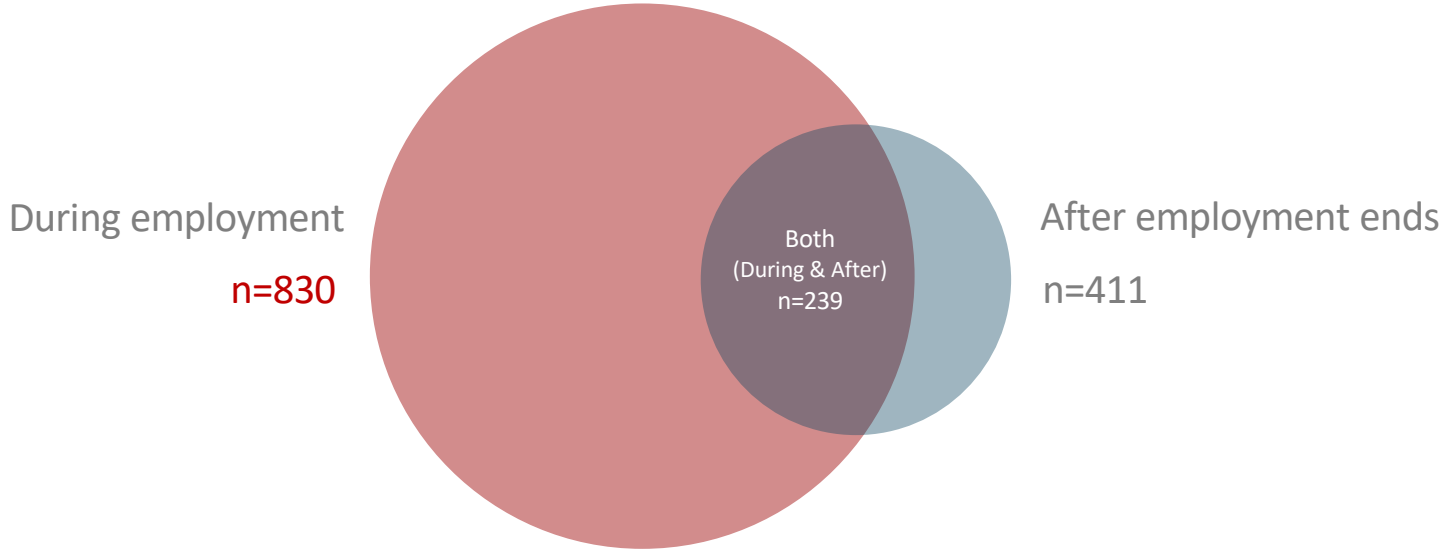
Malicious insider activity has occurred at various stages during the employment lifecycle.



Row	Count	a	b	c	d
1	292	X			
2	162		X		
3	46			X	
4	172				X
5	30		X	X	
6	22	X		X	
7	26	X	X		
8	12	X	X	X	
9	23			X	X
10	61		X		X
11	109	X			X
12	13		X	X	X
13	13	X		X	X
14	14	X	X		X
15	7	X	X	X	X

X = Malicious activity occurred

timing of malicious activity

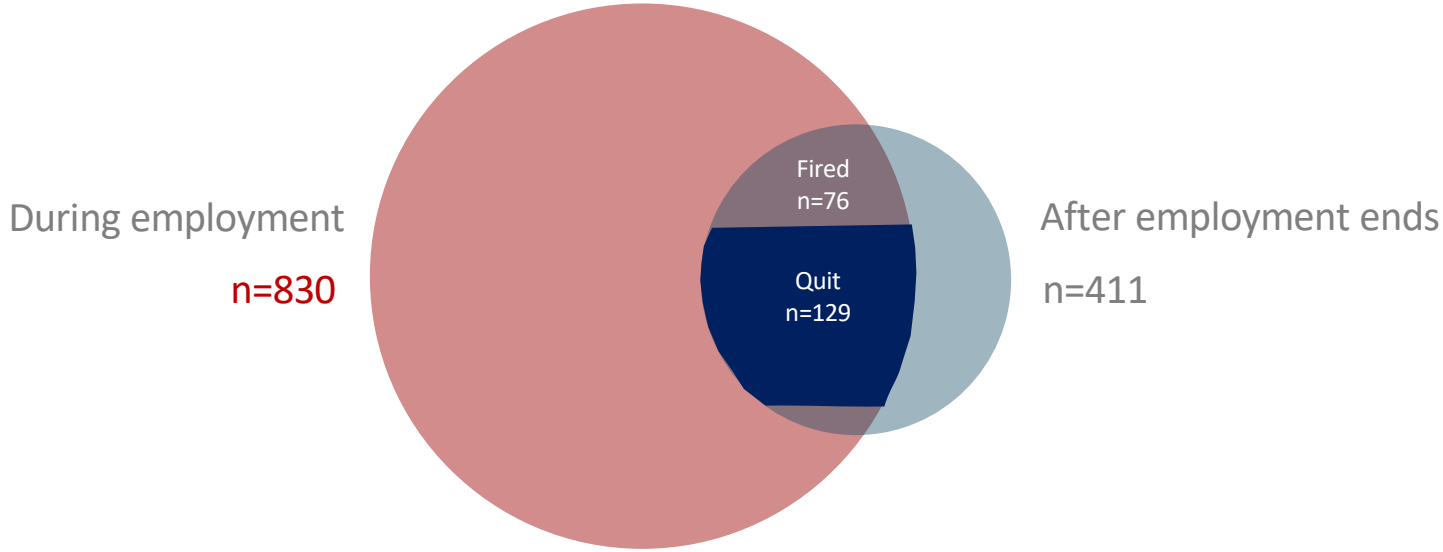


239 (29%) malicious insiders, who were active during employment, remained active after employment ended.

TTPs used during and after employment are largely different.
In 208 of the 239 cases, the TTPs used after the insider's separation from the organization was different.

Take away: Insiders are active during and after employment. Over 25% return to cause harm.

timing of malicious activity

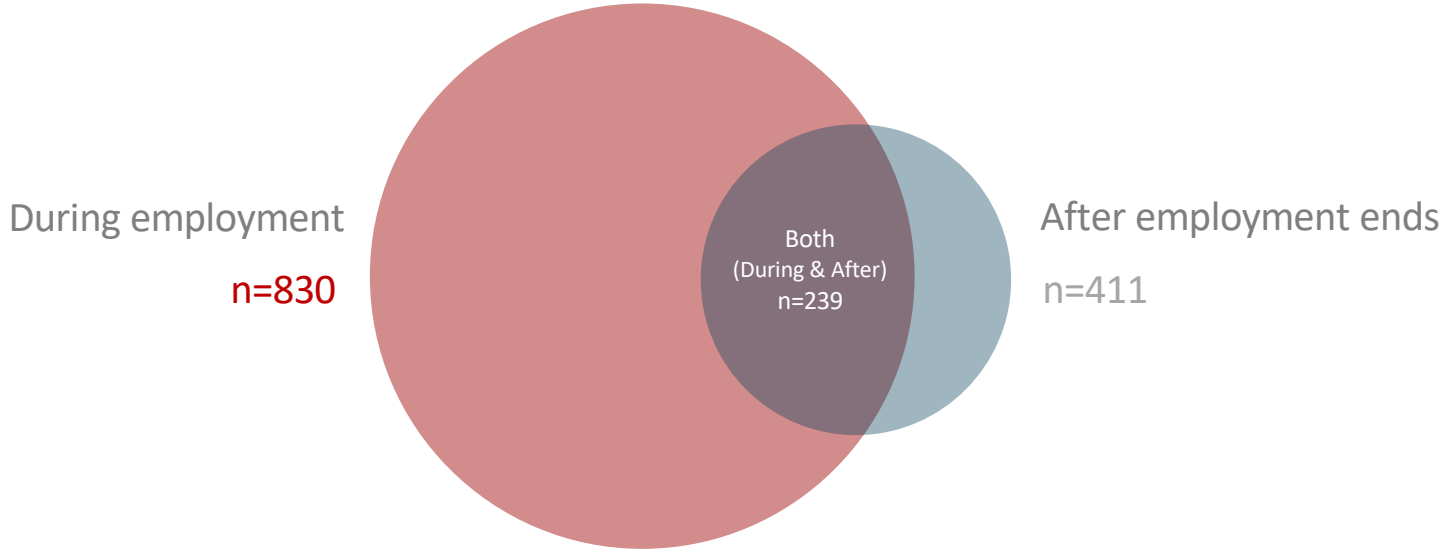


239 (29%) malicious insiders, who were active during employment, remained active after employment ended.

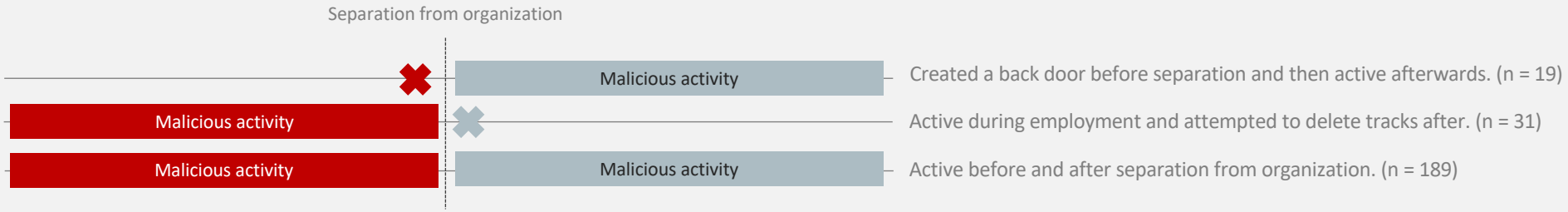
The majority of insiders who were active in pre- and post-separation, voluntarily resigned from their organizations.

black hat BRIEFINGS

timing of malicious activity



Malicious insiders who were active both during and after employment, typically fell into one of three scenarios.

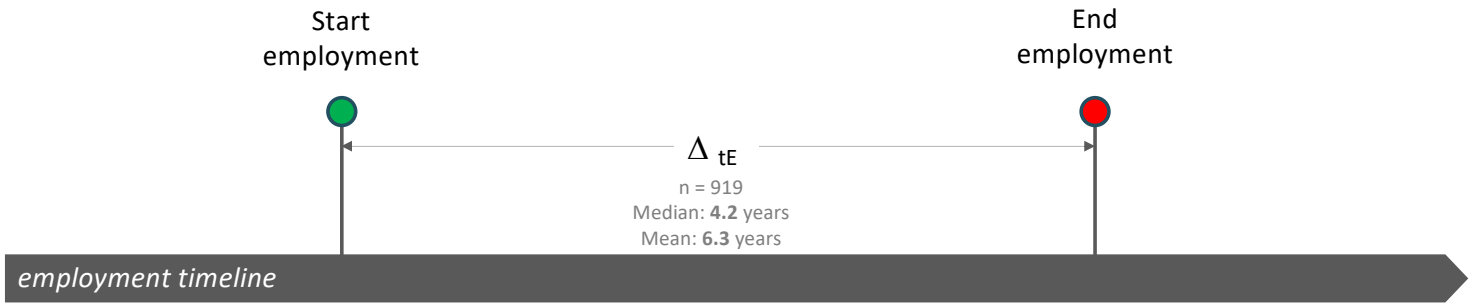


How long after employment started did an insider start acting malicious?

start of malicious activity

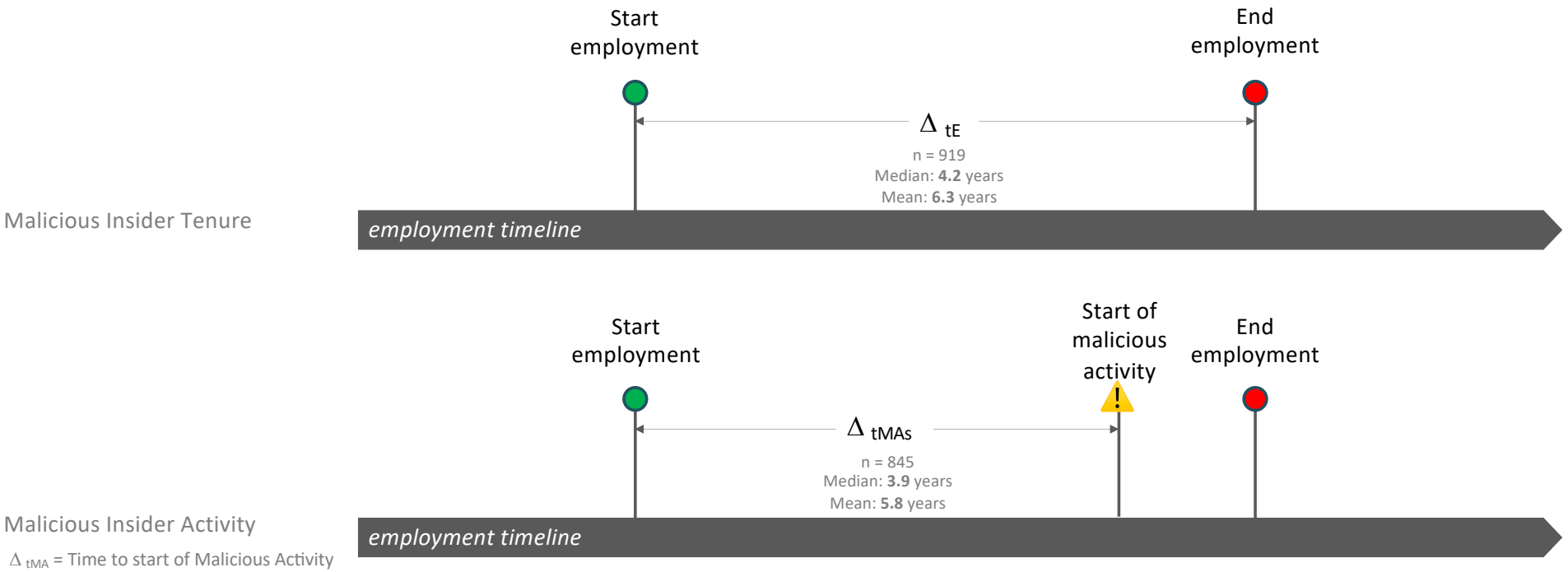
919 of the 1,002 cases contained details regarding the employment tenure of the malicious insider.
845 of the 1,002 cases contained details of when malicious insider threat activity started with respect to start of employment.

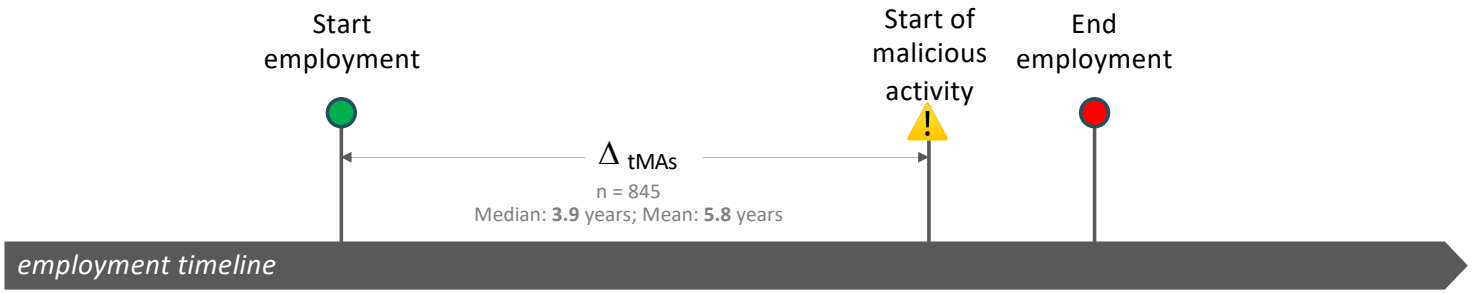
Malicious Insider Tenure

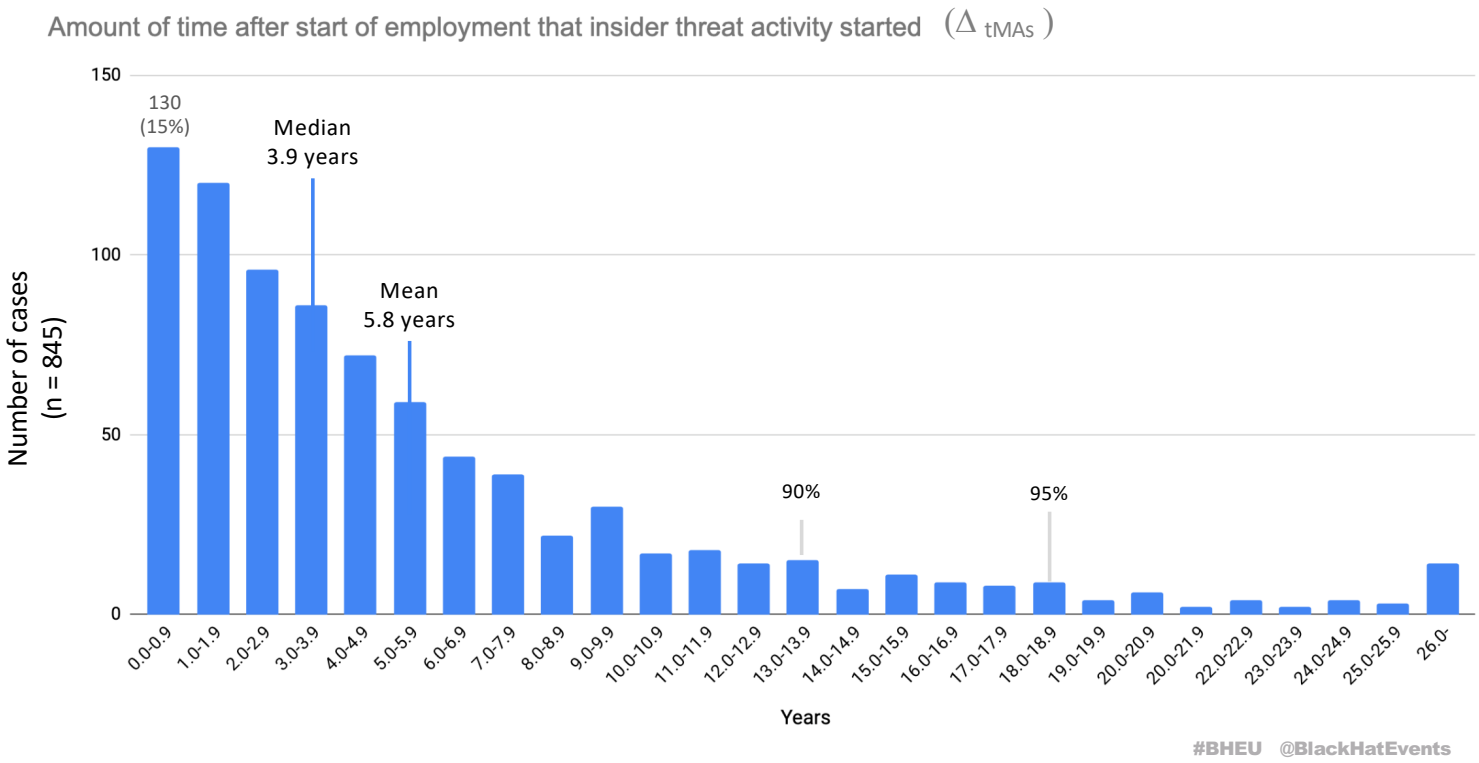


start of malicious activity

919 of the 1,002 cases contained details regarding the employment tenure of the malicious insider.
845 of the 1,002 cases contained details of when malicious insider threat activity started with respect to start of employment.

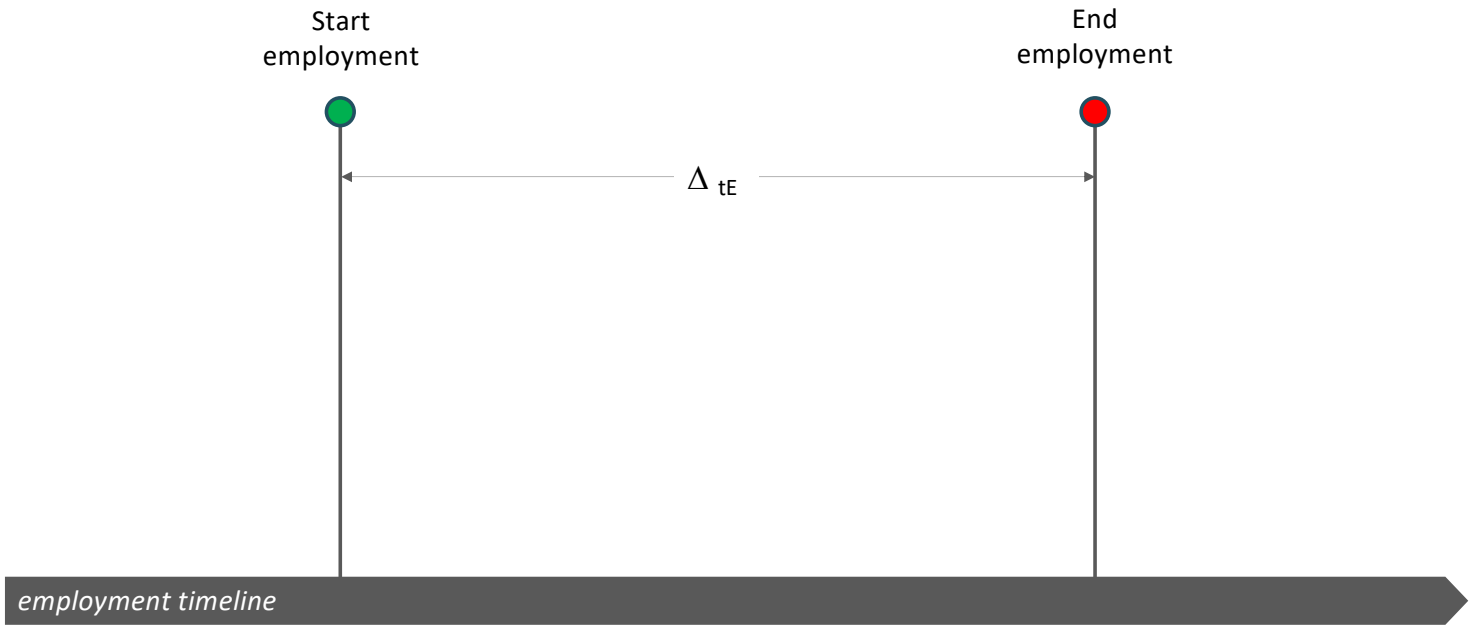



Start employment
Start of malicious activity
End employment
Δ tMAs
n = 845
Median: 3.9 years; Mean: 5.8 years
employment timeline


Amount of time after start of employment that insider threat activity started (Δ tMAs)
Number of cases (n = 845)
150
100
50
0
130 (15%)
Median 3.9 years
Mean 5.8 years
90%
95%
0.0-0.9
1.0-1.9
2.0-2.9
3.0-3.9
4.0-4.9
5.0-5.9
6.0-6.9
7.0-7.9
8.0-8.9
9.0-9.9
10.0-10.9
11.0-11.9
12.0-12.9
13.0-13.9
14.0-14.9
15.0-15.9
16.0-16.9
17.0-17.9
18.0-18.9
19.0-19.9
20.0-20.9
20.0-21.9
22.0-22.9
23.0-23.9
24.0-24.9
25.0-25.9
26.0-
Years

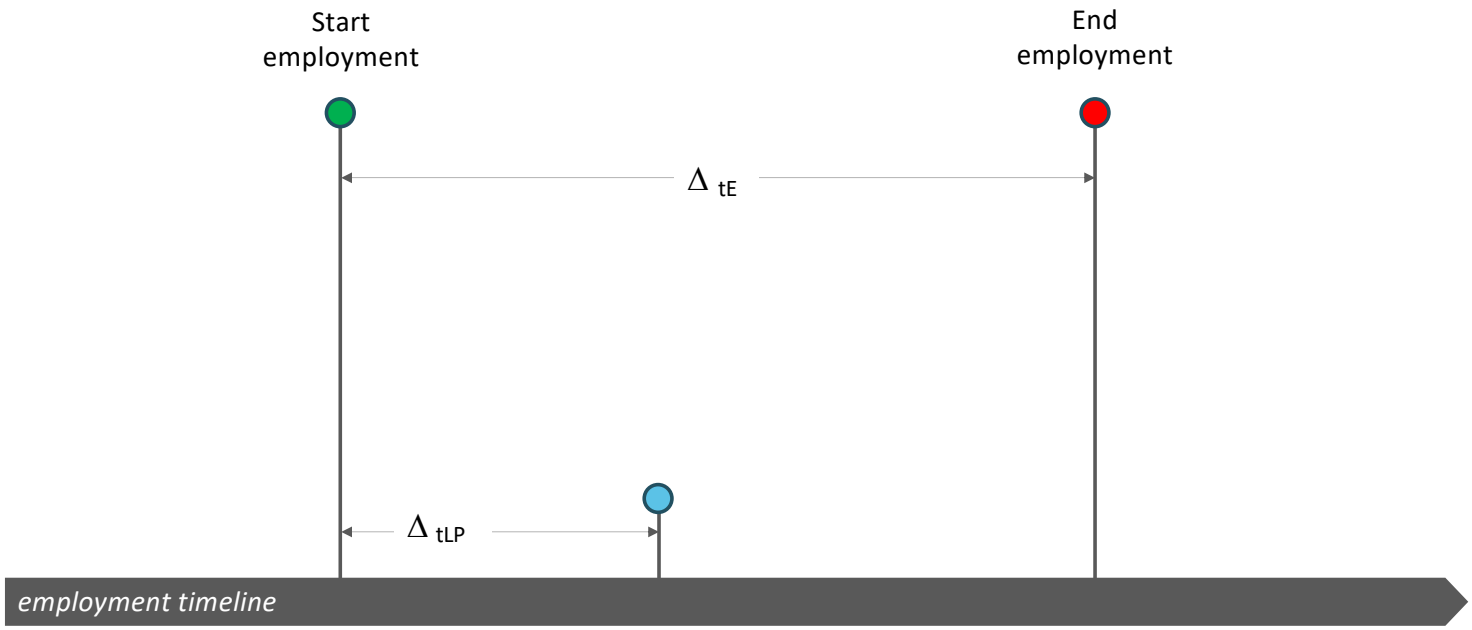
start of malicious activity

Standard Employee



start of malicious activity

Standard Employee

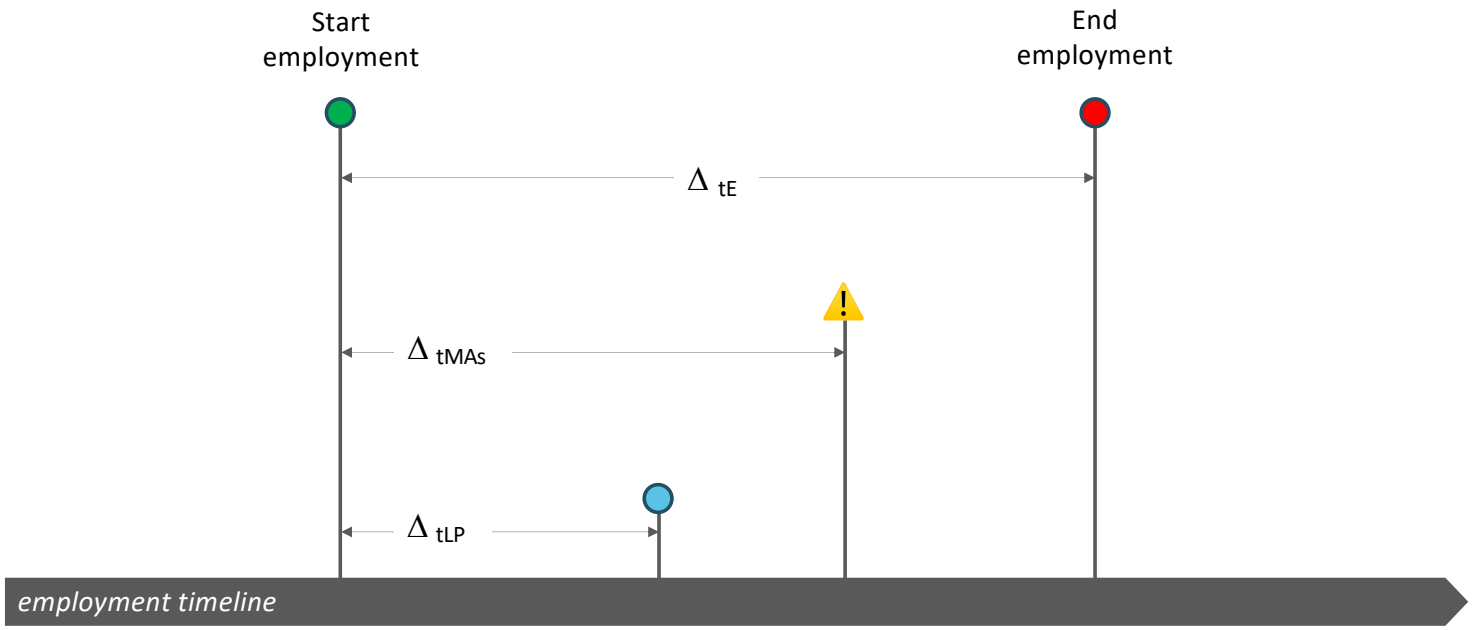


Learning Period (LP) for Machine Learning Detection Tools

Δ_{tLP} = Time of Learning Period

start of malicious activity

Malicious Insider



Learning Period (LP) for Machine Learning Detection Tools

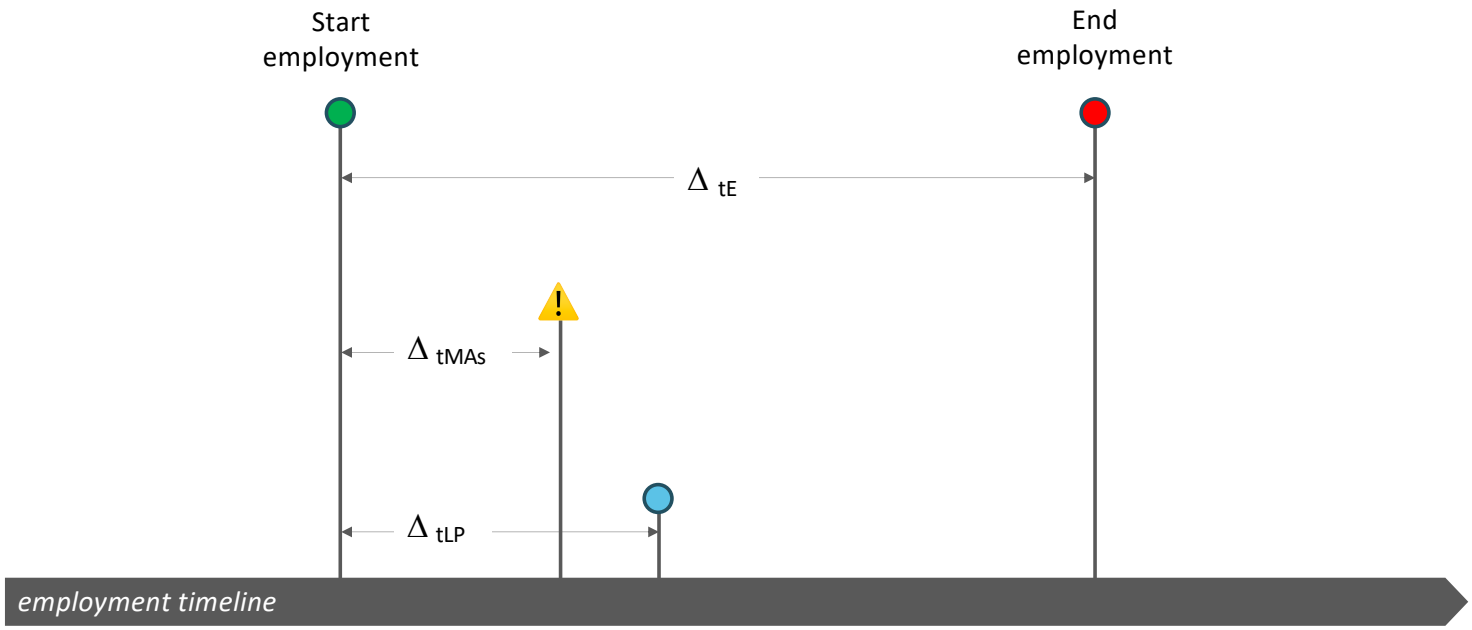
Ideally, malicious activity would occur after the learning period completes.

start of malicious activity

Malicious Insider

Learning Period (LP)
for Machine Learning
Detection Tools

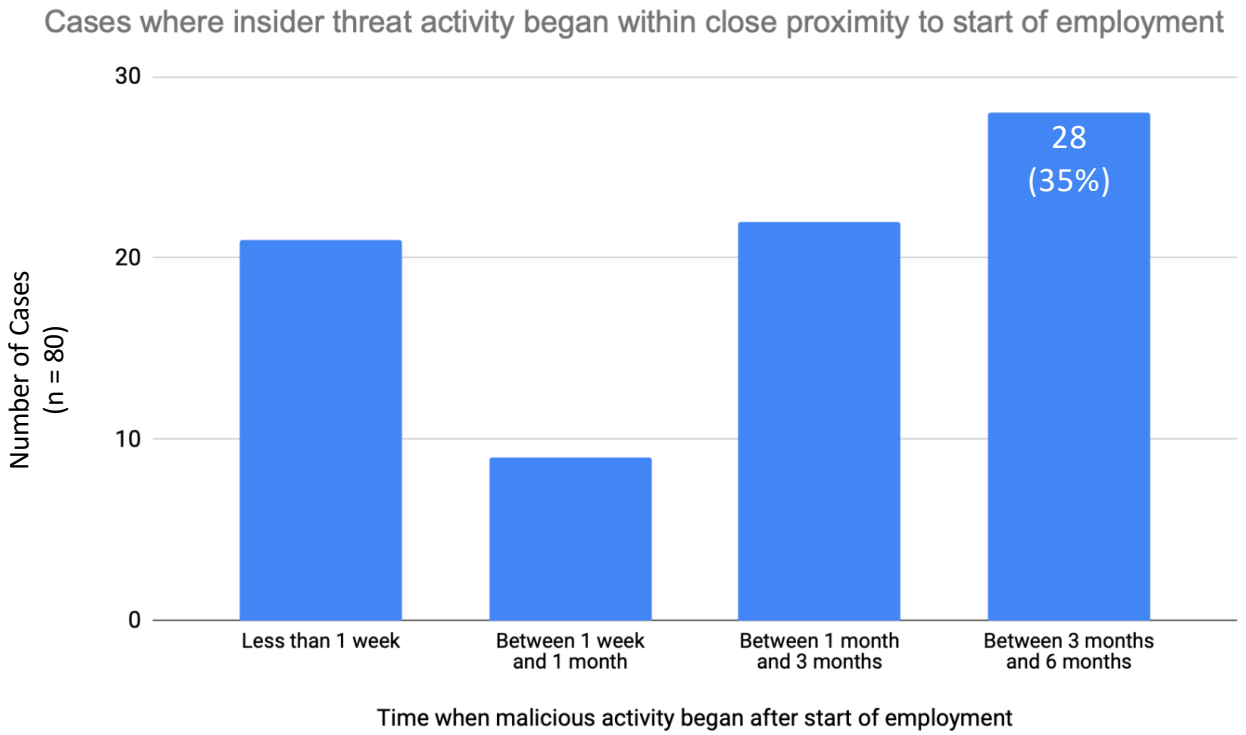
When malicious activity occurs within LP, there is a potential problem.



start of malicious activity

845 of the 1,002 cases contained details of when malicious insider threat activity started with respect to start of employment.
80 cases had malicious activity begin with 180 days after the start of employment.

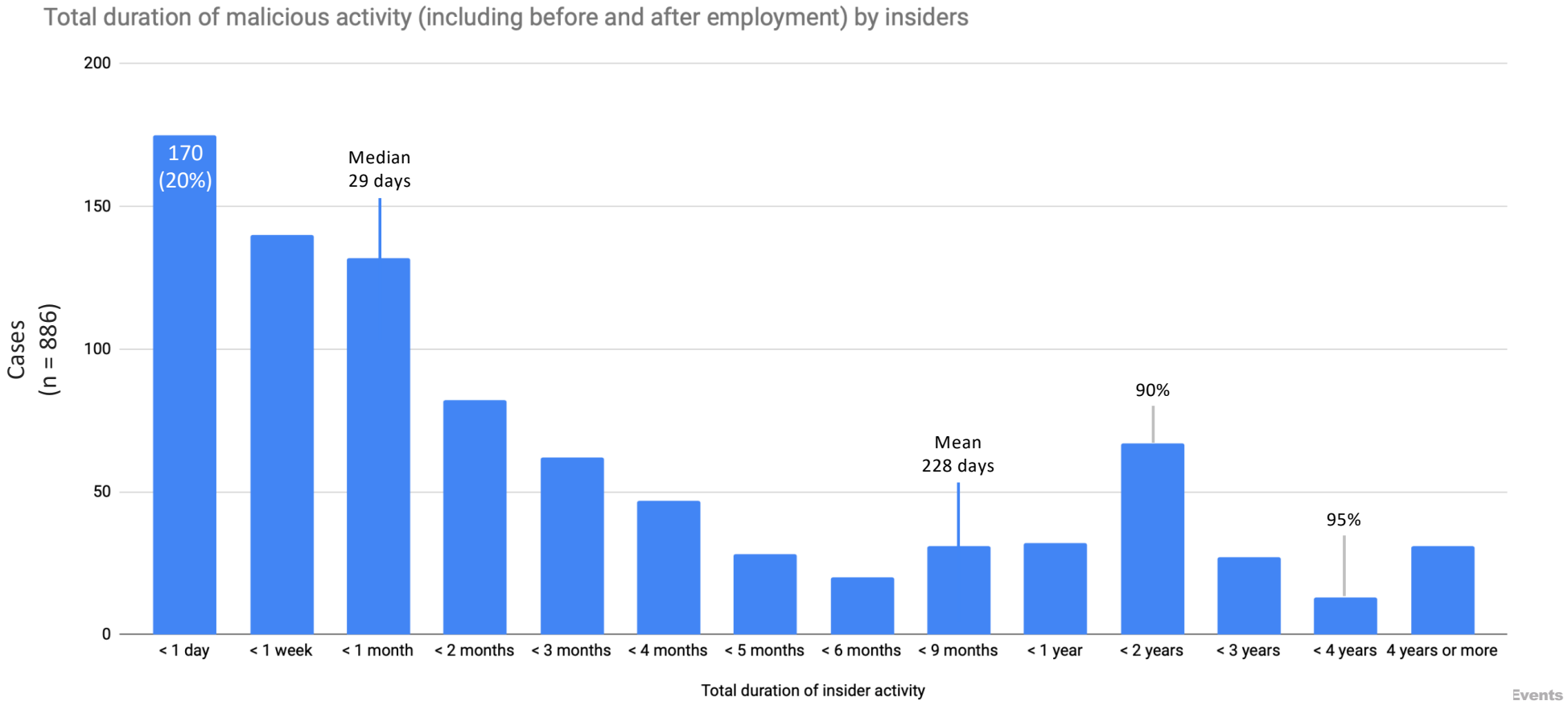
Take away: These insiders will likely not be detected by tools that are still learning "normal behavior." This limits the effectiveness of synthetic datasets.



What was the average duration of malicious activity by an insider?

duration of malicious activity

886 of 1,002 cases contained quantifiable information about the duration of the activity.



combination of attributes

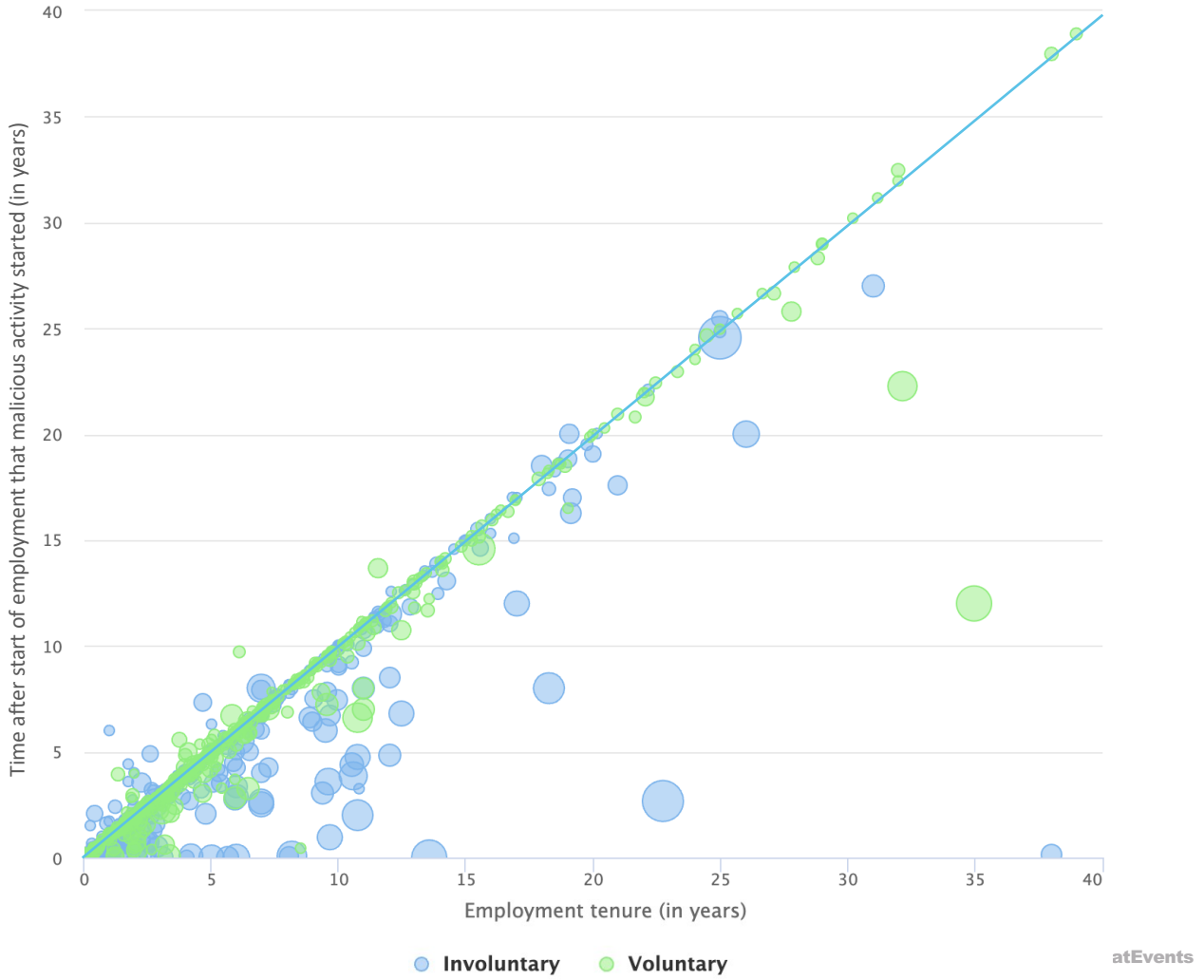
799 of 1,002 cases contained quantifiable data with respect to tenure, start of activity, and duration of activity.

Most insider threat activity occurs within proximity of separation from the organization, which is depicted by the blue diagonal line with a slope of 1.

Most activity occurs within the first six years of employment.

Note:

Size of bubbles indicate duration of malicious activity.



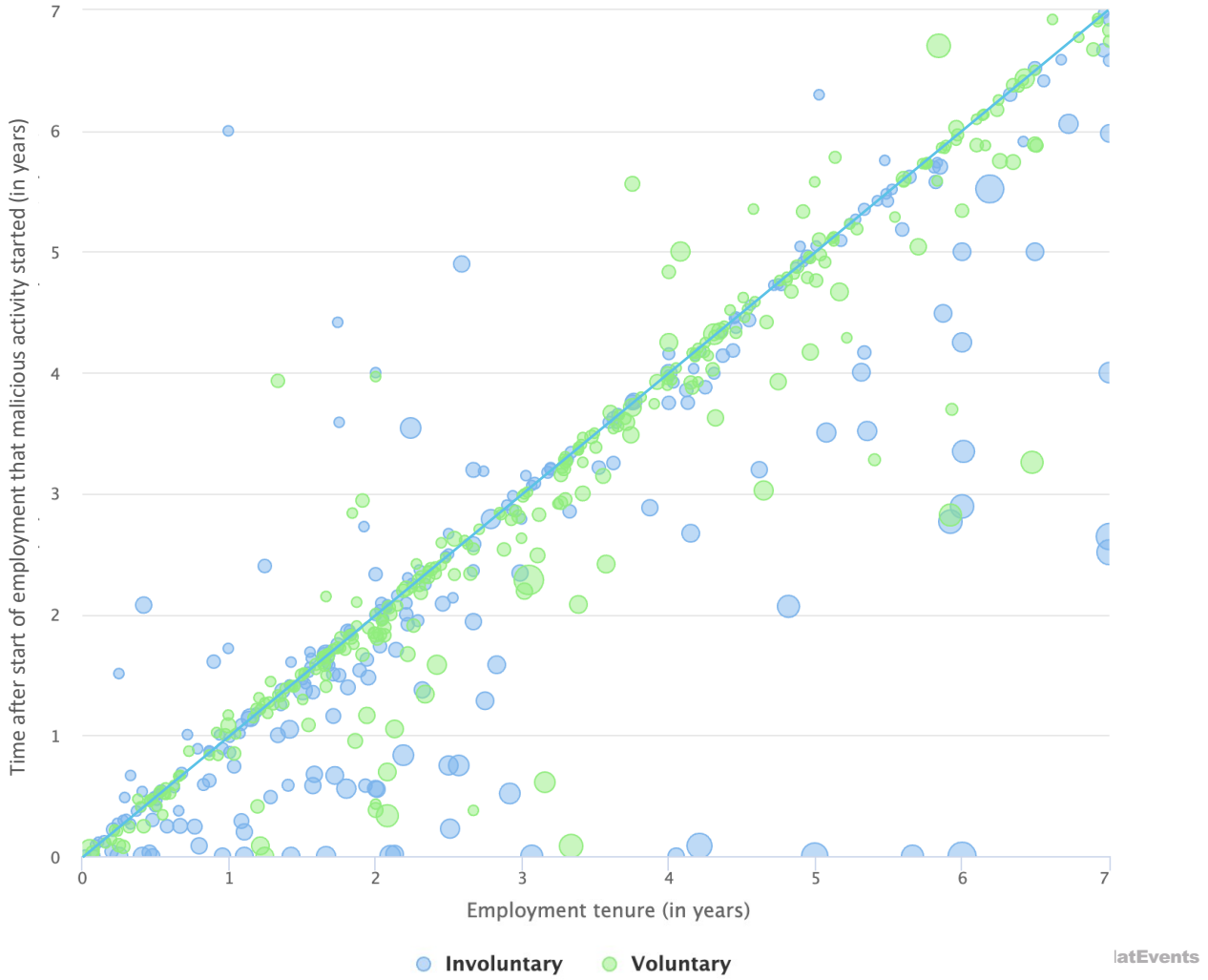
combination of attributes

799 of 1,002 cases contained quantifiable data with respect to tenure, start of activity, and duration of activity.

Notes:

Graph focuses on $\Delta_{tE} < 7$.

Size of bubbles indicate duration of malicious activity.



combination of attributes

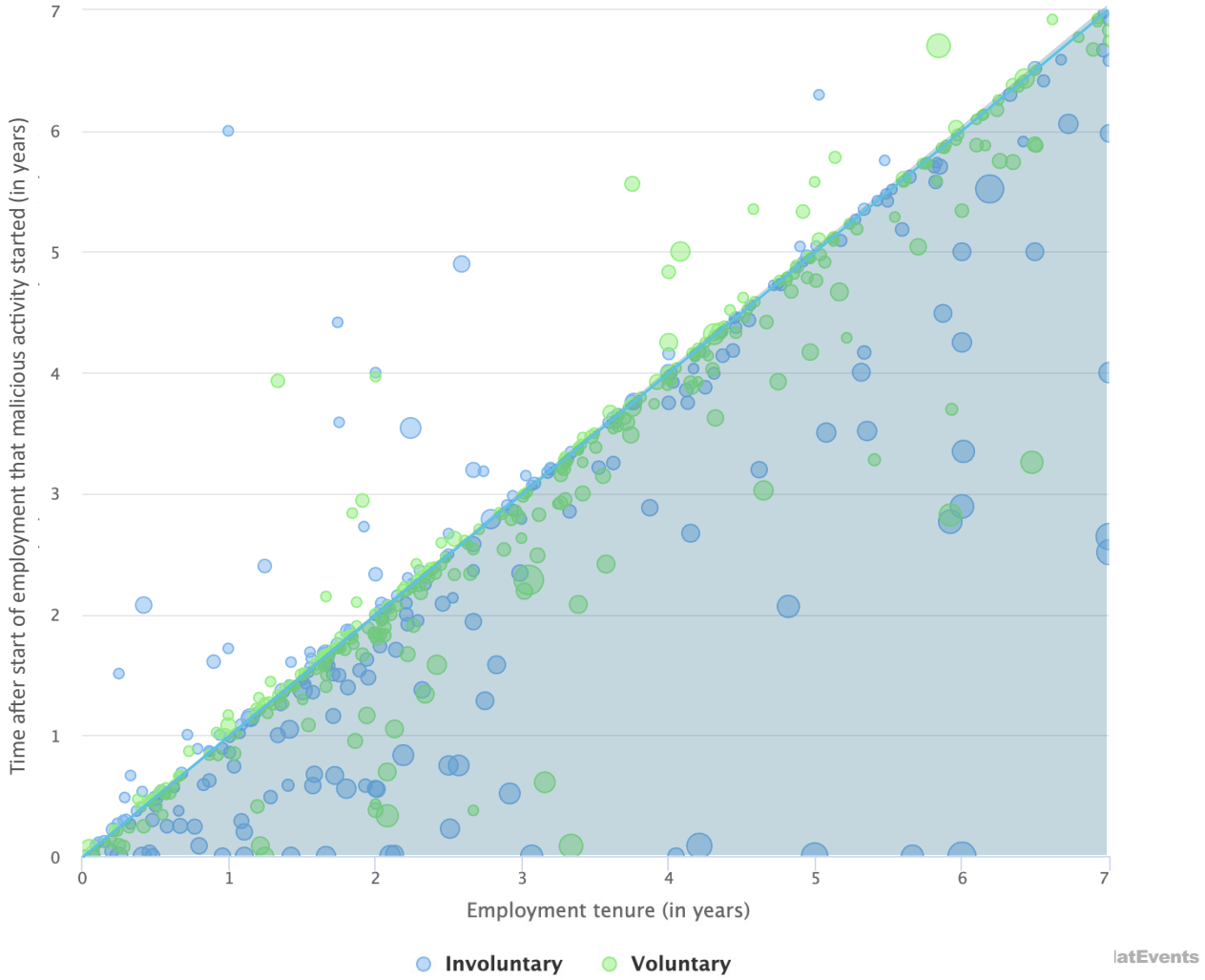
799 of 1,002 cases contained quantifiable data with respect to tenure, start of activity, and duration of activity.

Notes:

Graph focuses on $\Delta_{tE} < 7$.

Size of bubbles indicate duration of malicious activity.

Shaded area is time during employment.



combination of attributes

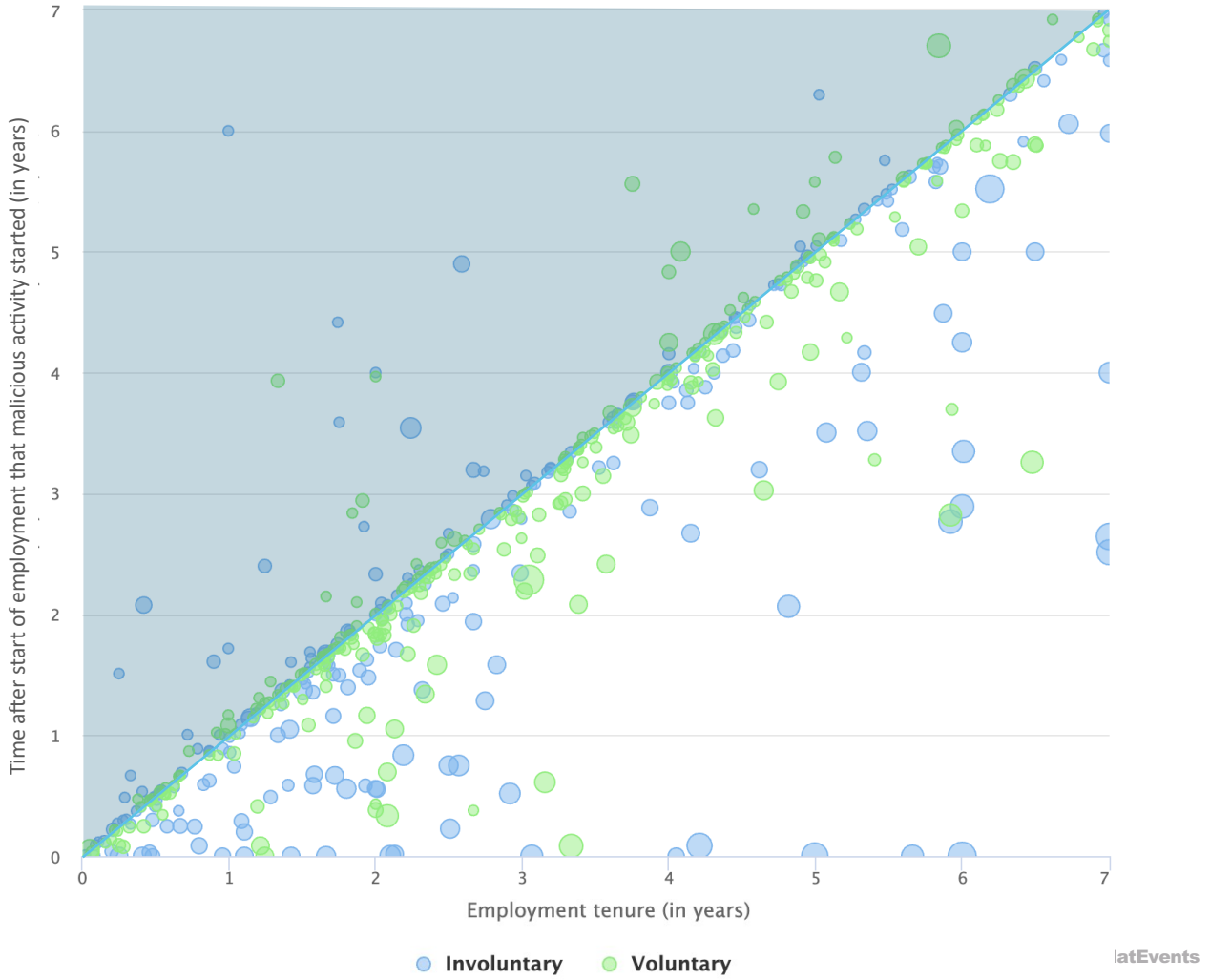
799 of 1,002 cases contained quantifiable data with respect to tenure, start of activity, and duration of activity.

Notes:

Graph focuses on $\Delta_{tE} < 7$.

Size of bubbles indicate duration of malicious activity.

Shaded area is time after employment.



combination of attributes

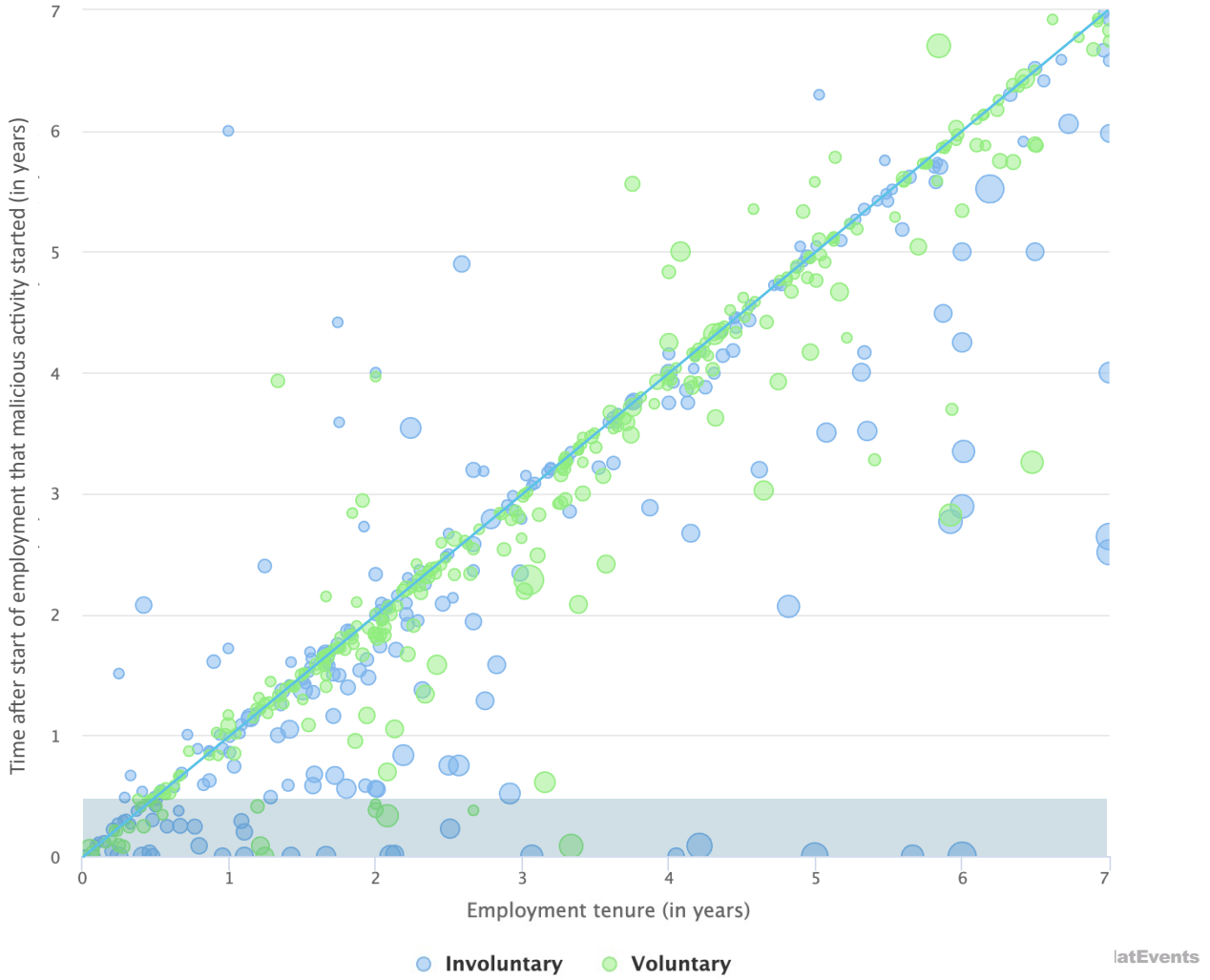
799 of 1,002 cases contained quantifiable data with respect to tenure, start of activity, and duration of activity.

Notes:

Graph focuses on $\Delta_{tE} < 7$.

Size of bubbles indicate duration of malicious activity.

Shaded area is first six months after start of employment.



combination of attributes

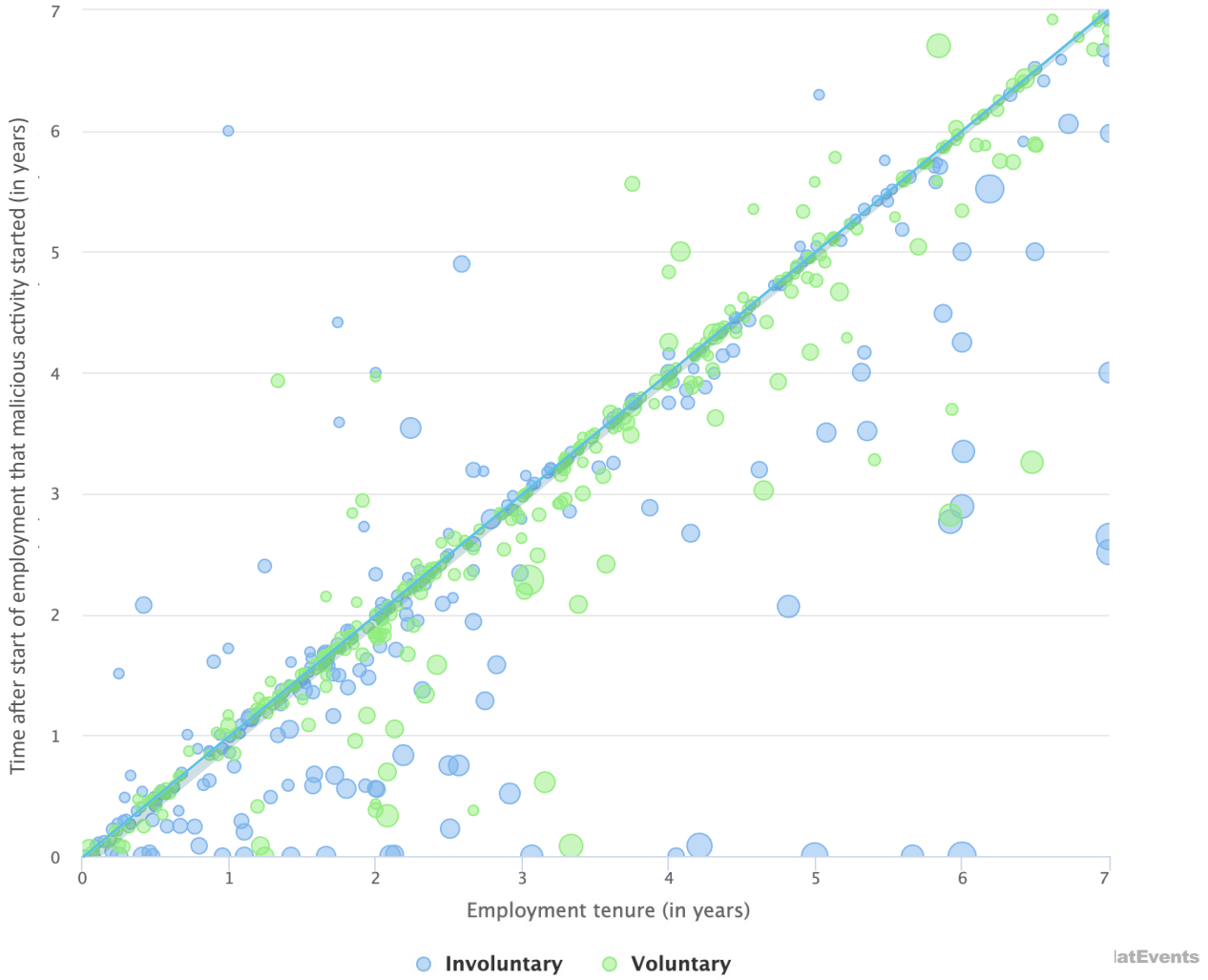
799 of 1,002 cases contained quantifiable data with respect to tenure, start of activity, and duration of activity.

Notes:

Graph focuses on $\Delta_{tE} < 7$.

Size of bubbles indicate duration of malicious activity.

Shaded area is approximately two weeks prior to separation.



combination of attributes

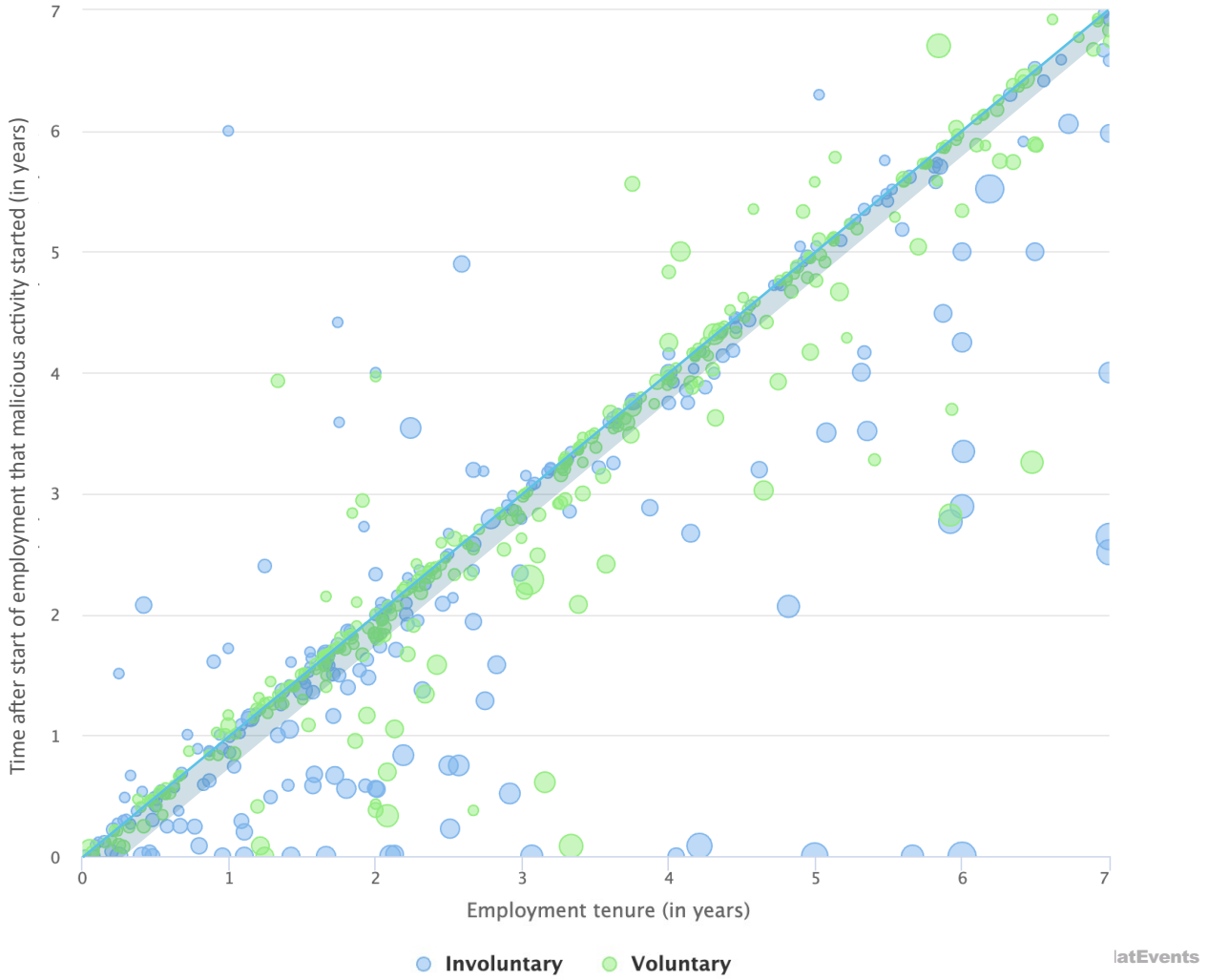
799 of 1,002 cases contained quantifiable data with respect to tenure, start of activity, and duration of activity.

Notes:

Graph focuses on $\Delta_{tE} < 7$.

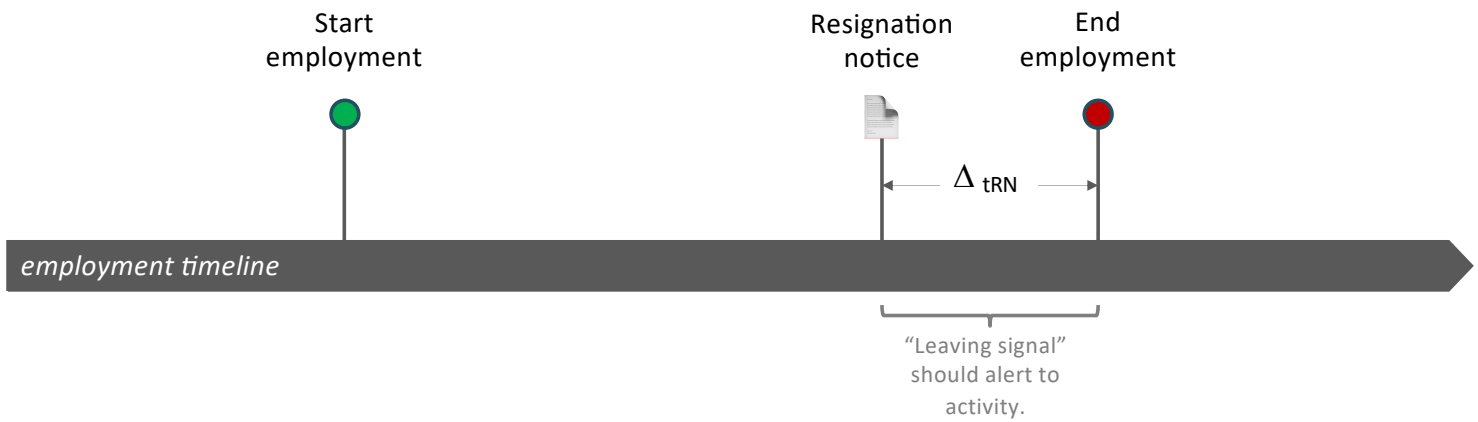
Size of bubbles indicate duration of malicious activity.

Shaded area is approximately three months prior to separation.



Insider resignations

resignation notices



Employee typically resigns

Δ_{tRN} = Time after Resignation Notice

Many companies, e.g., AWS, Booz Allen, Cisco, IBM, parts of the U.S. government, and others that enable enhanced monitoring once the "leaving signal" is triggered to detect malicious activity.

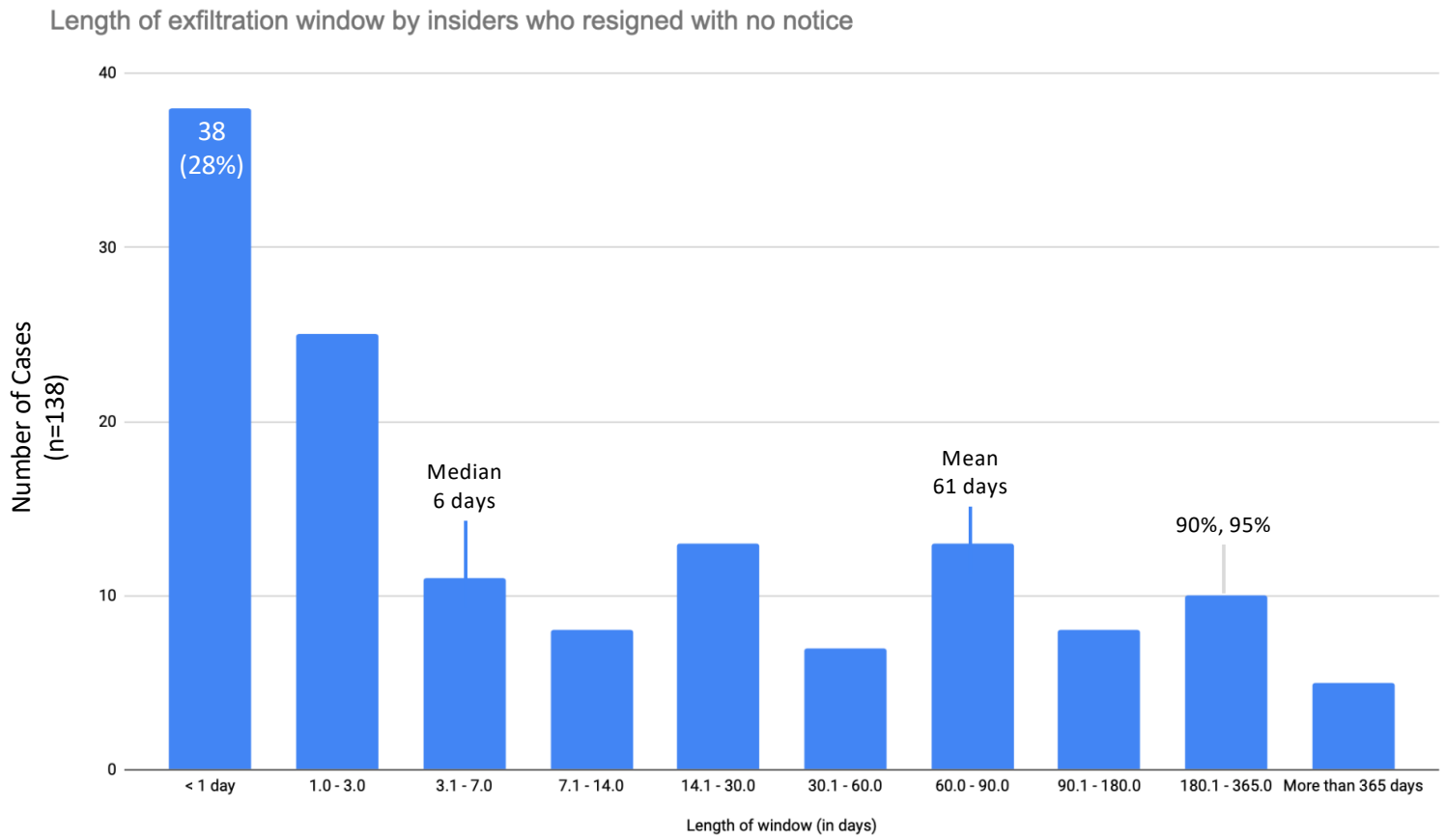
resignation notices

Malicious insider resigns

Of the 507 malicious insiders who voluntarily separated from their organizations 147 gave no notice, i.e., $\Delta_{tRN} = 0$.

Take away: There is no data from the leaving signal for forensic examiners to use in investigations.

Of the 507 cases where there was voluntary separation, 147 cases had insiders resign with no notice, i.e., $\Delta_{tRN} = 0$.



resignation notices

Of the 507 cases where there was voluntary separation, 147 cases had insiders resign with no notice, i.e., $\Delta_{tRN} = 0$.
122 of the 147 insiders exfiltrated data from company before leaving.

Most common exfiltration pathways for those who resigned with no notice

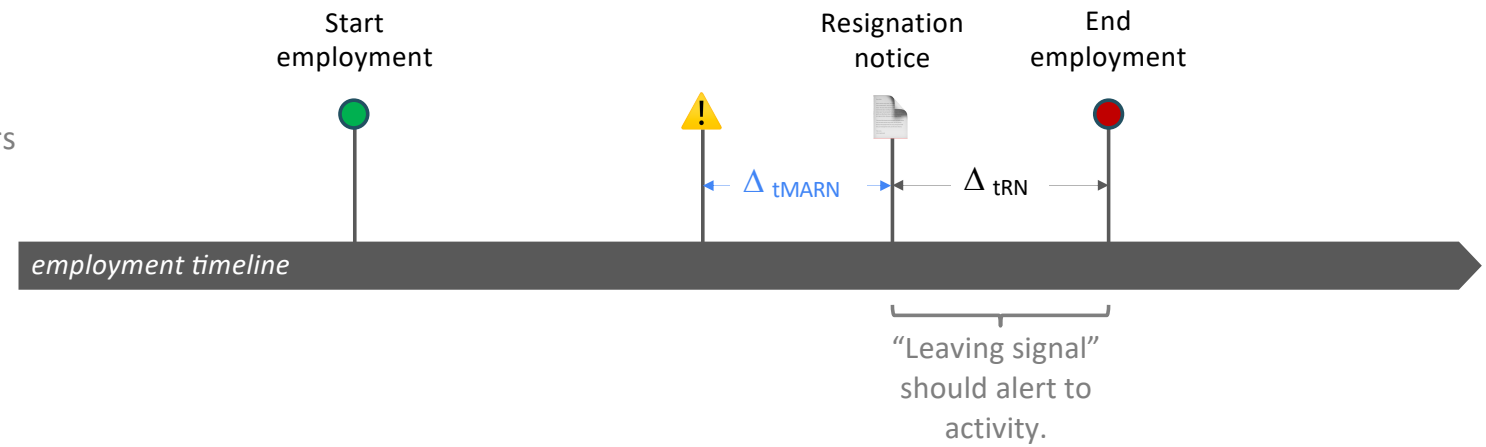
Exfiltration Pathway	Count
Email	68
External storage device	48
Multiple external storage devices	25
Cloud	22
Web apps	21
Used multiple exfiltration pathways	50

How long before a separation signal did malicious activity begin?

resignation notices

Malicious insider resigns and malicious activity occurs before resignation

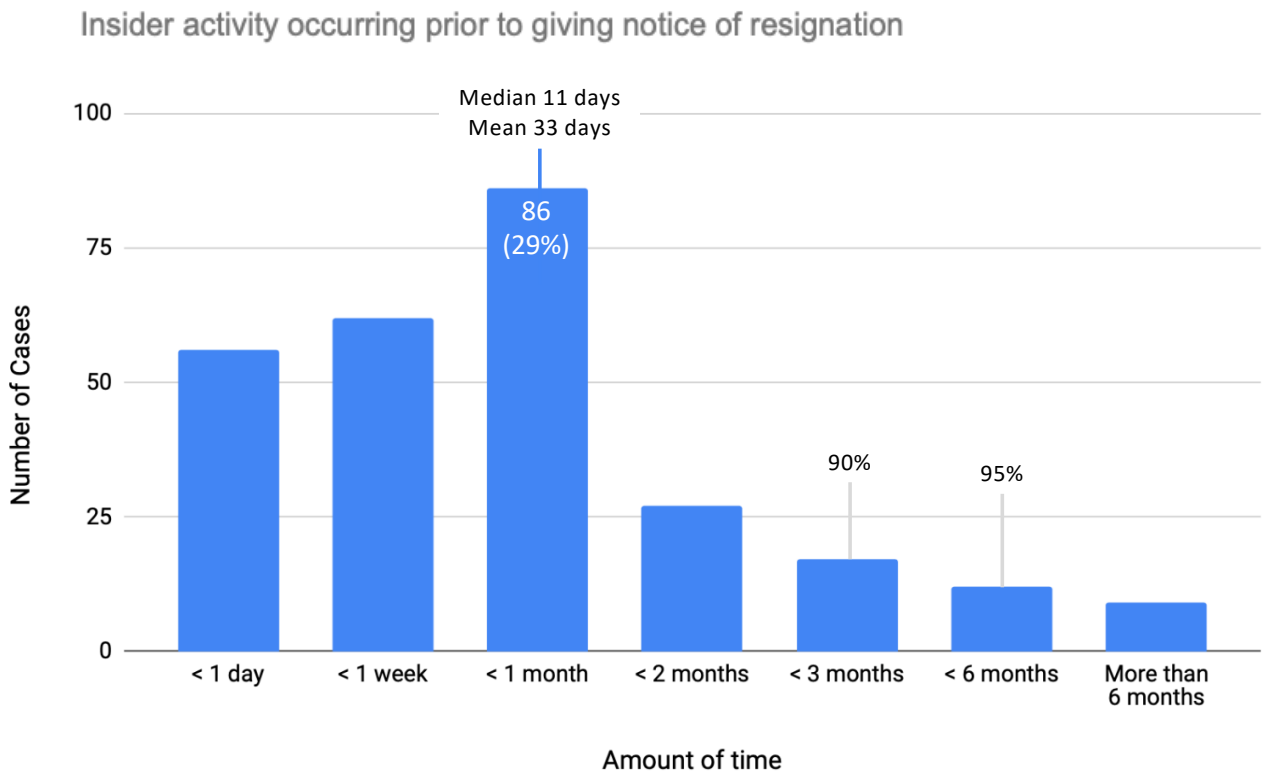
Δ_{tMARN} = Time of Malicious Activity before Resignation Notice



resignation notices

Of the 507 who voluntarily separated from their organizations, 325 engaged in malicious activity prior to submitting the resignation notice, i.e., Δ_{tMARN}, e.g., after they had a job offer at another firm or after having established a competing firm.

274 cases had quantifiable data pertaining to Δ_{tMARN}.



Malicious activity after employment

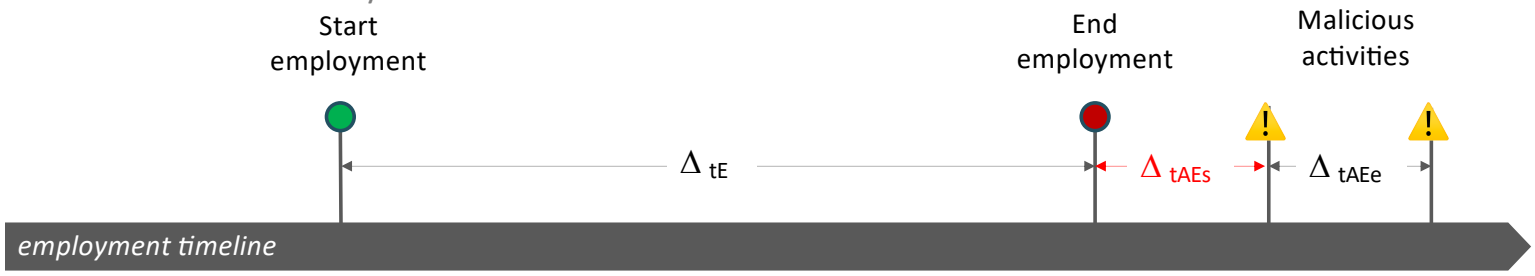
Insider threat does not always occur inside employment.
It frequently occurs after employment with inside knowledge.

How long after separating from an organization did a malicious insider engage?

post-separation activity

411 of 1,002 cases involved malicious activity after the insider separated from the organization.
363 cases where the start time of malicious activity was documented.

Insider threat activity occurring after employment ends

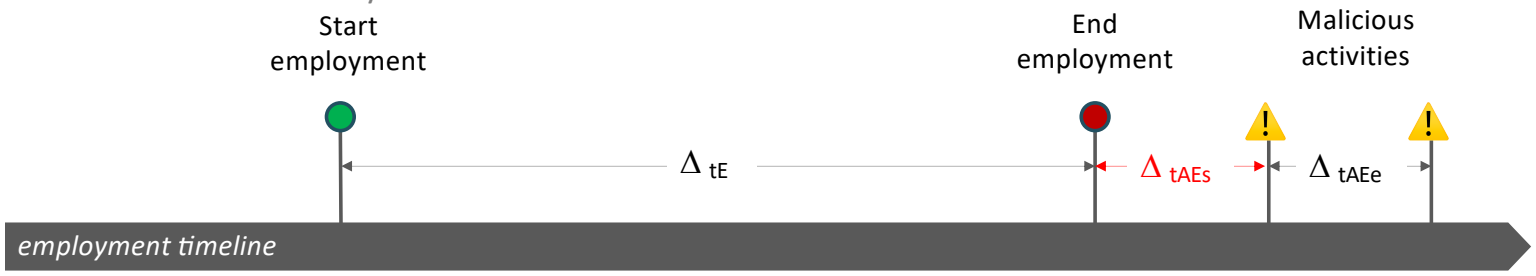


Δ_{tAEs} = Time between end of employment and start of malicious activity
Δ_{tAEe} = Time between start and end of malicious activity after employment

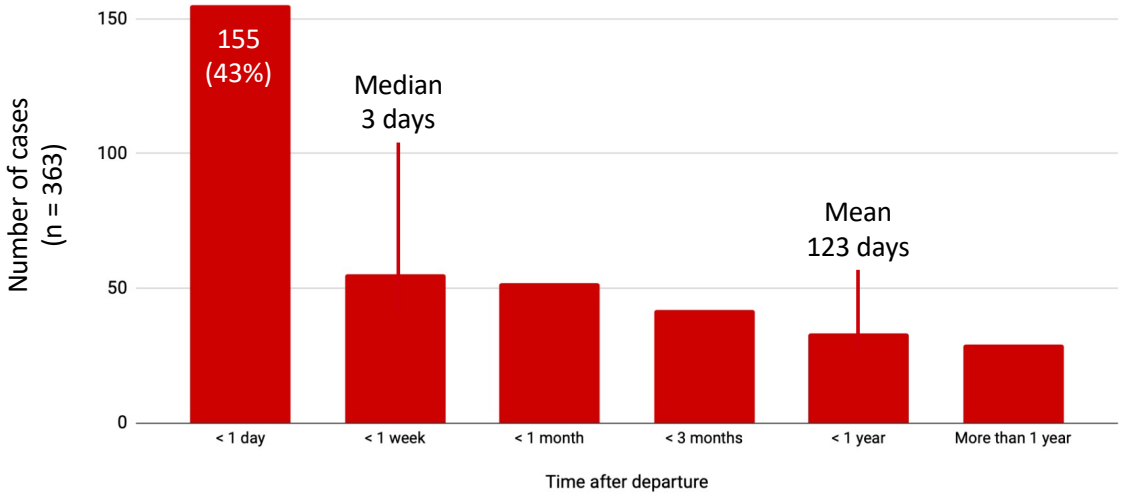
post-separation activity

411 of 1,002 cases involved malicious activity after the insider separated from the organization.
363 cases where the start time of malicious activity was documented.

Insider threat activity occurring after employment ends



Amount of time after separation that insider re-engaged organization (Δ tAEs)

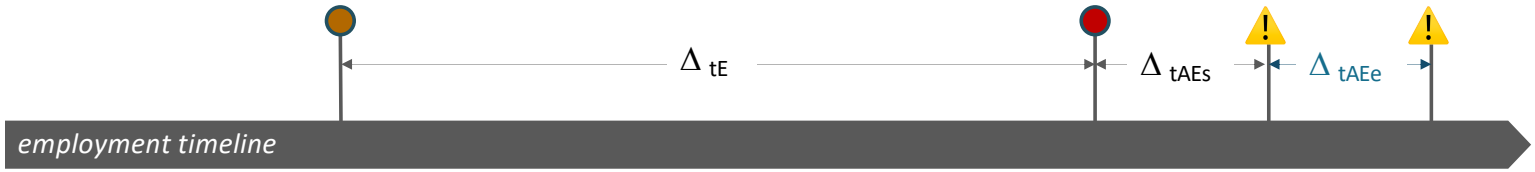


What was the duration of malicious activity after the insider separated?

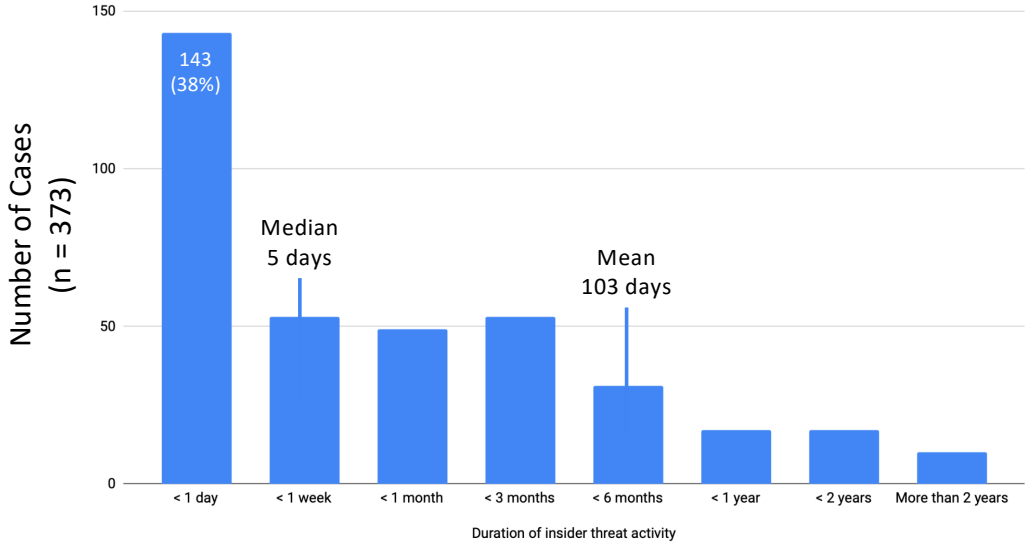
post-separation activity

411 of 1,002 cases occurred where there was malicious activity after the insider separated from the organization.
373 cases where the duration of malicious activity was documented.

Insider threat activity occurring after employment ends



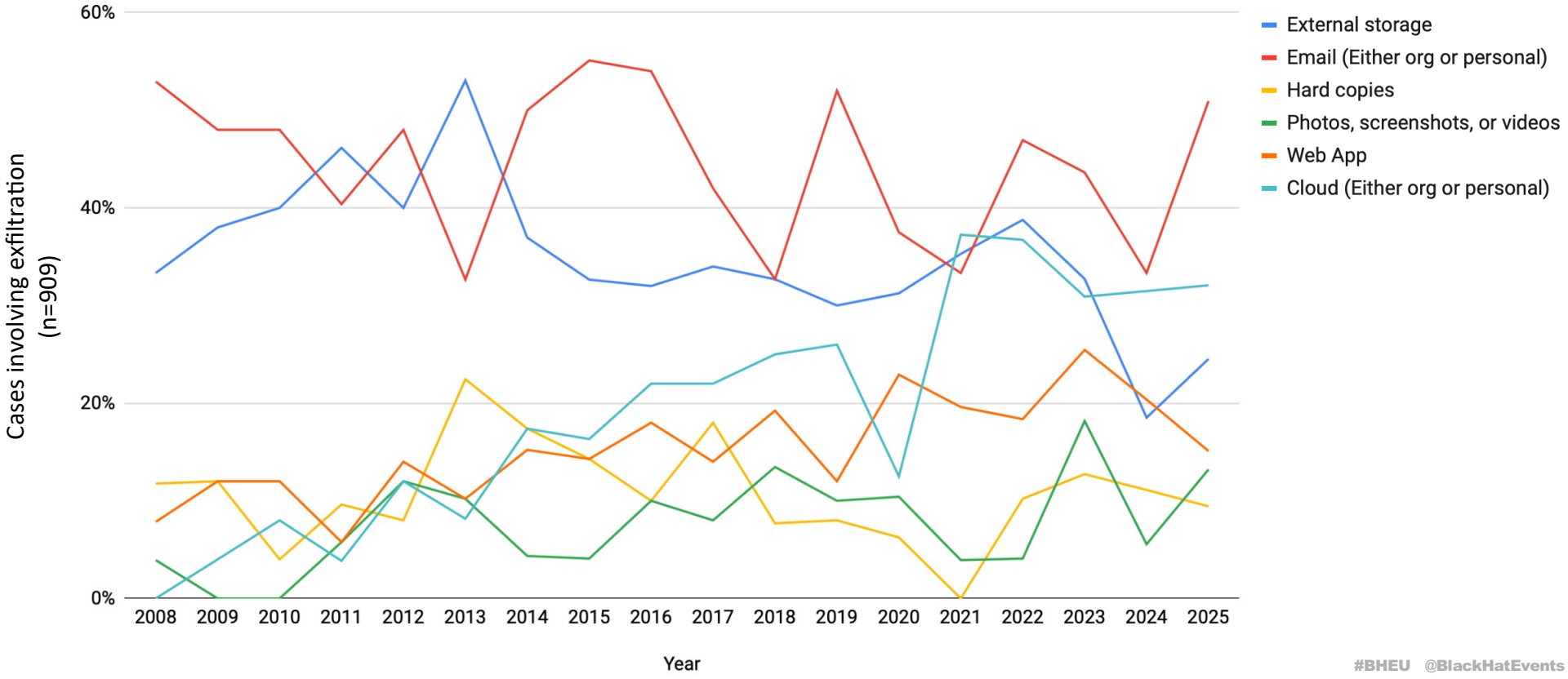
Length of insider threat activity after insider separated from organization (Δ_{tAEe})



Exfiltration

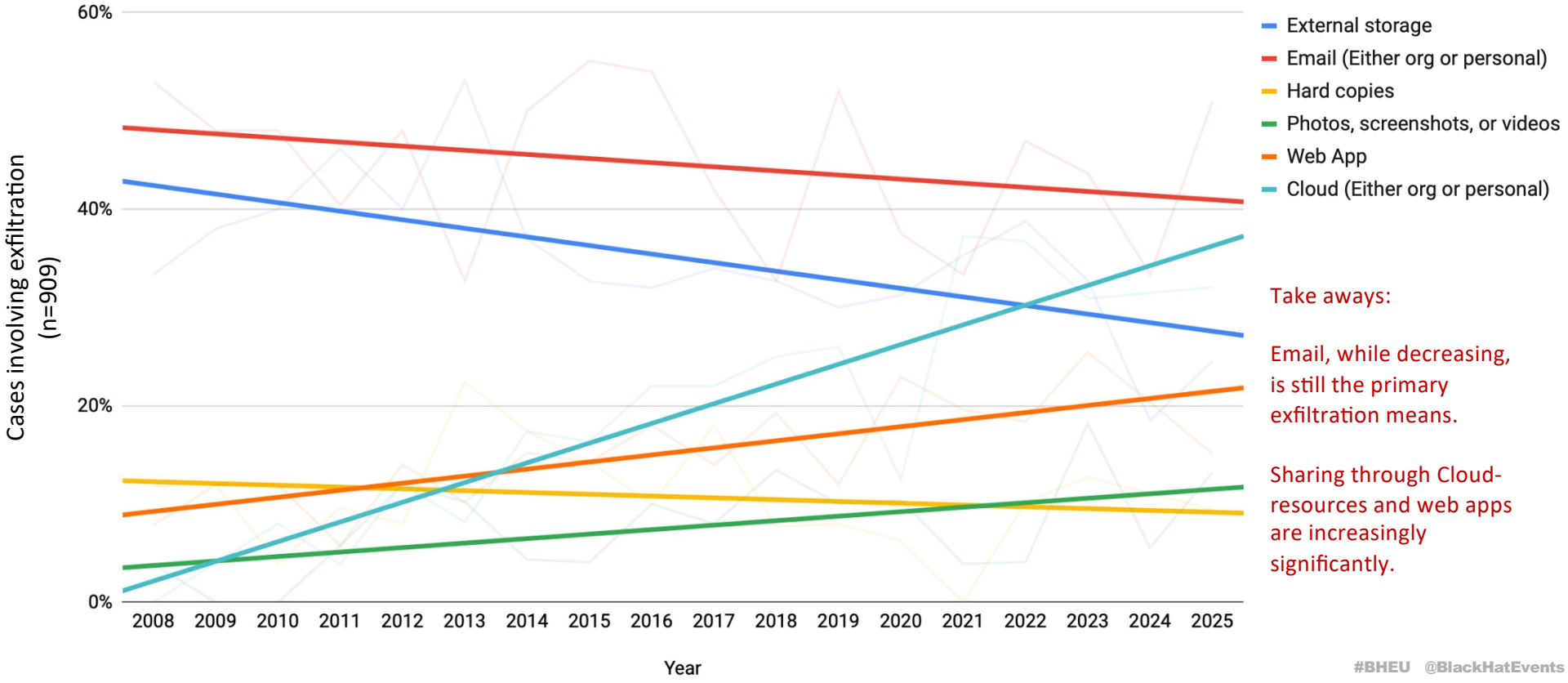
909 of 1,002 cases of insider threat activity involved data exfiltration.

Exfiltration cases with exfiltration pathways by percent



909 of 1,002 cases of insider threat activity involved data exfiltration.

Exfiltration cases with exfiltration pathways by percent



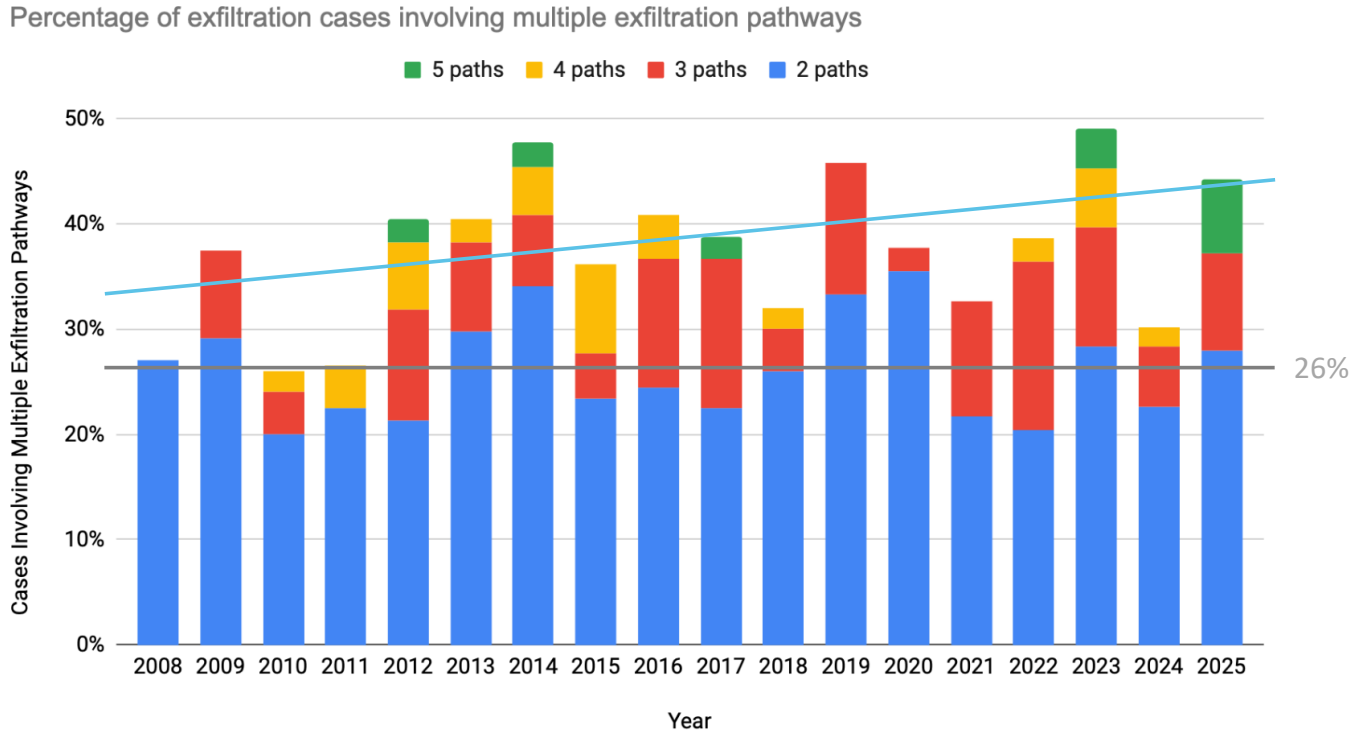
Take aways:

Email, while decreasing, is still the primary exfiltration means.

Sharing through Cloud-resources and web apps are increasingly significantly.

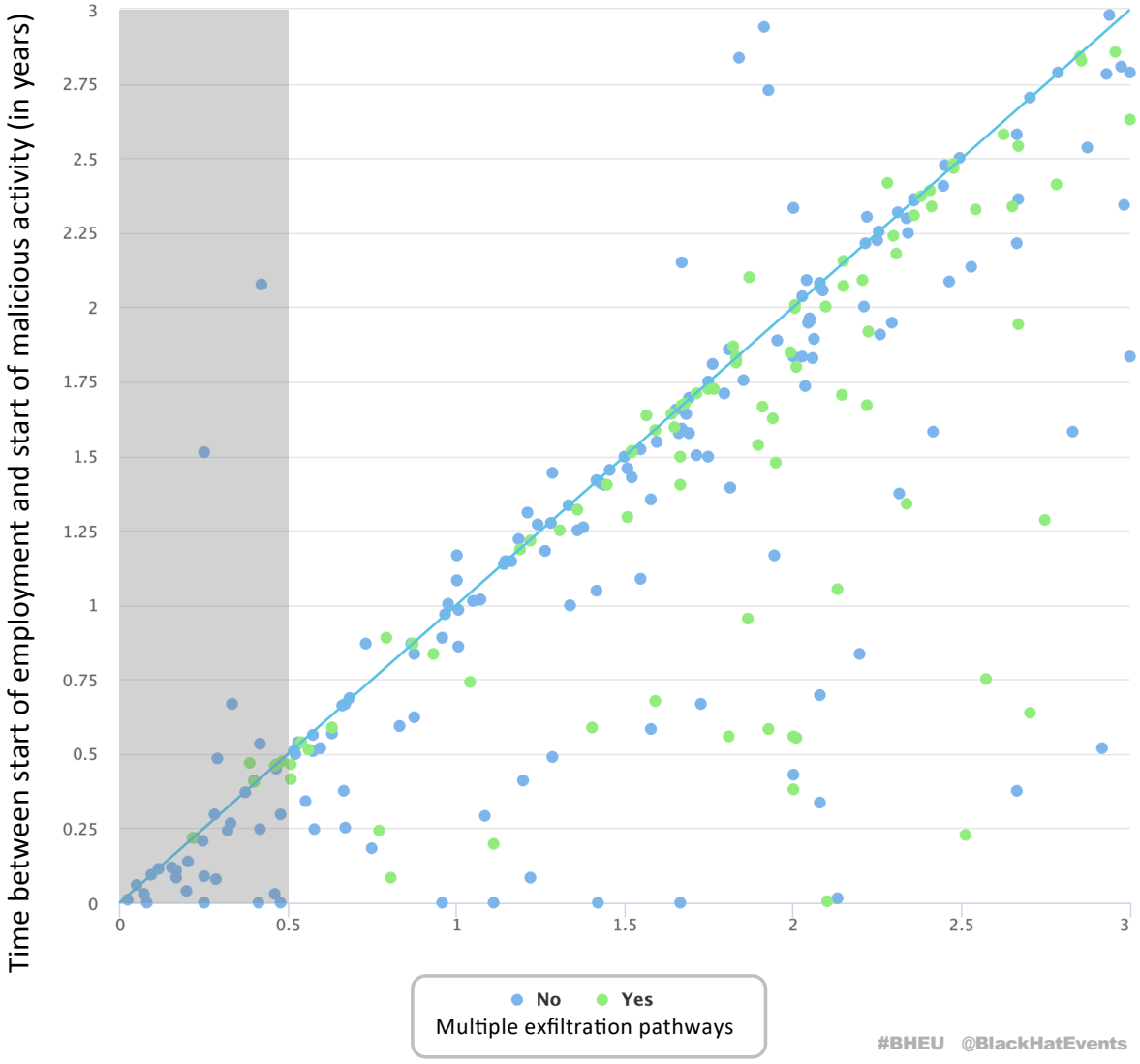
909 of 1,002 cases of insider threat activity involved data exfiltration.
320 cases of insider threat activity involved data exfiltration using multiple pathways.

Take away: The trend of using multiple exfiltration pathways by a single malicious insider is increasing.
This behavior is not mimicked in popular synthetic datasets.



909 of 1,002 cases of involved data exfiltration.

For new employees, whose tenure is six months or less, typically, only one exfiltration pathway is used.

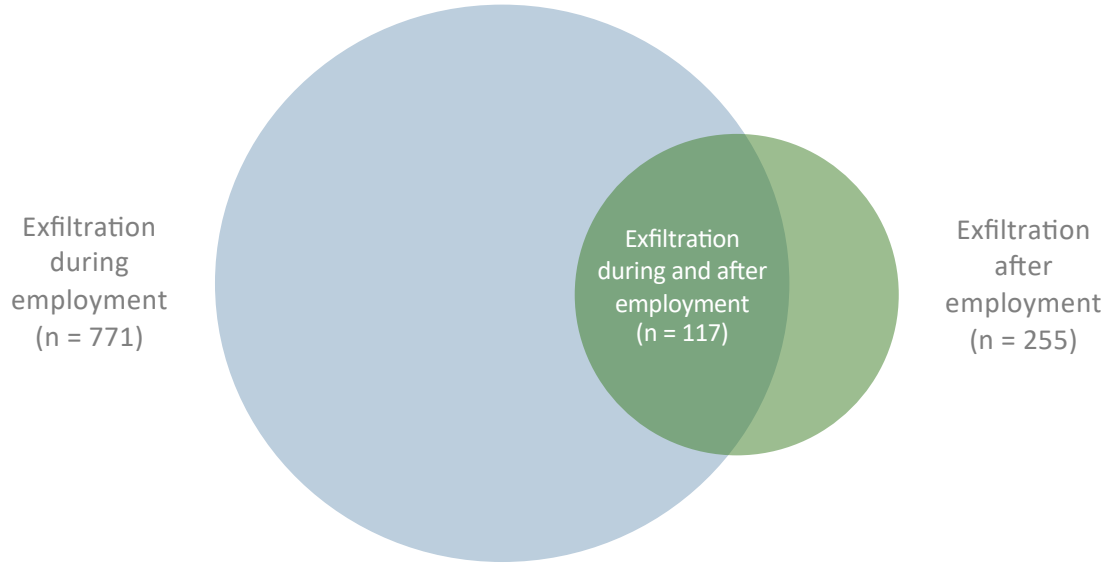


909 of 1,002 cases of insider threat activity involved data exfiltration.

Take aways:

Exfiltration occurred after employment ended in 28% of cases.

Using credentials of other employees, changing recovery account settings, adding mail-forwarding rules, and having laptops in possession of the insider after separation makes post-exfiltration possible.



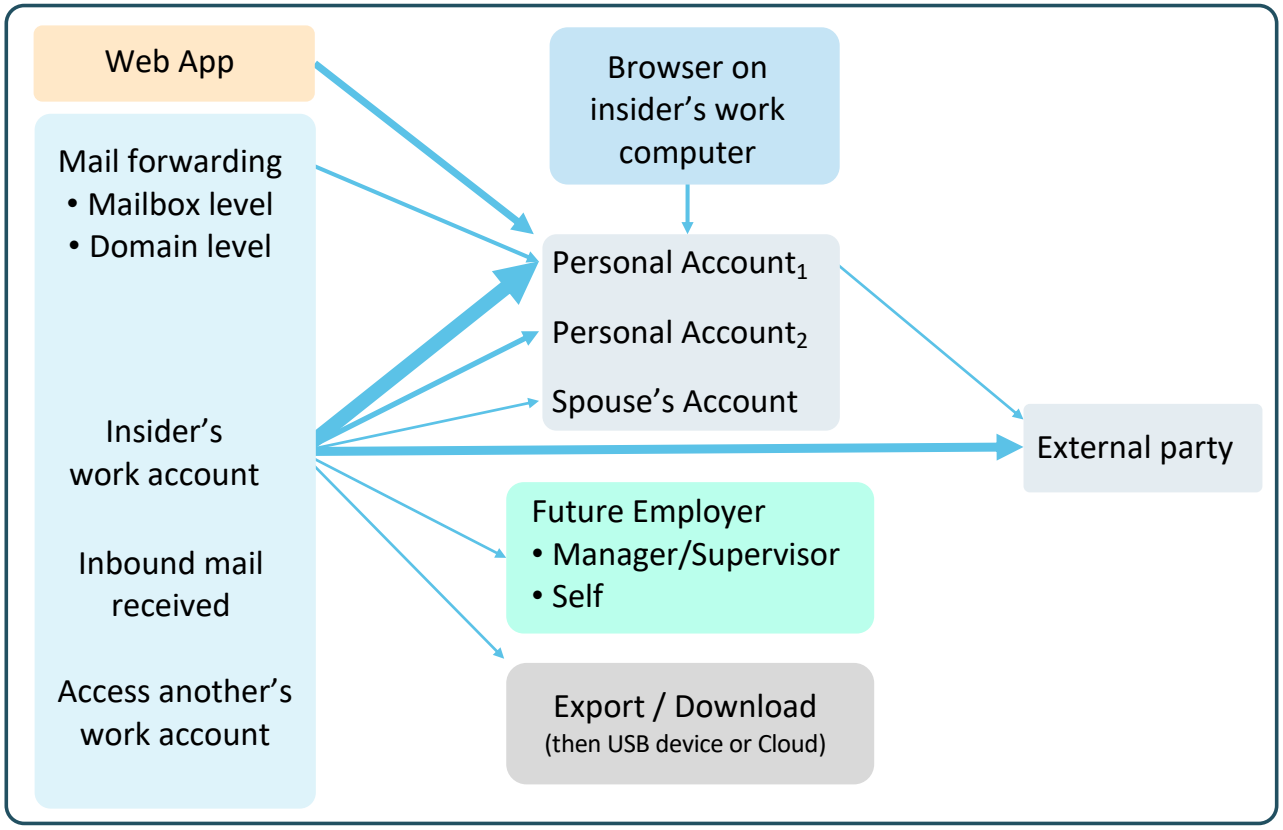
Top exfiltration techniques during employment:
- Email (307)
- External storage devices (269)
- Cloud (106)
- Hard copies (95)
- Smartphones (69)

Top exfiltration techniques during and after employment:
- Email (31)
- Corp web app (27)
- Cloud (21)
- External storage device (18)
- Smartphone (2)

Top exfiltration techniques after employment:
- Corp web app (69)
- Email (60)
- Cloud (40)
- External storage devices (28)
- Equipment theft (16)

Email was the most popular form of data exfiltration.

909 of 1,002 cases of insider threat activity involved data exfiltration.
398 involved exfiltration via email.



Take aways:

- Sources of evidence go beyond looking for sent mail, e.g., outbound and inbound mail, browser artifacts.
- Multiple recipients may be involved.
- Exported mail, accessing another's account, and mail from external web app may not be obvious.

exfiltration via email

909 of 1,002 cases of insider threat activity involved data exfiltration.
398 involved exfiltration via email.

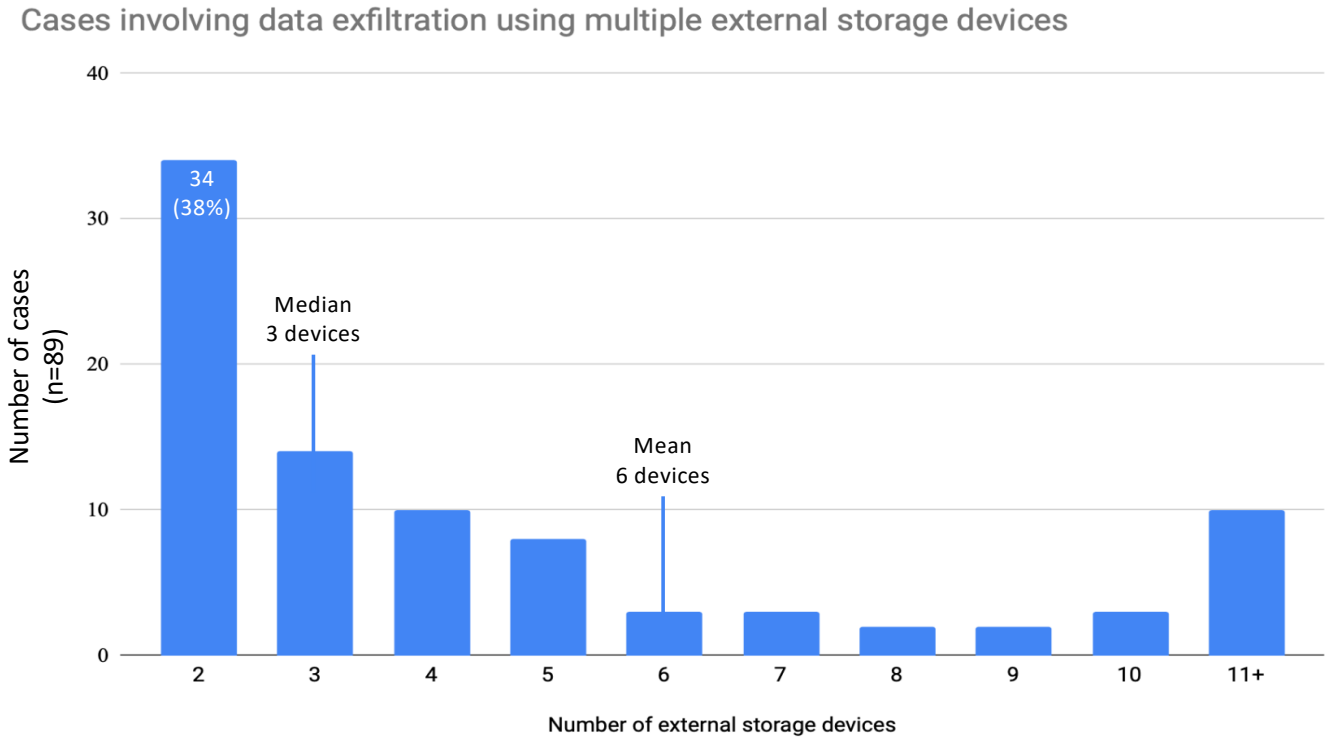
Take away: The most common exfiltration practice is sending material from a work account to one or more personally owned email accounts. External recipients have also included accounts for future employment, competitors, and spouses.

Most common uses of email	Count
Sent email from work account to personal account	164
Sent email to personal account from unspecified source (could be work account or uploaded to a personal account)	72
Sent email from work account to third party	61
Accessed email account of co-worker	40
Re-routed email or enabled mail-forwarding rules at mailbox or server level	32
When sending email to personal account, used multiple personal accounts	23
Downloaded emails or mailbox and exfiltrated by copying to storage device	24
Received incriminating email to work account from self or third party	22
Upload content to personal webmail account and sent mail	21
Sent email from work account to work account at future employer	15
Sent email from work account to personal account used by spouse	11

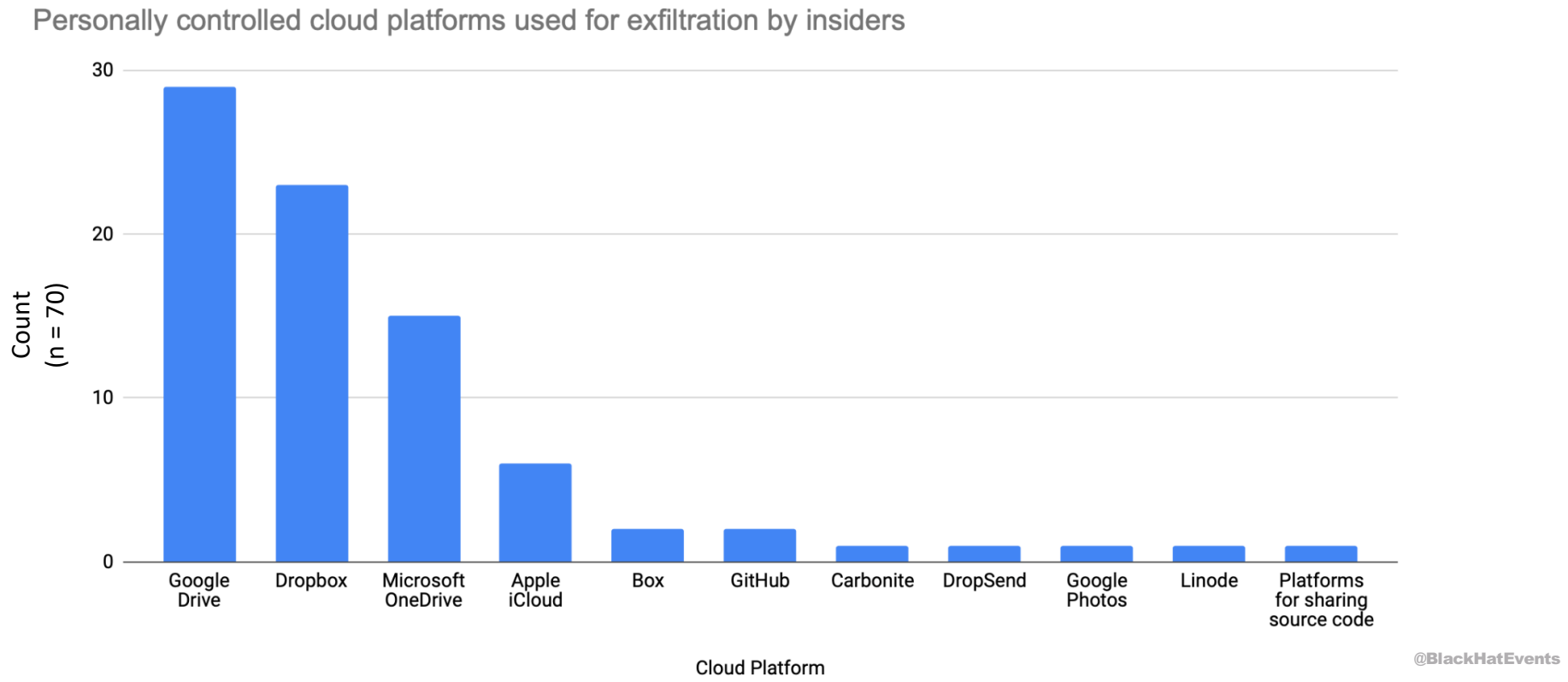
external storage devices

909 of 1,002 cases of insider threat activity involved data exfiltration.
315 cases of data exfiltration used external storage devices, e.g., USB flash drives.
115 cases reported data exfiltration occurred using multiple external storage devices. 89 cases provided quantifiable data.

Take away: When external storage devices are used for data exfiltration, there is a likelihood that multiple devices were used.

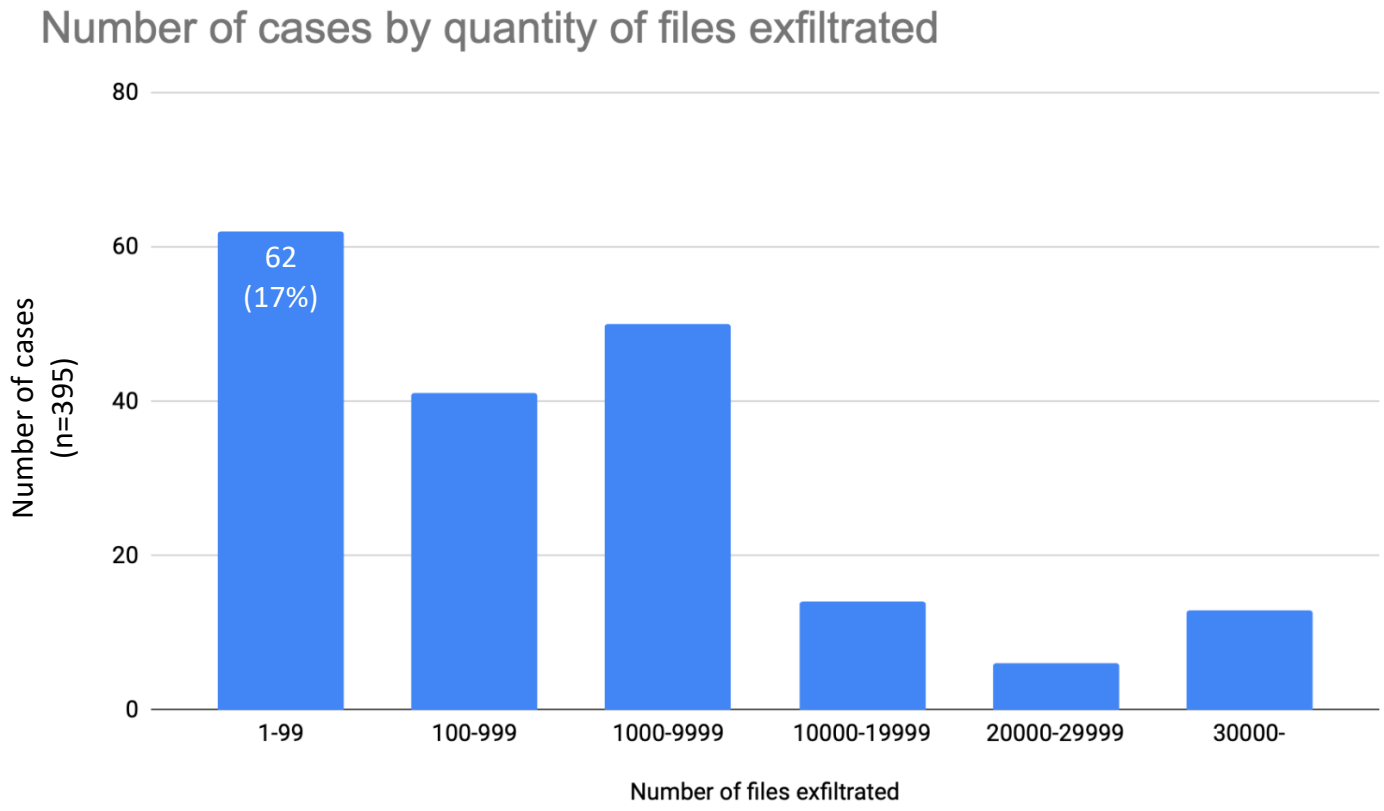


909 of 1,002 cases of insider threat activity involved data exfiltration.
93 cases involved exfiltration via the insider's personally controlled Cloud environment. 70 provided names of products.
11 cases involved insiders using multiple Cloud platforms for data exfiltration.



number of files exfiltrated

909 of 1,002 cases of insider threat activity involved data exfiltration.
395 cases provided quantified data about the number of files exfiltrated.

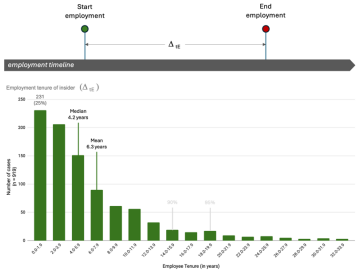


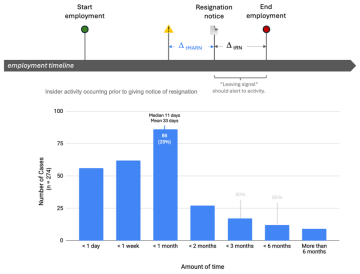
Description *There are times when malicious insiders perform certain activities to gain additional access to the organization's systems.*	Cases of it used during employment	Cases of it used during & after employment	Cases of it used after employment	Total
Used another employee's credentials (Note: 63 of the 120 instances were for insiders who were not in IT roles and did not work for IT companies.)	40	11	70	121
Install unauthorized software	76	1	19	96
Performed work, planning, or research for a competitor on the organization's computer system	48	1	0	50
Theft of equipment (beyond insiders who retained equipment beyond end of employment and returned it)	20	0	16	36
Shared credentials with unauthorized individuals	19	2	6	27
Broadened sharing permissions to access to data stored in the Cloud	20	0	2	22
Installed unauthorized hardware (not including external storage devices)	11	1	3	15
Modified a recovery account by adding a personal email address in lieu of organizationally controlled address	7	0	2	9
Extracted data from a vendor under the guise of legitimate use	4	1	3	8
Bypass multi-factor authentication	5	0	1	6
Installed a Virtual Machine (VM) on an organization's host and performed unauthorized activity in the VM	2	0	1	3

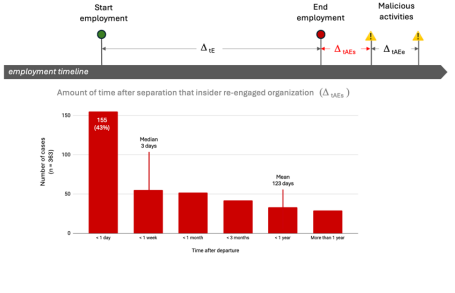
Put it together.

black hat BRIEFINGS

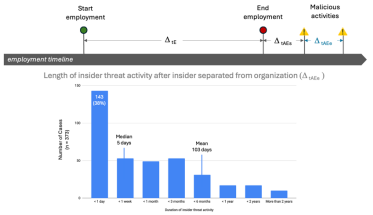
Employment tenure
+
Malicious activity in relation to start of employment
+
Duration of activity
+
Quantity of files
+
Separation notice (before and after)
+
Separation
+
Exfiltration mechanisms
+
Resignation window
+
Working for a competitor

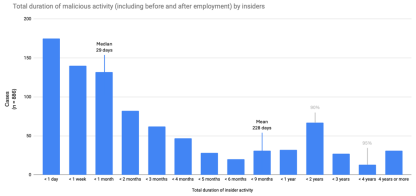


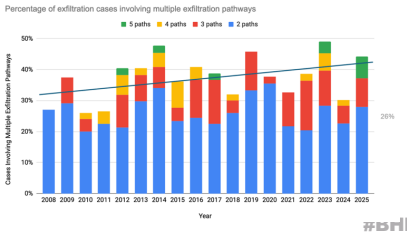




Category	Count
No notice	147
1 day's notice	15
1-7 days' notice	39
7-13 days' notice	31







Damage to systems.

damage to systems

334 of 1,002 cases contained damage to corporate systems.

Take away: Damage was primarily done by malicious insiders who quit rather than were fired.

Separation Mechanism	Number of cases involving damage
Voluntary resignation	168
Terminated, e.g., fired	108
Termination mechanism not identified	34
Contracted ended	12
RIF'd; Laid off	12

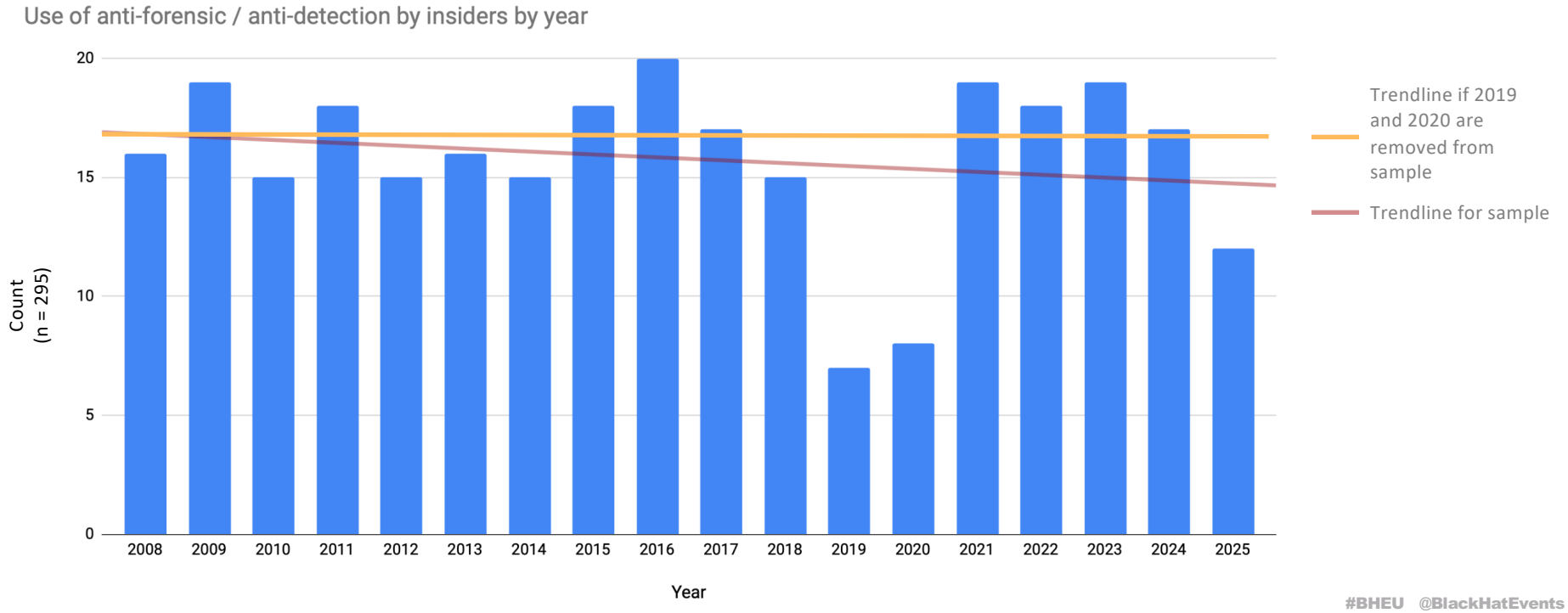
damage to systems

Description	Cases of damage during employment	Cases of damage during & after employment	Cases of damage after employment	Total
Deleted enterprise data	105	5	72	182
Delete locally stored data (Most attributed to anti-forensic / anti-detection efforts)	106	3	62	171
Delete email from system (Most attributed to anti-forensic / anti-detection efforts)	83	5	43	131
Modified the configuration of IT systems	57	5	54	116
Locked out legitimate users	32	9	58	99
Modifications to existing data	44	3	41	78
Damage to web app	15	0	30	45
Made an IT system inoperable	15	1	28	44
Damage to Cloud system or data stored in Cloud environment	14	3	25	42
Damage to public website	8	5	30	43
Damage to source code	6	2	11	19
Hijack social media sites	4	0	14	18

anti-forensic / anti-detection techniques

295 of 1,002 cases claimed to involve the insider performing anti-forensic / anti-detection techniques.
274 cases provides specific details of the TTP.

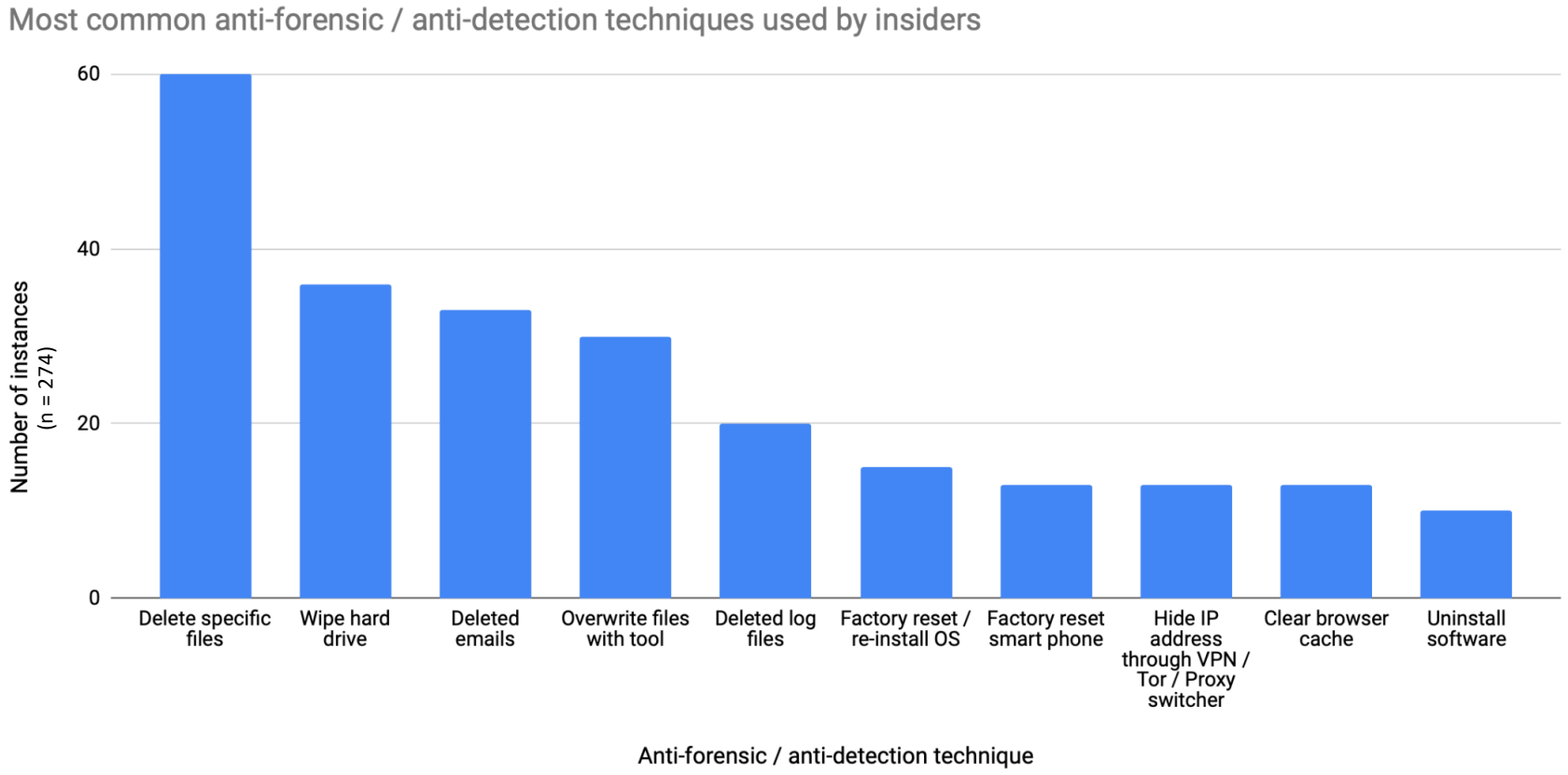
Take away: When 2020 is removed from the sample, the trend of insiders using anti-forensic / anti-detection techniques slightly increases.



Anti-forensics / anti-detection techniques

anti-forensic / anti-detection techniques

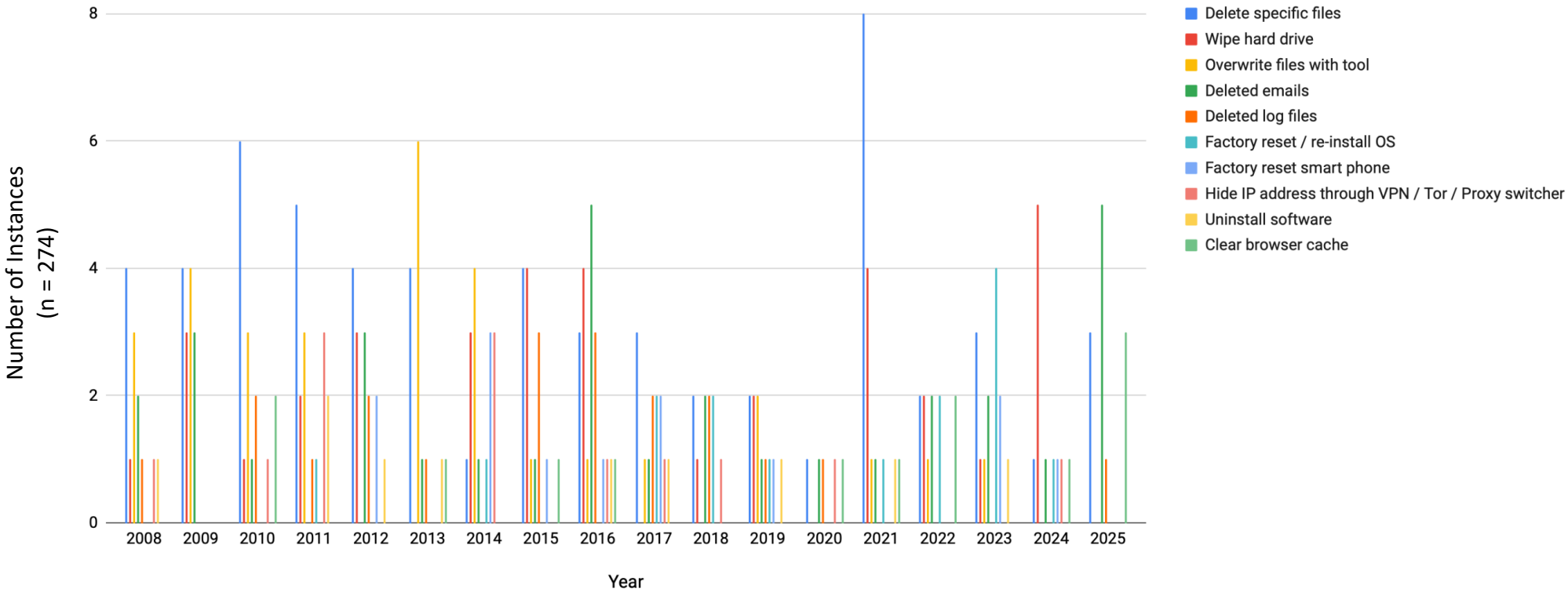
295 of 1,002 cases claimed to involve the insider performing anti-forensic / anti-detection techniques.
274 cases provides specific details of the TTP.



anti-forensic / anti-detection techniques

295 of 1,002 cases claimed to involve the insider performing anti-forensic / anti-detection techniques.
274 cases provides specific details of the TTP.

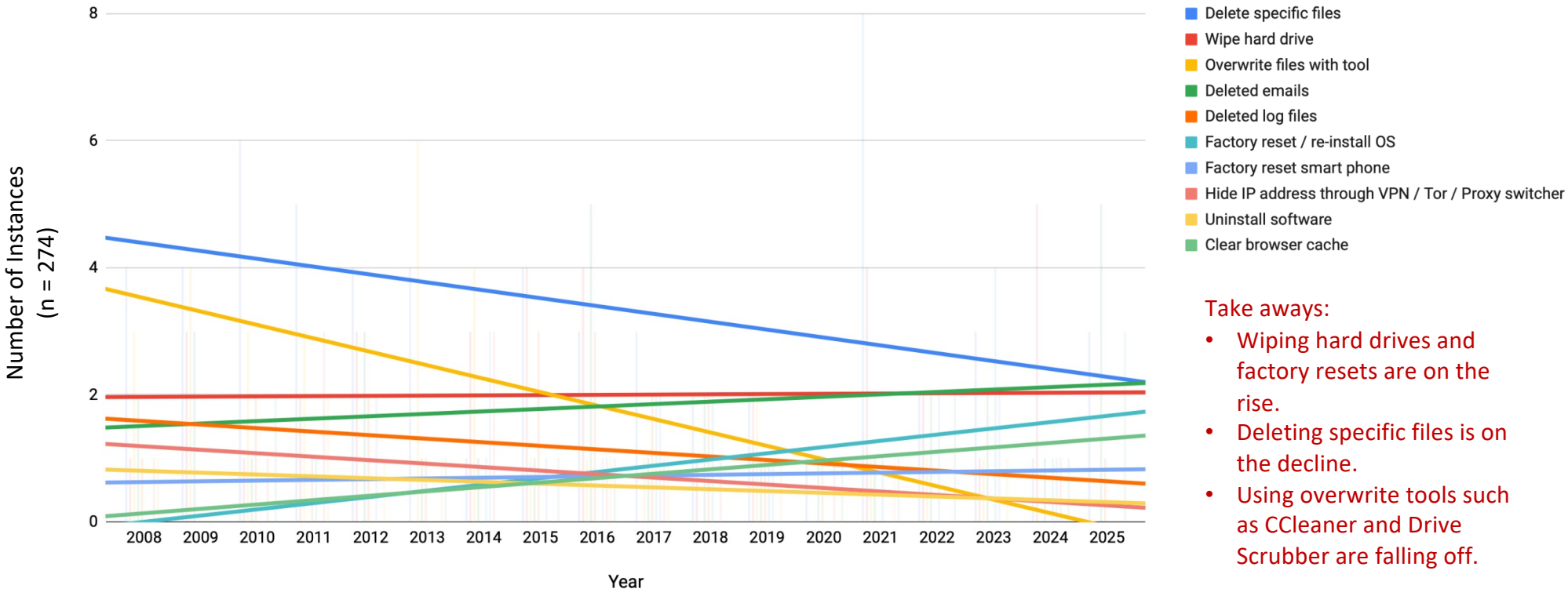
Most common anti-forensic / anti-detection techniques used by insiders by year



anti-forensic / anti-detection techniques

295 of 1,002 cases claimed to involve the insider performing anti-forensic / anti-detection techniques.
274 cases provides specific details of the TTP.

Most common anti-forensic / anti-detection techniques used by insiders by year



Take aways:

- Wiping hard drives and factory resets are on the rise.
- Deleting specific files is on the decline.
- Using overwrite tools such as CCleaner and Drive Scrubber are falling off.

Co-conspirators

What percentage of cases involved the insider colluding with other employees?

co-conspirators

313 of 1,002 cases (31%) involved co-conspirators, i.e., other insiders within the organization were involved.

TTPs

111 cases had insider and co-conspirator(s) using same TTPs.
91 cases had insider and co-conspirator(s) using different TTPs.
66 cases had insider and co-conspirator(s) using same and different TTPs.

External party involvement

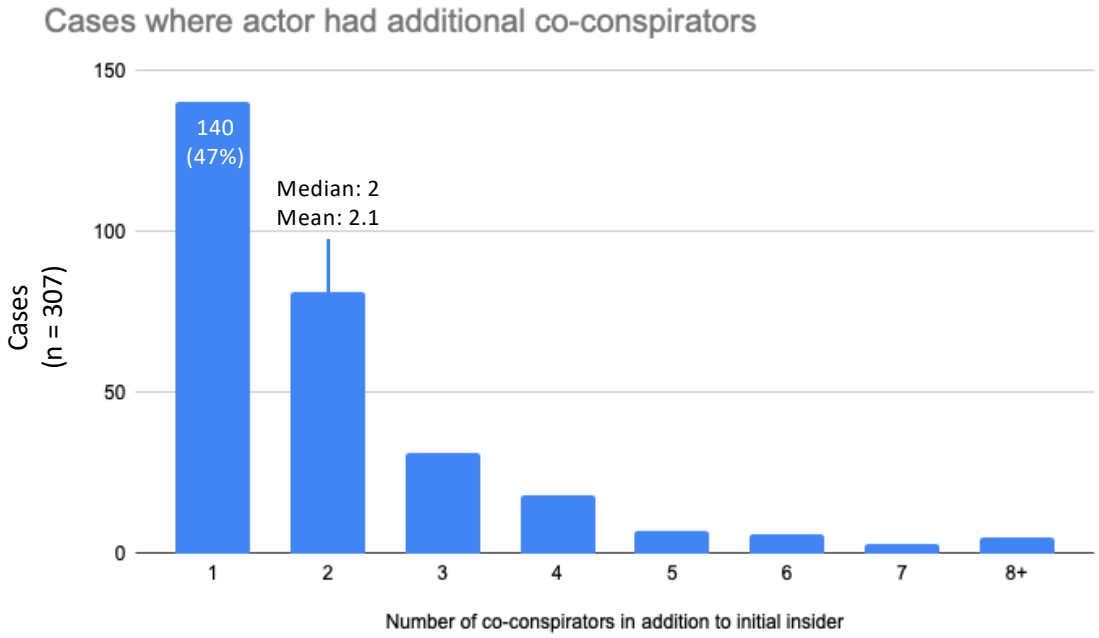
292 cases (29%) involved insider collaborating with an external party

When an insider engaged in collusion,
how many employees assisted on average?

co-conspirators

313 of 1,002 cases (31%) involved co-conspirators, i.e., other insiders within the organization were involved.
111 cases had insider and co-conspirator(s) using same TTPs.
91 cases had insider and co-conspirator(s) using different TTPs.
66 cases had insider and co-conspirator(s) using same and different TTPs.

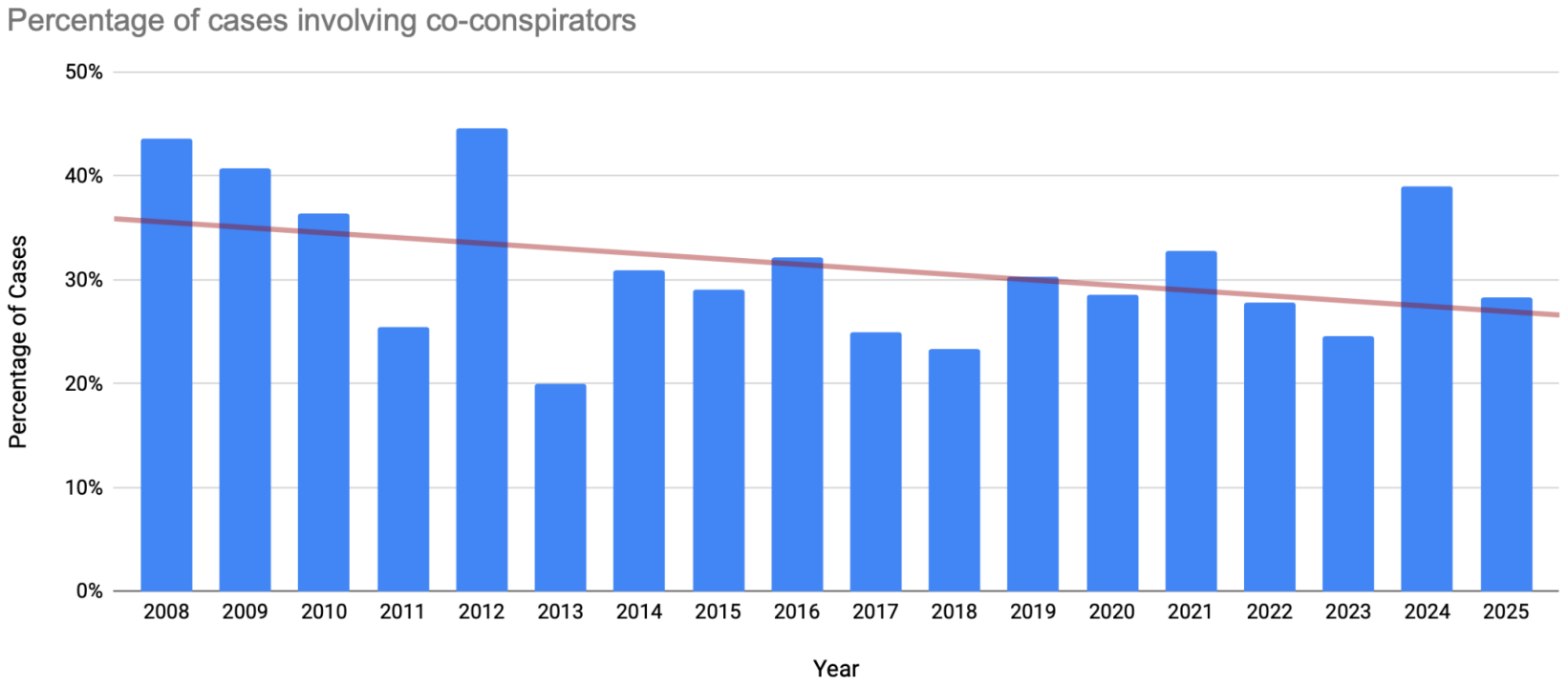
Take away: When co-conspiracy occurred, there were frequently two co-conspirators (in addition to the insider) making dyadic attribution difficult.



co-conspirators

313 of 1,002 cases (31%) involved co-conspirators, i.e., other insiders within the organization were involved.

Take away: There is a downward trend in the sample of cases involving co-conspirators.



co-conspirators

313 of 1,002 cases (31%) involved co-conspirators, i.e., other insiders within the organization were involved.

Take away: Insiders who work with co-conspirators are typically embedded within the organization longer, start insider threat activity later during employment and conduct insider threat activity longer.

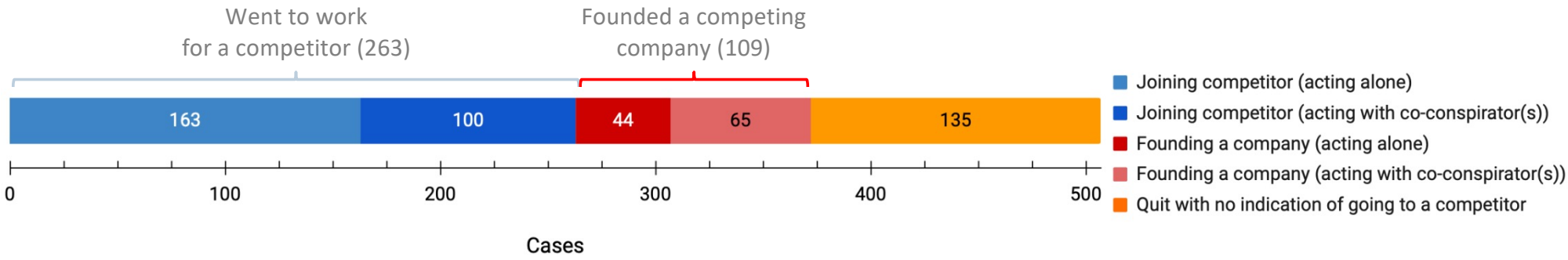
Characteristic	Cases without co-conspirators	Entire sample	Cases with co-conspirators
Employment tenure of insider	n: 635 Median: 4.1 years Mean: 6.2 years	n: 919 Median: 4.2 years Mean: 6.3 years	n: 284 Median: 4.7 years Mean: 6.5 years
Time after start of employment that insider activity began	n: 579 Median: 3.7 years Mean: 5.8 years	n: 845 Median: 3.9 years Mean: 5.8 years	n: 266 Median: 4.3 years Mean: 6.0 years
Duration of insider activity	n: 611 Median: 26 days Mean: 238 days	n: 886 Median: 29 days Mean: 228 days	n: 275 Median: 41 days Mean: 206 days

competing after employment

507 of the 1,002 cases involved malicious insider voluntarily separating from organization.
372 malicious insiders directly competed in next position of employment.
165 cases involved acting with co-conspirator.

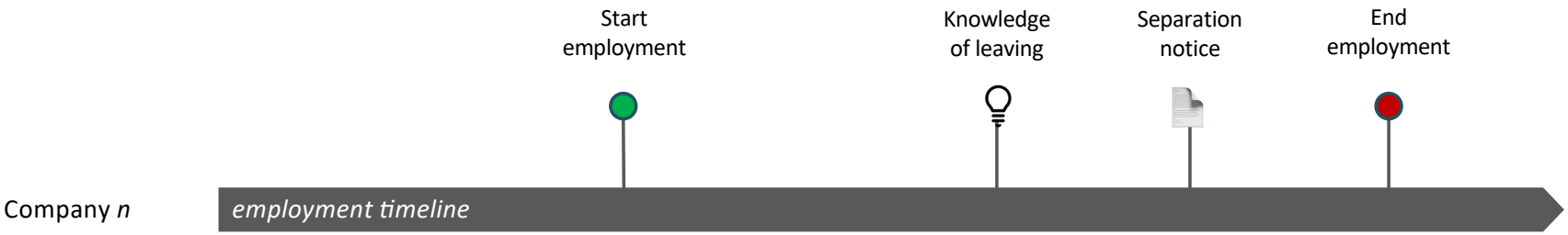
Take aways: 1. Malicious insiders go to or form competing organizations and stolen intellectual property can be re-used.
2. Co-conspirators play a significant role in insider-threat cases.

Cases where insider quit or claimed to retire and competed in next job

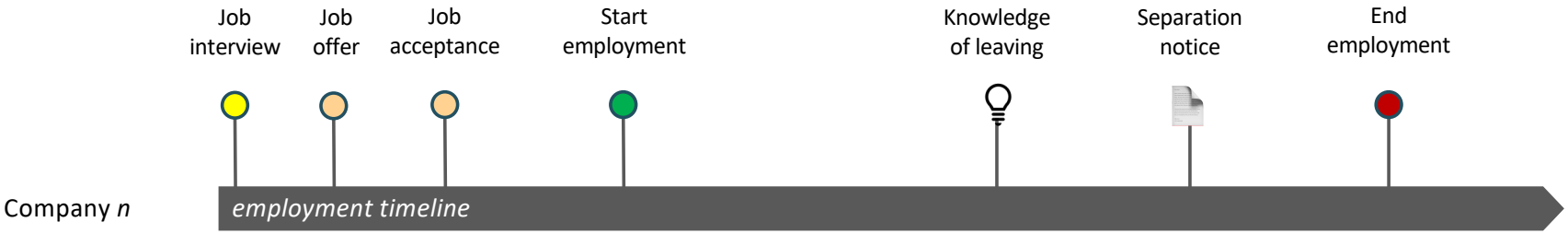


competing after employment

507 of the 1,002 cases involved malicious insider voluntarily separating from organization.
372 malicious insiders directly competed in next position of employment.

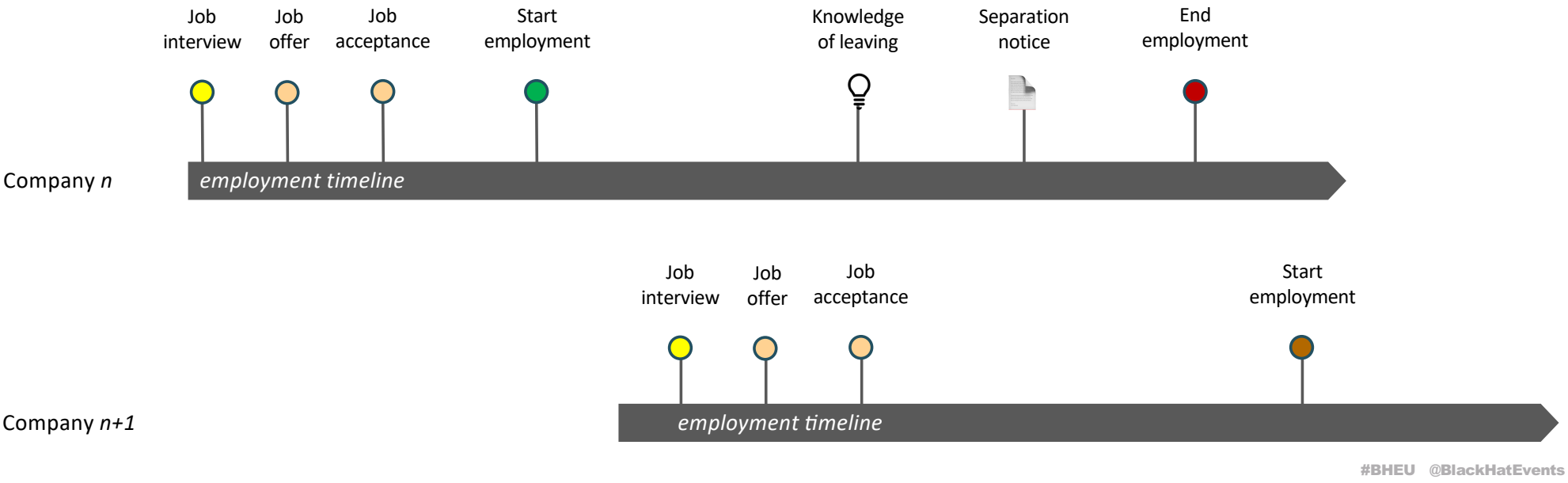


507 of the 1,002 cases involved malicious insider voluntarily separating from organization.
372 malicious insiders directly competed in next position of employment.



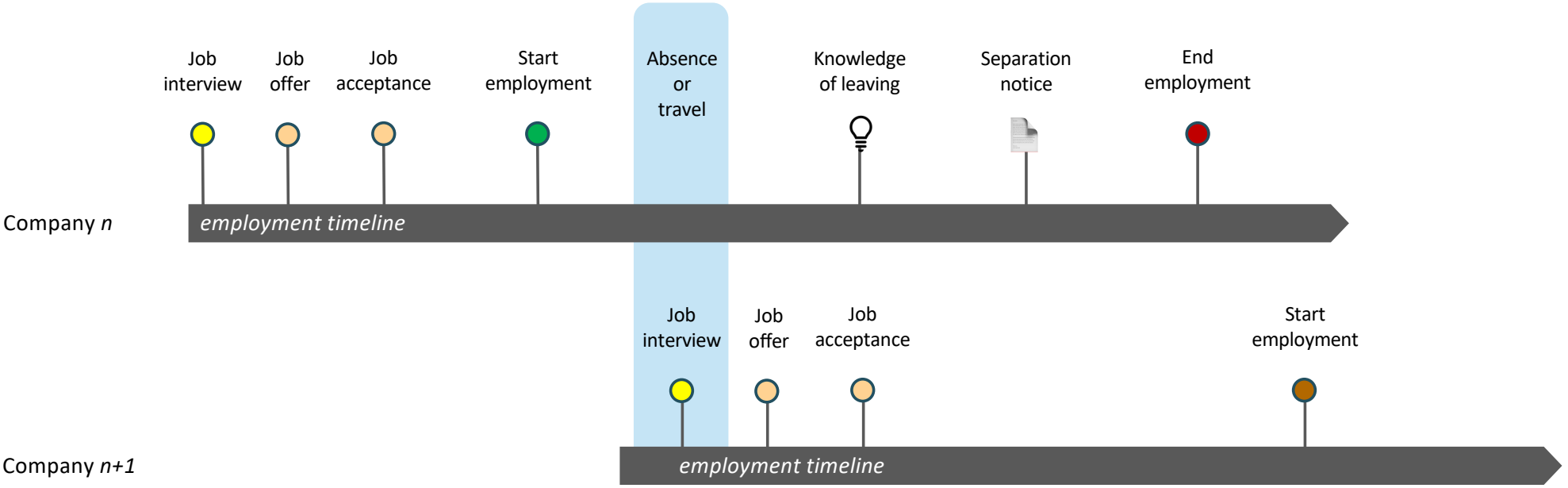
competing after employment

507 of the 1,002 cases involved malicious insider voluntarily separating from organization.
372 malicious insiders directly competed in next position of employment.



competing after employment

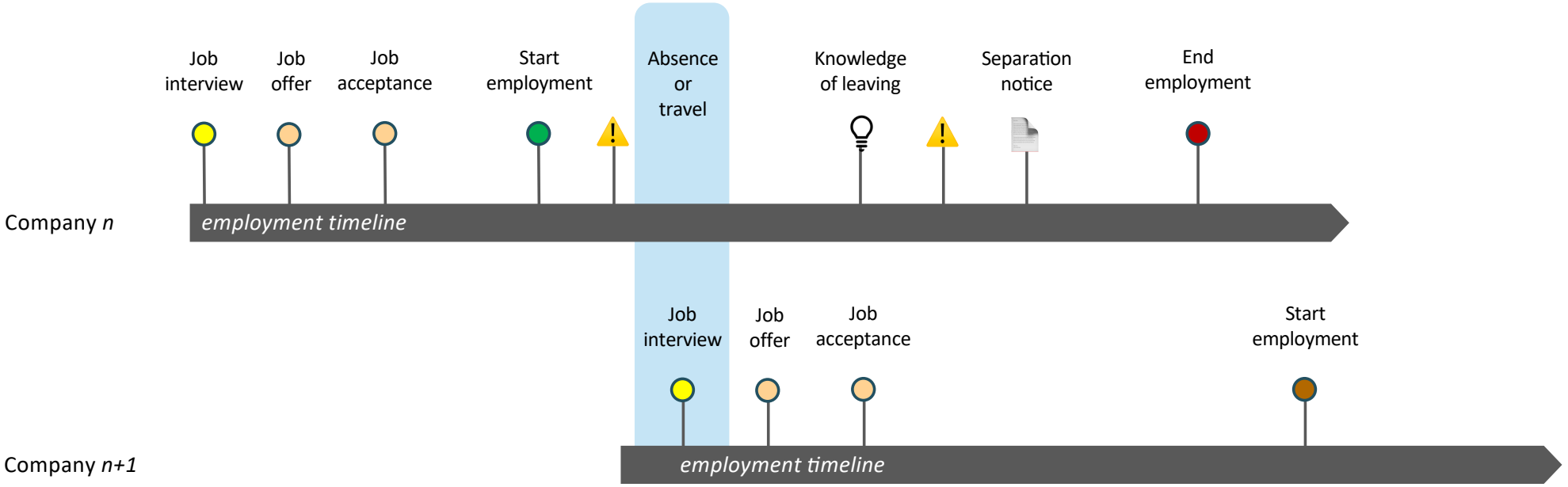
507 of the 1,002 cases involved malicious insider voluntarily separating from organization.
372 malicious insiders directly competed in next position of employment.



competing after employment

507 of the 1,002 cases involved malicious insider voluntarily separating from organization.
372 malicious insiders directly competed in next position of employment.

Take aways: Malicious activity in preparation for interview and in preparation for new employment.
When insider is founding a competing company, travel is replaced by registering a company.



Investigating insider threat cases is challenging.

Easier to address when it is viewed as multi-dimensional.

black hat BRIEFINGS

Michael Robinson
Senior Security Analyst; Digital Forensic Examiner; Adjunct Professor


black hat
BRIEFINGS
DECEMBER 10-11, 2025
EXCEL LONDON / UNITED KINGDOM
Understanding Trends & Patterns In Insider Threat
Analysis Of 1,000+ Cases
Michael Robinson
#BHEU @BlackHatEvents

Backup Material

Exfiltration Technique	Count
Email, including: - Content uploaded through browser to personal account - Mail sent from work account to personal account - Mail sent from work account to 3rd party - Mail forwarding rules at domain level - Mail forwarding rules at mailbox level - Re-routing mail to another domain - Log into another user's email and read or forward	368
External storage device	296
Cloud, including corporate or personally controlled Cloud environments	159
Web apps	128
Hard copies	90
Photograph	41
Theft of IT equipment	36
Encrypted communication app such as WeChat	30
Text message	25
Phone call and discussed material	23
Requested co-worker download material and transfer it	21
Download through VPN	20

Exfiltration Technique	Count
CD / DVD	16
Screenshot	14
Custom code to copy / backup data	11
Upload to personal website	8
Installed commercial backup software	7
Remote access software installed on workstation, e.g., AnyDesk	7
Video recording	6
Contact vendor and request data	4
Install Virtual Machine on local computer	4
Install keylogger	4
Audio recording	3
File transfer software, e.g., FileZilla or LimeWire	3
Install spyware	3
Communication through social media's channel, e.g., messages through Facebook or LinkedIn	2
Forensic imaging software or drive cloning software	2
Read contents on screen to another individual on the phone	2
Request customers send data directly to personal email account	2
Windows Remote Desktop Protocol	2
Docker containers	2

Exfiltration Technique	Count
AirDrop	1
ChatGPT upload	1
Copy and paste sensitive contents into new Word Documents	1
Cron job	1
Custom code installed within company's website	1
File synchronization software, e.g., SyncToy	1
PuTTY	1
Stealing corporate security video	1
Steganography tool	1
Stitch files together with a tool such as Adobe Acrobat	1
Web chat, e.g., Google Hangouts	1
uTorrent	1

Anti-forensic / Anti-detection Technique	Count
Deleted specific files (less than total wipe)	57
Wiped hard drive of corporate laptop or computer	36
Overwrote data using software such as CCleaner or Drive Scrubber	29
Deleted email	28
Deleted logs	19
Performed a factory reset / re-installed the operating system	15
VPN / Tor / Proxy switcher / Mask IP address	13
Performed a factory reset of the smartphone	13
Deleted browser cache	10
Uninstalled software and related logs	10
Physical destroyed computer or storage device	8
Deleted specific data from phone	6
Encrypted files	5
Accessed the corporate network through public Wi-Fi or neighbor's Wi-Fi	4
Repurposed hard drive / tech upgrade	4
Wiped USB device	4
Reformatted hard drive	3
Used webmail to avoid triggering corporate mail monitoring	3
Booted from OS on USB	2
Changed details on copyright and license	2

Anti-forensic / Anti-detection Technique	Count
Changed log retention	2
Deleted Cloud account after sharing completed	2
Encrypted hard drive	2
Performed timestomping / Changed system clock	2
Encrypted a hard drive	2
Changed the litigation hold settings on user account to allow files to be purged	1
Created a webmail account and set display name to name of another employee	1
Deleted backdoor account after it was used	1
Deleted backups	1
Deleted the Virtual Machine on the workstation	1
Disabled security cameras	1
Disconnected computer from the Internet to avoid remote monitoring / wiping	1
Encrypted communication channel	1
Logged off corporate computer to avoid detection	1
Modified data in corporate database so records were traced back to fictitious user	1
Renamed USB device to make unused device appear like the one that was used for exfiltration	1
Swapped hard drives in corporate computer	1
Transmitted emails below a threshold / limit to avoid detection	1
Used a burner phone for communication	1

Anti-forensic / Anti-detection Technique	Count
Used a fake name to open support tickets or file bugs	1
Used another employee's account to hide activity	1
Used command line in lieu of GUI	1
Used Incognito mode on the browser	1
Used separate laptops	1
Used steganography	1
Changed the password on computer	1
Cleared bash history	1
Cleared cache / temp files	1
Deleted chats	1
Deleted Cloud files	1
Deleted GitHub account after exfiltration	1
Disabled apps on smartphone	1
Filed a bug to bypass security	1
Cleared printer's history	1
Had Another employee badged in/out	1
Hid malicious script within legitimate script	1
Installed a Virtual Machine on the workstation	1
Removed labels or document markings	1
Renamed files	1

Anti-forensic / Anti-detection Technique	Count
Renamed files	1
Shredded physical documents	1
Surrendered unrelated laptop for inspection	1
Talked on phone to avoid electronic record	1
Used a gift card for purchases to avoid tracking	1


black hat
BRIEFINGS
DECEMBER 10-11, 2025
EXCEL LONDON / UNITED KINGDOM
Understanding Trends & Patterns In Insider Threat
Analysis Of 1,000+ Cases
Michael Robinson
#BHEU @BlackHatEvents