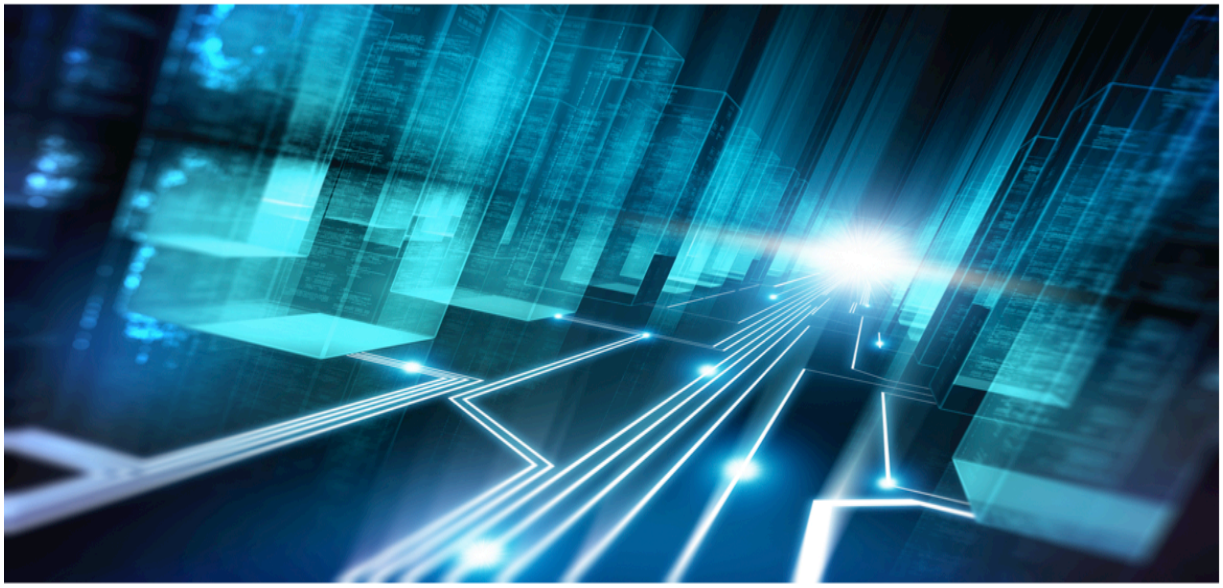


Network Forensic Investigations Market Study

Sponsored by IBM

Independently conducted by Ponemon Institute LLC

Publication Date: December 2014

Network Forensic Investigations Market Study

Ponemon Institute, December 2014

Part 1. Introduction

Ponemon Institute is pleased to present the results of *Network Forensic Investigations Market Study* sponsored by IBM. The purpose of this research is to understand how organizations are using forensic tools to investigate attacks against the network, possible security breaches and insider attacks.

We surveyed 251 US IT and IT security practitioners in organizations that employed some sort of technology to assist with IT security incident forensics investigations beyond a SIEM solution and are either a principal investigator of this technology or a member of a team investigating the solution. Following are the topics covered in this study:

- Perceptions about the use of existing forensic tool
- Estimating forensic workflows
- Network forensic skills and practices

Following are the most salient findings from this research:

Existing forensic tools are complex but considered effective. Fifty-six percent of respondents have a very positive or positive impression about their existing forensic tool and 69 percent of respondents say their technology is very effective (29 percent) or effective (40 percent).

How accurate are forensic investigations? An average of only 19 percent of all network attacks investigated by the IT security team are proved to be actual attacks, an average of 31 percent of security breaches investigated by the IT security team are proven to be actual attacks. Fifty-one percent of insider attacks investigated by the IT security team are actual attacks.

In a forensic investigation, most time is spent on insider attacks. It takes on average more than 70 hours to investigate an insider attack and suspected security breaches consume an average of 59 hours. To investigate a suspected network attack takes far less time (43 hours).

The detection to containment part of the forensic investigation consumes the most time for an insider attack. It takes an average of 9 days to complete one investigation from detection to containment of an insider attack. This is followed by 7 days to complete one forensic investigation of a security breach from detection to containment. It takes far less time to investigate a network attack.

Most IT security teams use forensic intelligence/analysis tools to help with the investigation of network attacks and security breaches. Eighty-four percent of respondents say all (44 percent) or most (40 percent) of investigations regarding network attacks and security breaches use forensic intelligence/analysis tools. However, only 40 percent of respondents say their forensic tools are integrated within a broader suite of IT security solutions such as SIEM.

Many organizations collect packet captures as part of their IT security analytical capabilities. Sixty-nine percent of respondents say their organizations collect packet captures. Full packet capture refers to the process of intercepting and logging all network (both header and payload) traffic. Of those respondents who say their organization collects packet captures, 40 percent of respondents say the collection occurs at data centers followed by network egress points.

Part 2. Key findings

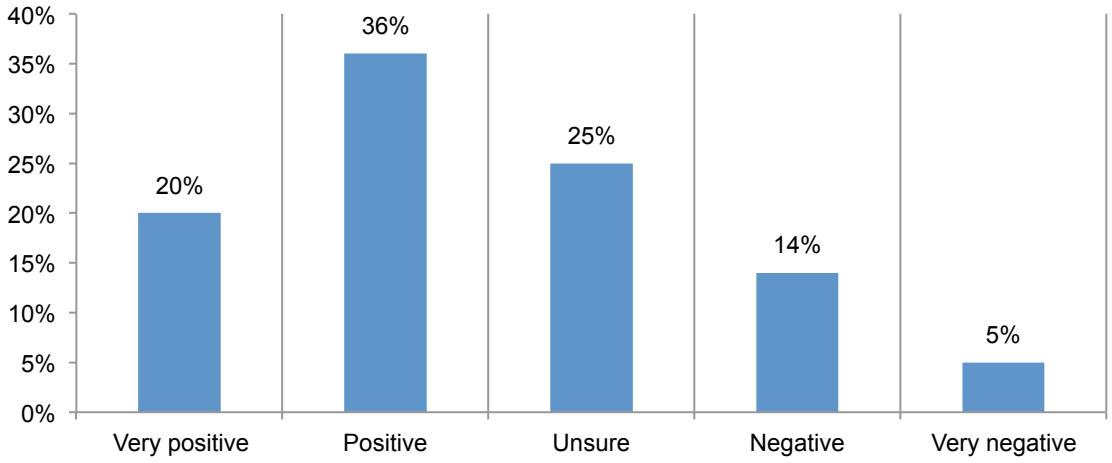
In this section, we analyze the findings of this research. The complete audited findings are presented in the appendix of this report. The report is organized according to the following themes:

- Perceptions about the use of existing forensic tool
- Estimating forensic workflows
- Network forensic skills and practices

Perceptions about the use of existing forensic tool

Existing forensic tools are complex but considered effective. As shown in Figure 1, 56 percent of respondents have a very positive or positive impression about their primary network forensic/analysis tool used by their IT security team. Sixty-nine percent of respondents say their technology is very effective (29 percent) or effective (40 percent).

Figure 1. What describes your impression of your organization's forensics/analysis tool?



Despite these positive impressions, Figure 2 reveals what respondents think about the technology's complexity. As shown, 73 percent of respondents say their primary network forensics/analysis tool is very difficult (30 percent) or difficult (43 percent) to use.

Figure 2. How difficult is it to use the forensics/analysis tool?

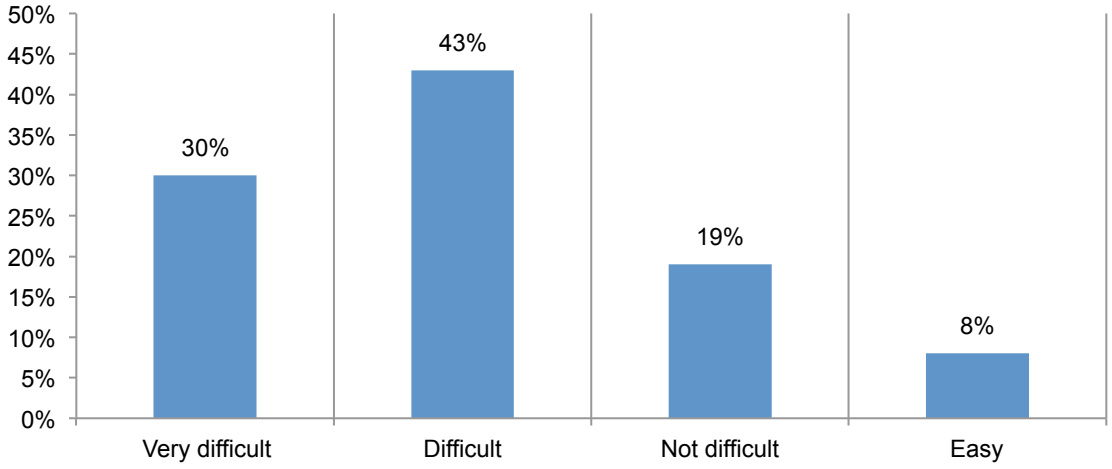
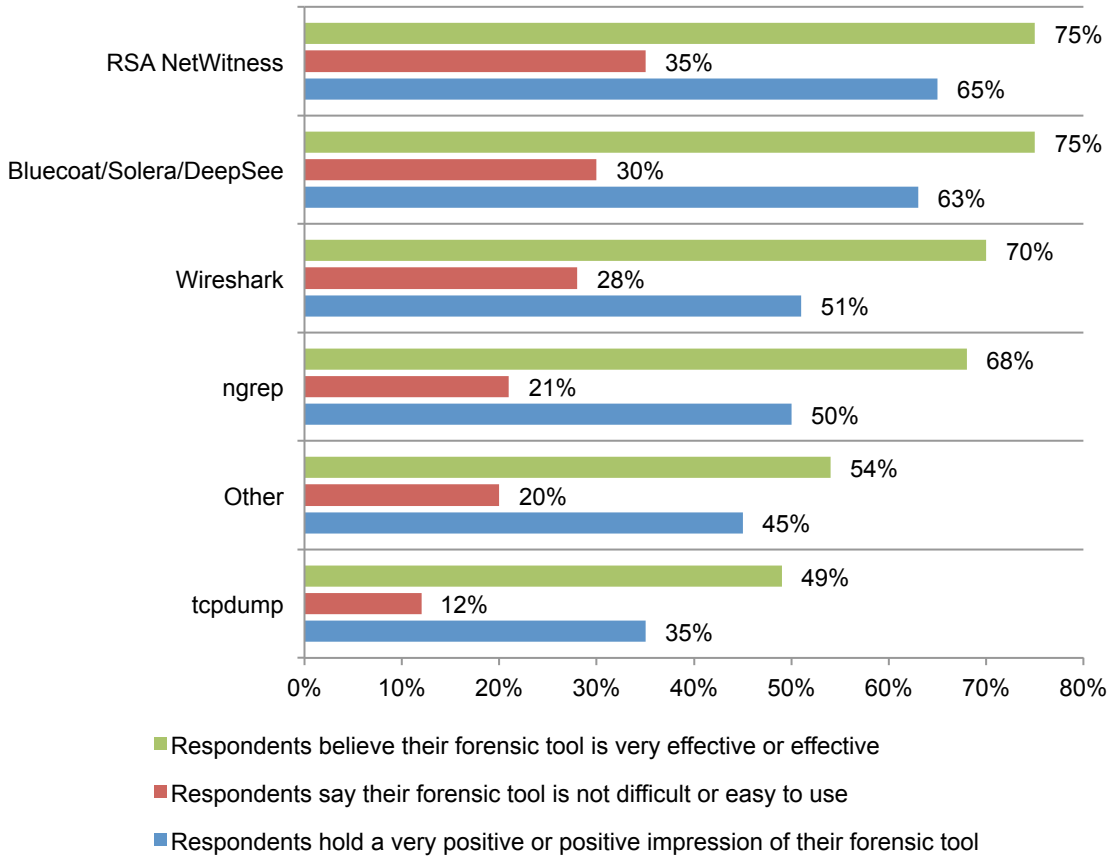


Figure 3 reports respondents' perceptions of leading primary network forensic tool used by their organizations. As can be seen, RSA Netwitness and Bluecoat/Solera/DeepSee achieve the highest product ratings with respect to effectiveness, ease of use and overall impressions. In contrast, tcpdump has the lowest ratings for all three perception categories.

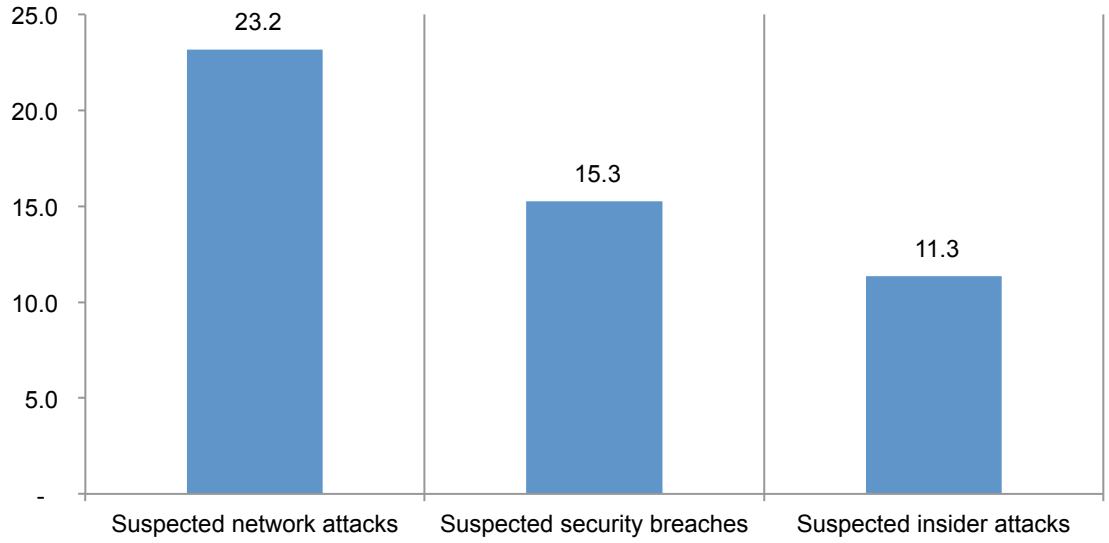
Figure 3. Three characteristics for six forensic investigation tools



Estimating forensic workflows

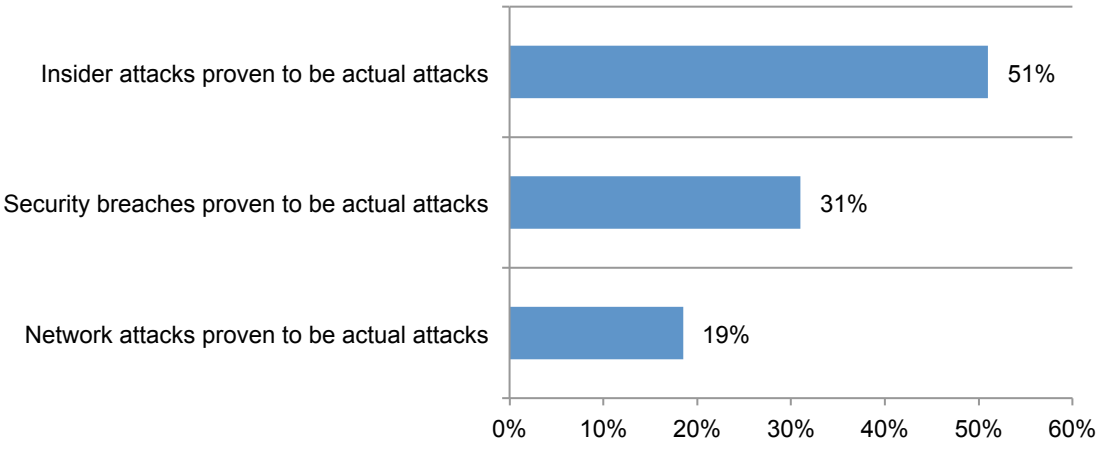
Security incidents and investigations reported in the past 12 months. Respondents were asked to estimate the number of IT security investigations involving forensics experts in the past year. According to Figure 4, the average number of investigations concerning suspected network attacks was almost two per month (23). Forensics investigations of suspected security breaches was 15 and suspected insider attacks was 11.

Figure 4. Security incidents and investigations reported in the past 12 months
Extrapolated frequencies



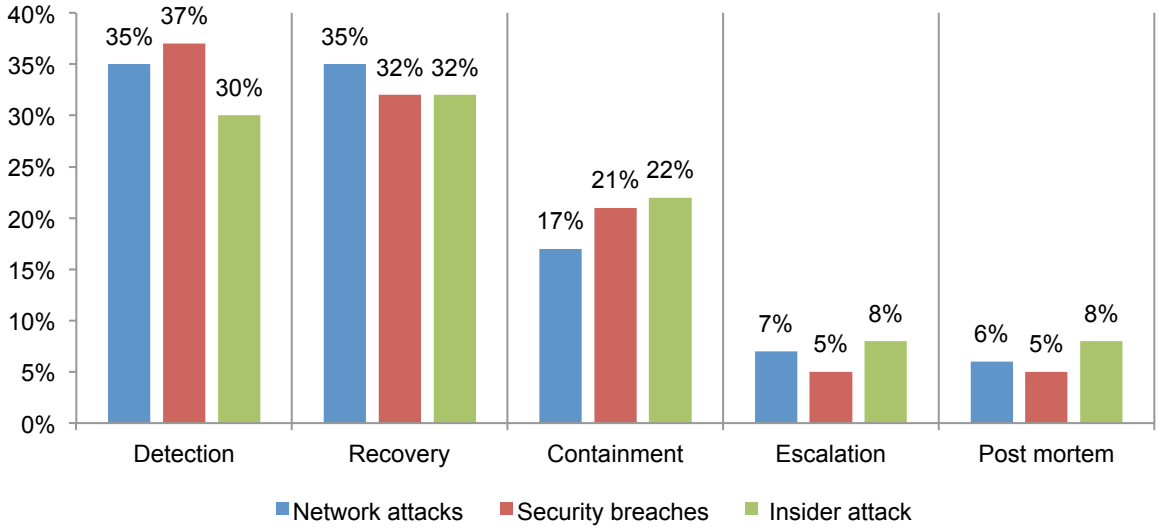
How accurate were the investigations? An average of only 19 percent of all network attacks investigated by the IT security team were proven to be actual attacks (Figure 5), an average of 31 percent of security breaches investigated by the IT security team were actual attacks. Fifty-one percent of insider attacks investigated by the IT security team were actual attacks.

Figure 5. Percentage of network attacks, security breaches and insider attacks investigated and determined to have occurred
Extrapolated percentage values



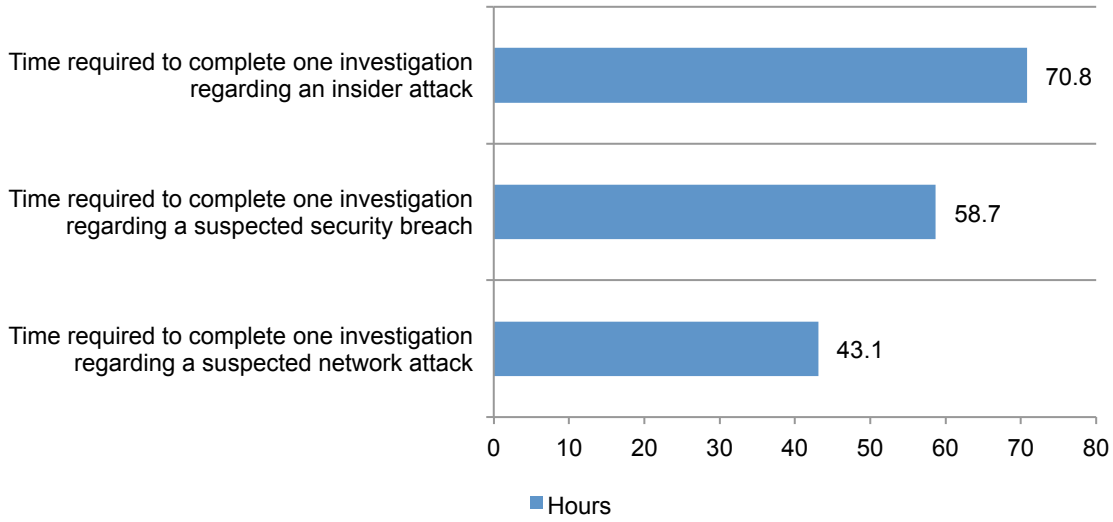
In the typical investigation, detection and recovery require the most time to complete. As shown in Figure 6, in investigating a network attack, security breach or insider attack, the greatest allocation of time is spent in the detection and recovery phase. Specifically, when investigating a suspected network attack, 70 percent of the time is spent on the detection and recovery phase.

Figure 6. Percentage of time required to complete each phase of the investigation



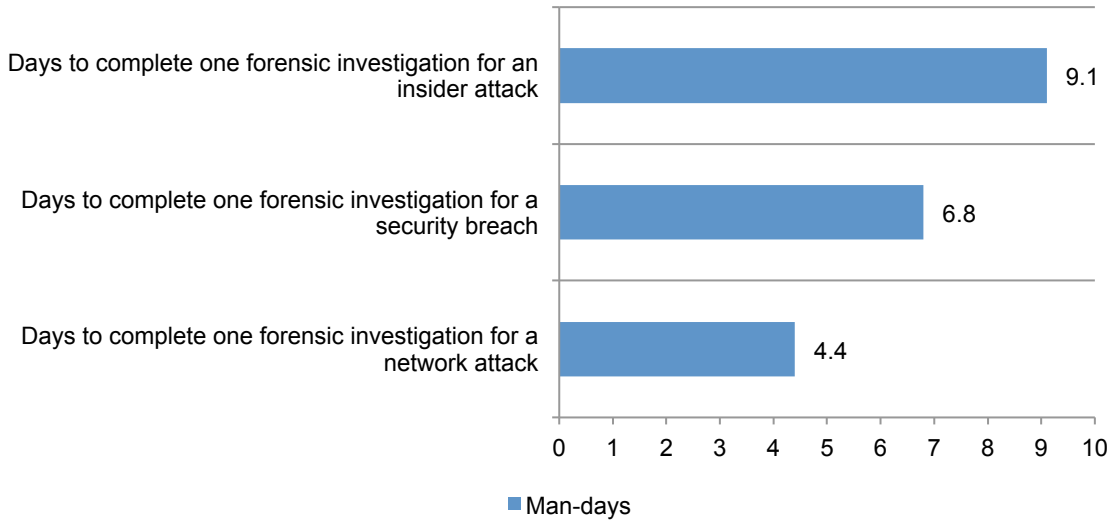
In a forensic investigation, most time is spent on insider attacks. Figure 7 shows the average time in hours it takes an IT security team to conduct a forensic investigation of a network attack, suspected security breach and insider attack. Insider attacks and suspected security breaches consume the most time (70.8 and 58.7 hours, respectively).

Figure 7. Forensic investigation time for a network attack, suspected security breach and insider attack



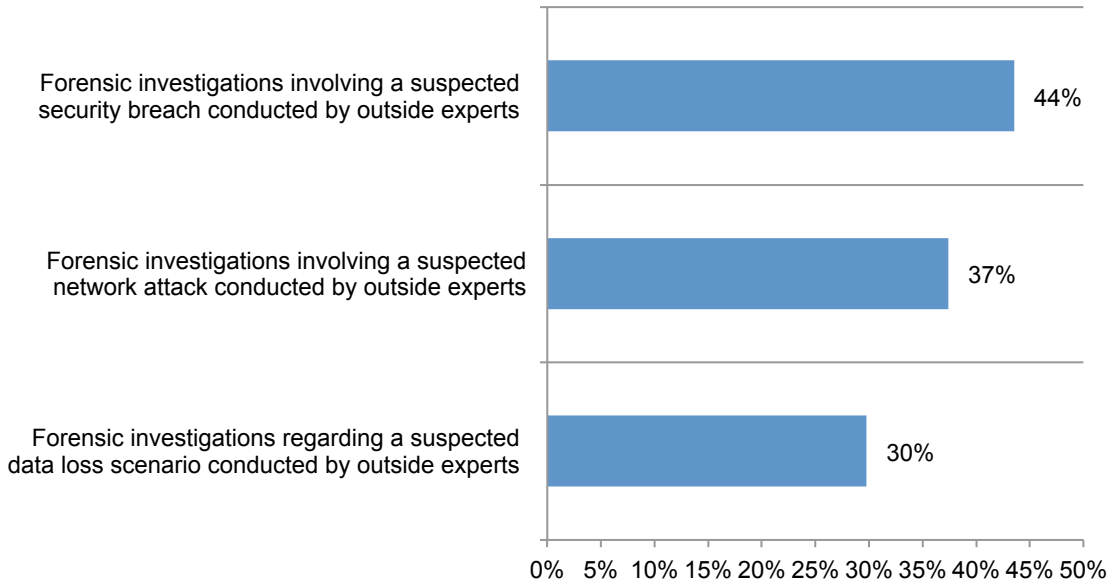
The detection to containment part of the forensic investigation consumes the most time for an insider attack. As shown in Figure 8, it takes an average of 9 days to complete one investigation from detection to containment of an insider attack. This is followed by 7 days to complete one forensic investigation of a security breach from detection to containment. It takes far less time to investigate a network attack.

Figure 8. Time it takes to complete one forensic investigation from detection to containment



The organization's IT security staff is most likely to conduct forensic investigations. Do organizations turn to outside experts to investigate a network attack, security breach or loss of data? According to Figure 9, consultants are mostly called in to investigate a suspected security breach. Consultants are less frequently involved in investigations concerning a suspected network attack (37 percent) or a suspected data loss scenario (30 percent).

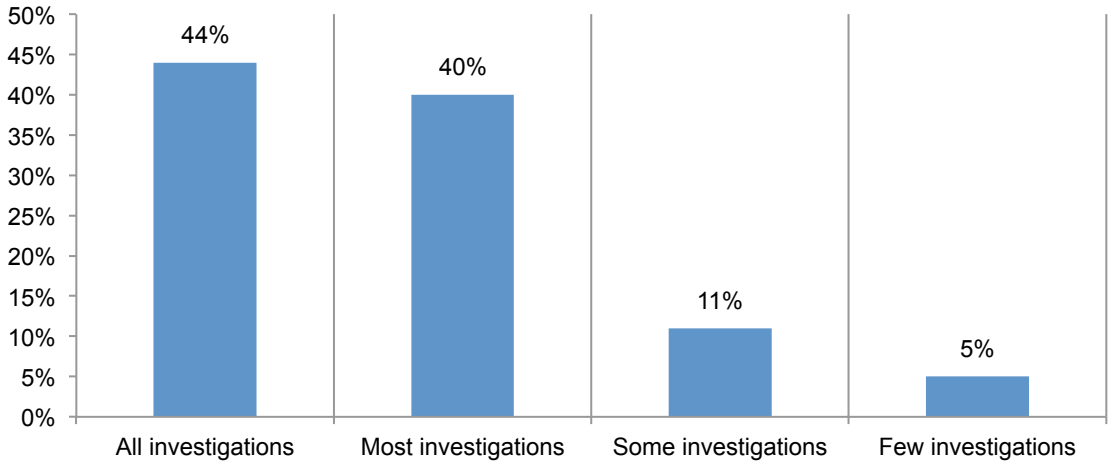
Figure 9. How often are consultants engaged to investigate a security incident?



Network forensic skills and practices

Most IT security teams use forensic intelligence/analysis tools to help with the investigation of network attacks and security breaches. Eighty-four percent of respondents say all (44 percent) or most (40 percent) of investigations regarding network attacks and security breaches use forensic intelligence/analysis tools, as shown in Figure 10. However only 40 percent of respondents say their forensic tools are integrated within a broader suite of IT security solutions such as SIEM.

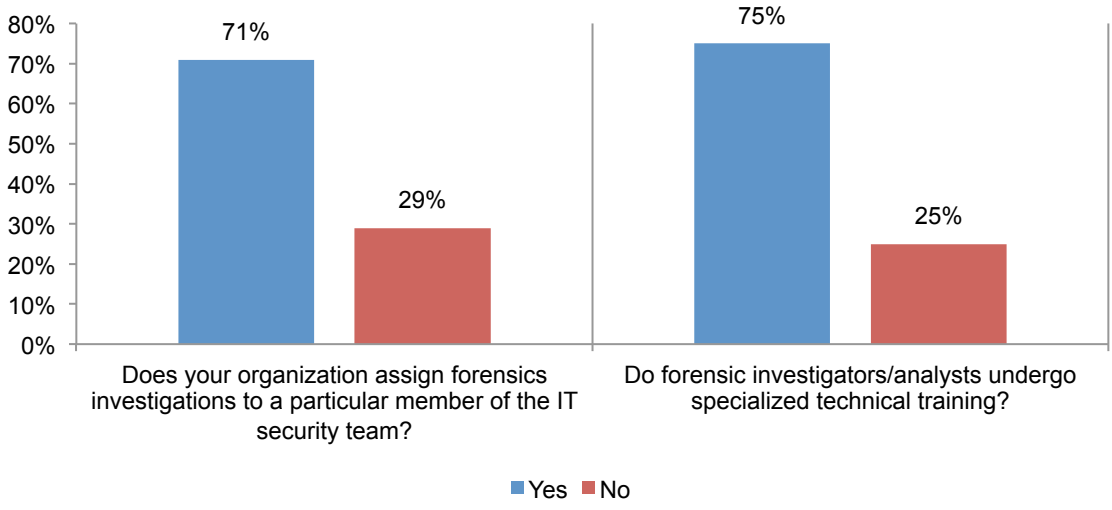
Figure 10. Does the IT security team use forensic intelligence tools to investigate network attacks and security breaches?



Forensic investigators are skilled in cyber security and other fields. As shown in Figure 11, the majority of organizations assign forensics investigations to a particular member of the IT security team (71 percent of respondents) with specialized training (75 percent of respondents).

On average individuals investigating suspected cyber attacks or breaches have 9 years experience and 56 percent of forensic investigators have advanced degrees and certifications in cyber security and other related fields.

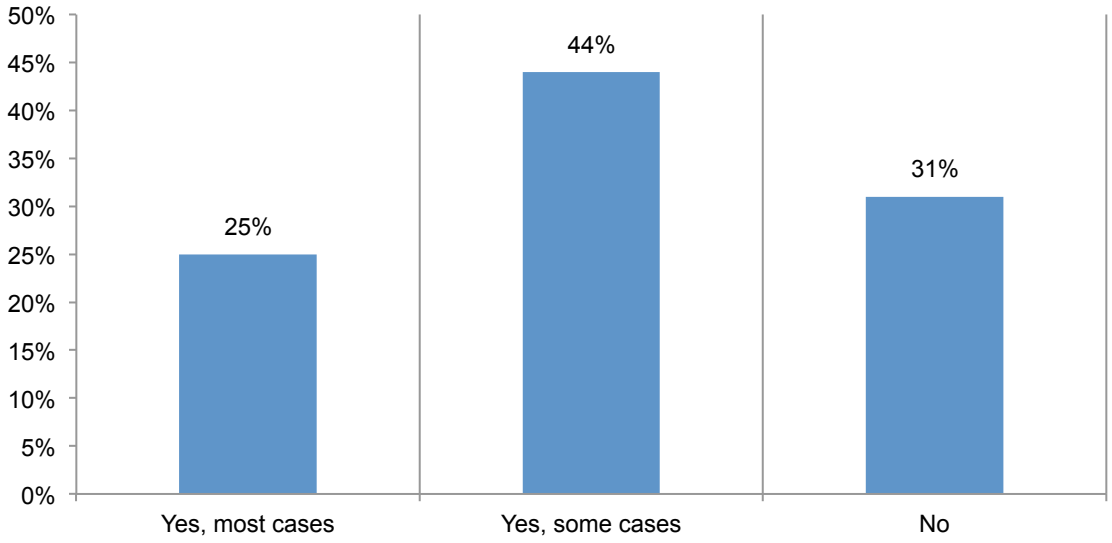
Figure 11. Are investigations assigned to one member of the IT security team and do they have specialized training?



Are organizations receiving actionable information? Only 44 percent of respondents say their IT security team receives alerts that would be helpful and provide guidance to forensic investigators regarding current threats. However, as shown in Figure 12, 69 percent of respondents believe their forensics search efforts deliver sufficient evidence to effectively prosecute the instigators of a network attack or data loss in most cases (25 percent) and some cases (44 percent).

Fifty-six percent of respondents say their organizations' incident investigations result in the production of threat indicators, which are then used to defend the organization from future attacks.

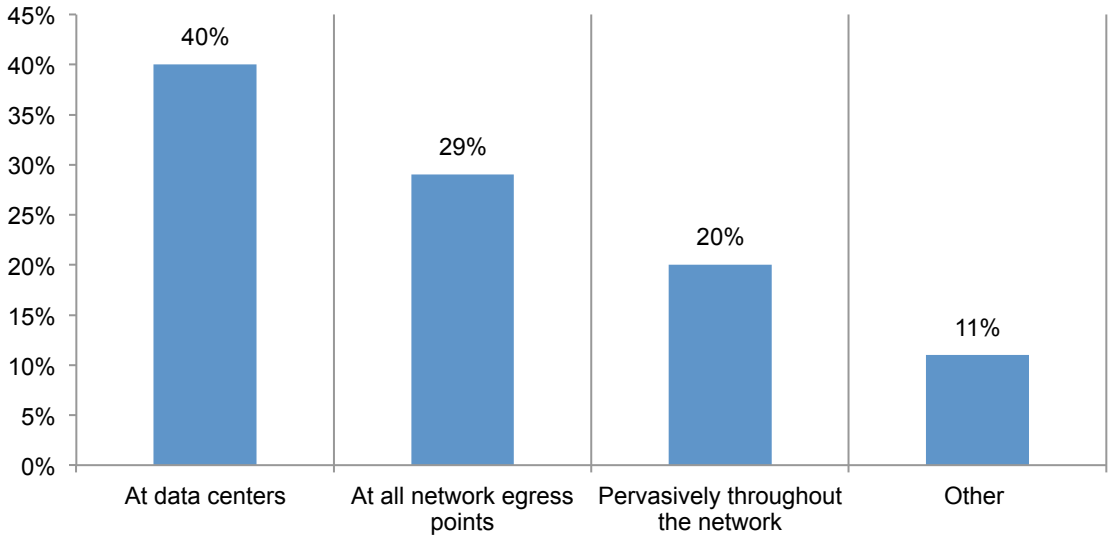
Figure 12. Does forensics provide evidence to prosecute the instigators of a network attack or data loss?



Many organizations collect packet captures as part of their IT security analytical capabilities. Sixty-nine percent of respondents say their organizations collect packet captures. Full packet capture refers to the process of intercepting and logging all network (both header and payload) traffic. Of those respondents who say their organization collects packet captures, 40 percent say the collection occurs at data centers followed by network egress points, as shown in Figure 13.

On average, organizations store full packet capture for 10 days. However, only 33 percent say their current solution allows their organization to maintain packet capture evidence over a sustained period of time. When asked how long their organization can retain raw network packet captures, the average response was 174 days.

Figure 13. Where does your organization collect full packet capture from the network?



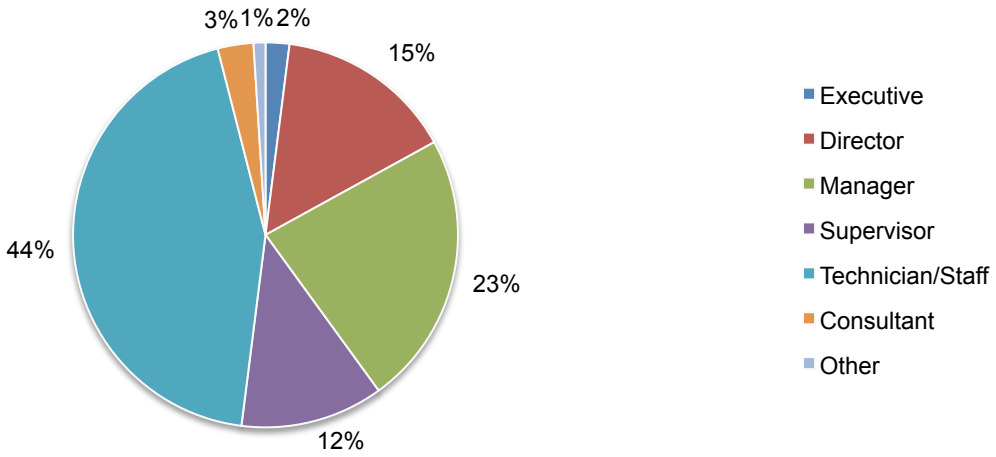
Part 3. Methods

A sampling frame composed of 7,668 IT and IT security practitioners located in US organizations that employ a technology to assist with IT security incident forensics investigations beyond a SIEM solution and are either a principal investigator of this technology or a member of a team investigating the solution were selected for participation in this survey. As shown in the Table 1, 331 respondents completed the survey. Screening removed 80 surveys. The final sample was 251 surveys (or a 3.3 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	7,668	100.0%
Total returns	331	4.3%
Rejected or screened surveys	80	1.0%
Final sample	251	3.3%

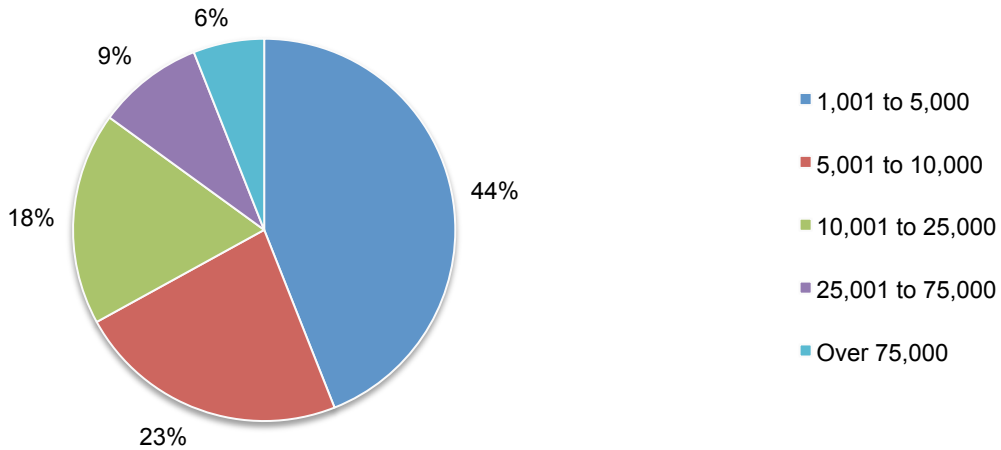
Pie chart 1 reports the current position or organization level of the respondent. More than half (52 percent) of respondents reported their current position is at or above the supervisory level.

Pie Chart 1. Position level within the organization



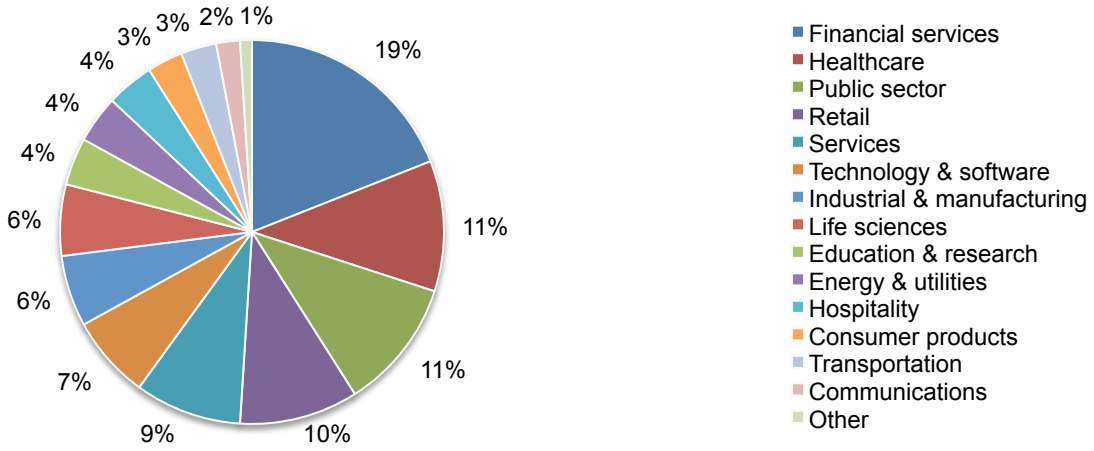
Pie chart 2 reports the full-time headcount of the global organization. More than half (67 percent) of respondents reported their organization employs between 1,000 and 10,000 full-time employees.

Pie Chart 2. Full-time headcount of the global organization



Pie Chart 3 reports the primary industry classification for the respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by healthcare (11 percent) and public sector (11 percent).

Pie Chart 3. The primary industry classification for the IT respondent



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners located in various organizations in the United States. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in October 2014.

Survey response	Freq	Pct%
Total sampling frame	7,668	100.0%
Total returns	331	4.3%
Rejected or screened surveys	80	1.0%
Final sample	251	3.3%

Part 1. Screening

S1a. Have you employed some sort of technology to assist with IT security incident forensics investigations beyond a SIEM solution?	Pct%
Yes	100%
No (stop)	0
Total	100%

S1b. If yes, please check the primary network forensics/analysis tool used by your organization to investigate network attacks and other security breaches?	Pct%
RSA NetWitness	28%
Bluecoat/Solera/DeepSee	30%
Wireshark	10%
tcpdump	9%
ngrep	11%
Other	12%
None (stop)	0%
Total	100%

S2. What best describes your level of involvement in network forensic investigations within your company)?	Pct%
Significant involvement (principal investigator)	44%
Some involvement (member of the investigative team)	56%
Minimal or no involvement (stop)	0%
Total	100%

Part 2. Perceptions about existing forensic tool

Q1a. What best describes your overall impression of the primary network forensics/analysis tool used by your IT security team?	Pct%
Very favorable	20%
Positive	36%
Unsure	25%
Negative	14%
Very negative	5%
Total	100%

Q1b. What best describes the level of complexity (or difficulty) in using your primary network forensics/analysis tool?	Pct%
Very difficult	30%
Difficult	43%
Not difficult	19%
Easy	8%
Total	100%

Q1c. What best describes the effectiveness of your primary network forensics/analysis tool?	Pct%
Very effective	29%
Effective	40%
Not effective	21%
Unsure	10%
Total	100%

Part 3. Background

Q2. What best describes your position level within the organization?	Pct%
Executive	2%
Director	15%
Manager	23%
Supervisor	12%
Technician/Staff	44%
Consultant	3%
Other	1%
Total	100%

Q3. What best describes the full-time headcount of your global organization?	Pct%	
1,001 to 5,000	44%	
5,001 to 10,000	23%	
10,001 to 25,000	18%	
25,001 to 75,000	9%	
Over 75,000	6%	Headcount
Total	100%	15,495

Q4. What best describes your organization's primary industry classification?	Pct%
Communications	2%
Consumer products	3%
Education & research	4%
Energy & utilities	4%
Financial services	19%
Healthcare	11%
Hospitality	4%
Industrial & manufacturing	6%
Life sciences	6%
Public sector	11%
Retail	10%
Services	9%
Technology & software	7%
Transportation	3%
Other	1%
Total	100%

Part 4. Estimating forensic workflows

Please estimate the number of IT security investigations involving forensic experts and/or specialized forensic tools in the past 12 months?		
Q5a. Suspected network attacks	Pct%	
Less than 1	0%	
1 to 5	12%	
6 to 10	20%	
11 to 20	30%	
21 to 50	21%	
More than 50	17%	Past year
Total	100%	23.2

Q5b. Suspected security breaches	Pct%	
Less than 1	0%	
1 to 5	44%	
6 to 10	15%	
11 to 20	15%	
21 to 50	19%	
More than 50	7%	Past year
Total	100%	15.3

Q5c. Suspected insider attack	Pct%	
Less than 1	12%	
1 to 5	25%	
6 to 10	28%	
11 to 20	23%	
21 to 50	9%	
More than 50	3%	Past year
Total	100%	11.3

Q6a. Approximately, what percent of network attacks investigated by the IT security team are proven to be actual attacks?	Pct%	
Less than 10%	43%	
10 to 25%	41%	
26 to 50%	11%	
51 to 75%	4%	
76 to 100%	1%	Proven attacks
Total	100%	19%

Q6b. Approximately, what percent of security breaches investigated by the IT security team are proven to be actual attacks?	Pct%	
Less than 10%	29%	
10 to 25%	28%	
26 to 50%	21%	
51 to 75%	15%	
76 to 100%	7%	Proven attacks
Total	100%	31%

Q6c. Approximately, what percent of insider attacks investigated by the IT security team are proven to be actual attacks?	Pct%	
Less than 10%	5%	
10 to 25%	12%	
26 to 50%	37%	
51 to 75%	23%	
76 to 100%	23%	Proven attacks
Total	100%	51%

The following tables contain the "typical" workflow relating to an IT security investigation. Please allocate all 100 points to each workflow category based on the time incurred to complete one investigation.	
Q7a. Network attacks	Allocated
Detection	35
Escalation	7
Containment	17
Recovery	35
Post mortem	6
Total	100

Q7b. Security breaches	Allocated
Detection	37
Escalation	5
Containment	21
Recovery	32
Post mortem	5
Total	100

Q7c. Insider attack	Allocated
Detection	30
Escalation	8
Containment	22
Recovery	32
Post mortem	8
Total	100

Q8a. Approximately, how much forensic investigative time is required to complete one investigation regarding a suspected network attack?	Pct%	
Less than 1 hour	2%	
1 to 4 hours	15%	
5 to 8 hours	33%	
1 to 2 days	23%	
2 to 5 days	11%	
More than 5 days	16%	Hours
Total	100%	43.1

Q8b. Approximately, how much forensic investigative time is required to complete one investigation regarding a suspected security breach?	Pct%	
Less than 1 hour	3%	
1 to 4 hours	8%	
5 to 8 hours	21%	
1 to 2 days	25%	
2 to 5 days	23%	
More than 5 days	20%	Hours
Total	100%	58.7

Q8c. Approximately, how much forensic investigative time is required to complete one investigation regarding insider attack?	Pct%	
Less than 1 hour	0%	
1 to 4 hours	4%	
5 to 8 hours	18%	
1 to 2 days	28%	
2 to 5 days	21%	
More than 5 days	29%	Hours
Total	100%	70.8

Q9a. Approximately, how long does it take to complete one forensic investigation from detection to containment for a network attack?	Pct%	
Less than 1 day	0%	
1 to 2 days	37%	
3 to 5 days	36%	
6 to 10 days	20%	
More than 10 days	7%	Man-days
Total	100%	4.4

Q9b. Approximately, how long does it take to complete one forensic investigation from detection to containment for a security breach?	Pct%	
Less than 1 day	0%	
1 to 2 days	11%	
3 to 5 days	31%	
6 to 10 days	38%	
More than 10 days	20%	Man-days
Total	100%	6.8

Q9c. Approximately, how long does it take to complete one forensic investigation from detection to containment for an insider attack?	Pct%	
Less than 1 day	0%	
1 to 2 days	10%	
3 to 5 days	12%	
6 to 10 days	22%	
More than 10 days	56%	Man-days
Total	100%	9.1

Q10a. Approximately, what percent of forensic investigations involving a suspected network attack are conducted by outside experts (consultants) rather than in-house staff?	Pct%	
Less than 10%	33%	
10 to 25%	21%	
26 to 50%	11%	
51 to 75%	16%	
76 to 100%	19%	% External
Total	100%	37%

Q10b. Approximately, what percent of forensic investigations involving a suspected security breach are conducted by outside experts (consultants) rather than in-house staff?	Pct%	
Less than 10%	30%	
10 to 25%	17%	
26 to 50%	12%	
51 to 75%	10%	
76 to 100%	31%	% External
Total	100%	44%

Q10c. Approximately, what percent of forensic investigations regarding a suspected data loss scenario are conducted by outside experts (consultants) rather than in-house staff?	Pct%	
Less than 10%	42%	
10 to 25%	25%	
26 to 50%	10%	
51 to 75%	9%	
76 to 100%	14%	% External
Total	100%	30%

Part 5. Network forensic skills and practices

Q11. Does your organization assign forensics investigations to a particular member of the IT security team?	Pct%
Yes	71%
No	29%
Total	100%

Q12. On average, what best describes the experience level (in years) of individuals who are responsible for investigating suspected cyber attacks or breaches for your organization?	Pct%	
Less than 2 years	0%	
2 to 4 years	15%	
5 to 8 years	35%	
9 to 15 years	32%	
More than 15 years	18%	Years
Total	100%	9.4

Q13. Do forensic investigators/analysts undergo specialized technical training?	Pct%
Yes	75%
No	25%
Total	100%

Q14. Approximately, what percent of forensic investigators/analysts employed by your organization have advanced degrees and/or certifications in cybersecurity or other related fields?	Pct%	
Less than 10%	7%	
10 to 25%	15%	
26 to 50%	23%	
51 to 75%	15%	
76 to 100%	40%	% degreed
Total	100%	56%

Q15. How often does the IT security team employ forensic intelligence/analysis tools to assist with investigations regarding network attacks and security breaches?	Pct%
All investigations	44%
Most investigations	40%
Some investigations	11%
Few investigations	5%
None	0%
Total	100%

Q16. Are your forensic tools integrated within a broader suite of IT security solutions such as SIEM ?	Pct%
Yes	40%
No	60%
Total	100%

Q17. Does your security team receive alerts that would provide guidance regarding current threats to forensic investigators?	Pct%
Yes	44%
No	56%
Total	100%

Q18. Do you believe your forensics search efforts deliver sufficient evidence to effectively prosecute the instigators of a network attack or data loss?	Pct%
Yes, most cases	25%
Yes, some cases	44%
No	31%
Total	100%

Q19. Does your organization currently collect packet captures as part of its IT security analytical capabilities?	Pct%
Yes	69%
No (skip)	31%
Total	100%

Q20. Where does your organization collect full packet capture from the network? Full packet capture refers to the process of intercepting and logging all network (both header and payload) traffic.	Pct%
At data centers	40%
At all network egress points	29%
Pervasively throughout the network	20%
Other (please specify)	11%
Total	100%

Q21. How many days of full packet capture is your organization storing?	Pct%	
None	0%	
Less than 1 day	14%	
About 1 day	45%	
About 1 week	16%	
About 1 month	22%	
More than 1 month	3%	
Other (please specify)	0%	Man-days
Total	100%	9.7

Q22. Does your current solution allow you to maintain packet capture evidence over a sustained period of time (i.e., months or years)?	Pct%
Yes	33%
No	67%
Total	100%

Q23. Approximately how long can your current resources retain raw network packet captures (maximum capacity)?	Pct%	
About 1 week	11%	
About 1 month	27%	
About 6 months	36%	
About 1 year	20%	
More than 1 year	6%	Man-days
Total	100%	174.1

Q26. Do your organization's incident investigations result in the production of threat indicators, which are then used to defend the organization from future attacks?	Pct%
Yes	56%
No	38%
Unsure	6%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.