Threat Intelligence & Incident Response: A Study of EMEA Organizations

Sponsored by AccessData

Independently conducted by Ponemon Institute LLC

Publication Date: March 2014

Threat Intelligence & Incident Response:
A Study of EMEA Organizations

Presented by Ponemon Institute, March 2014

Part 1. Introduction

When a cyber attack or other security incident occurs, CISOs and their security teams must be able to explain the details of the incident to senior management. Often without being given the time to gather the necessary intelligence to provide an accurate assessment of the problem.

Sponsored by AccessData, we are pleased to present the findings of *Threat Intelligence & Incident Response: A Study of EMEA Organizations*[1]. Ponemon Institute surveyed 521 IT and IT security practitioners in EMEA who are involved in handling security and incident response for their company.

We asked respondents what they would do if their company had a cyber attack and the CEO and board of directors wanted a briefing on what happened. The meeting is called so soon after the incident that they are not able to have all the facts. Would they say everything is under control or ask for more time to investigate? While 22 percent say they would need more time, 33 percent would say it's been resolved. In any event, 50 percent of respondents say most CISOs, probably because of fears of the reaction from the CEO and board, would modify, filter or water-down their report.

Why threat intelligence is important

The recent Target data breach and the circumstances surrounding the detection and remediation of the incident makes the case for the importance of having threat intelligence processes in place. In his testimony before a Senate committee, Target's Chief Financial Officer John Mulligan stated that the security breach affecting up to 110 million holiday shoppers lasted three days longer than previously thought. The malicious software that enabled hackers to steal information from credit and debit cards from November 27 to December 15 was later found on 25 additional checkout machines and continued to collect shoppers' information for three more days. On December 27, Target also acknowledged contrary to early reports that personal identification numbers to debit and credit cards were also exposed.

Following are some of the most interesting findings:

- An average of 29 percent of all cyber attacks are undetected.
- Seventy-nine percent of respondents say detection of a cyber attack takes too long and 80 percent say there is little or no prioritization of incidents.
- Forty-five percent of respondents say their security products do not support the import of threat intelligence from other sources.
- Fifty-one percent of respondents do not believe their security team has sufficient skills to investigate and remediate a security incident.
- Thirty-six percent of respondents say it could take a year to know the root cause of a cyber attack and 43 percent of respondents say their organizations will never know with certainty.
- Eighty-six percent of respondents rate the investigation of mobile devices as difficult.
- Sixty-one percent of respondents say they are not able to conduct investigation on mobile devices in response to e-discovery requests or they are unsure. In the case of being able to locate sensitive data on mobile devices, 56 percent say they are not able to or are unsure.

[1] A separate report presents both U.S. and EMEA findings: *Threat Intelligence & Incident Response: A Study of U.S. and EMEA Organizations,* sponsored by AccessData and conducted by Ponemon Institute, February 2014.

Part 2. Key findings

Following is an analysis of the key findings based on responses from EMEA IT and IT security practitioners. The complete audited findings are presented in the appendix of the report.

The main themes of the research are:

- The use of threat intelligence to defend against cyber attacks
- The current state of incident response
- Getting to the root cause is critical to stopping future attacks
- Mobility and e-discovery

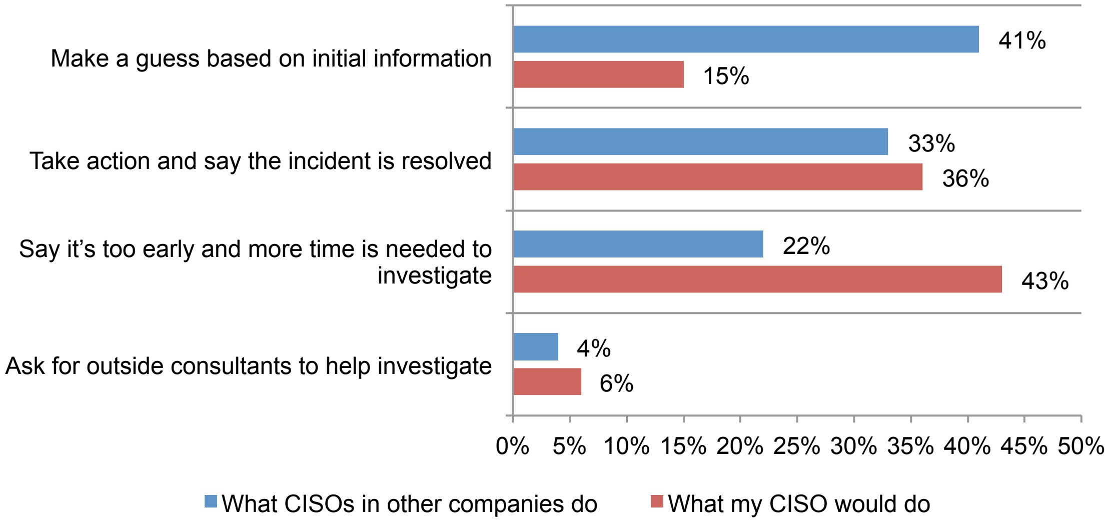
The use of threat intelligence to defend against cyber attacks

A lack of threat intelligence puts CISOs jobs at risk. In this study, we asked respondents to imagine what has become an increasingly common scenario. The organization has a security incident and the CEO and board want an explanation and impact assessment. Unfortunately, the meeting is called before the CISO and the security team have a complete picture of the causes and effects of the incident.

As shown in Figure 1, most respondents say CISOs in other organization would feel forced to take a best effort guess with the initial information they have or take immediate action on what is known and tell the CEO it's been taken care of and resolved.

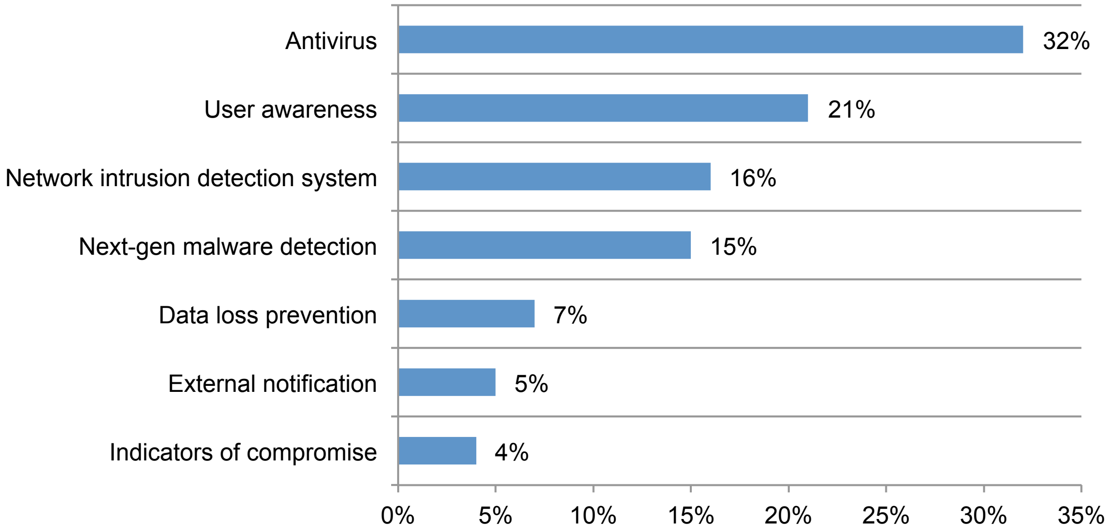
The same figure reports what respondents think they would do. In this case, only 15 percent say they would make a guess. Forty-three percent would be courageous enough to say it is too early to understand what happened and more time is needed. In any event, 50 percent of respondents say most CISOs, probably because of fears of the reaction from the CEO and board, would modify, filter or water-down their report.

Figure 1. What do you tell the CEO & Board about the cyber attack?



Cyber attacks go undetected. On average, 29 percent of all security incidents and cyber-attacks are never detected. As shown in Figure 2, most respondents say their organization normally uses antivirus solutions to detect security incidents followed by user awareness and network intrusion detection systems.

Figure 2. Security team's methods for detecting security incidents



In defending their organizations against cyber attacks, respondents say comprehensive endpoint, network and logfile visibility is very important. While only 24 percent of organizations in this study use a next generation security solution to contain or remediate cyber attacks, most say it is able to detect and prevent cyber attacks.

Current security products make it difficult to import and use threat intelligence. Fifty-five percent of respondents say external threat intelligence is the most valuable. However, 57 percent say they are not able to efficiently and effectively use threat intelligence with their existing security products. As shown in Figure 3, 45 percent say none of their security products support imported threat intelligence and another 38 percent say if they do import threat intelligence it is only used by some of their security products.

Figure 3. The ability to import and utilize threat intelligence with your existing security products

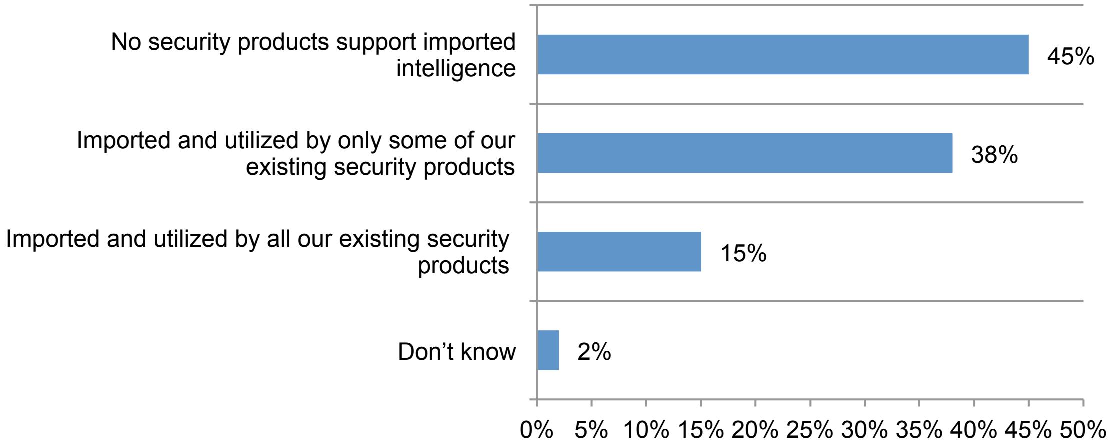
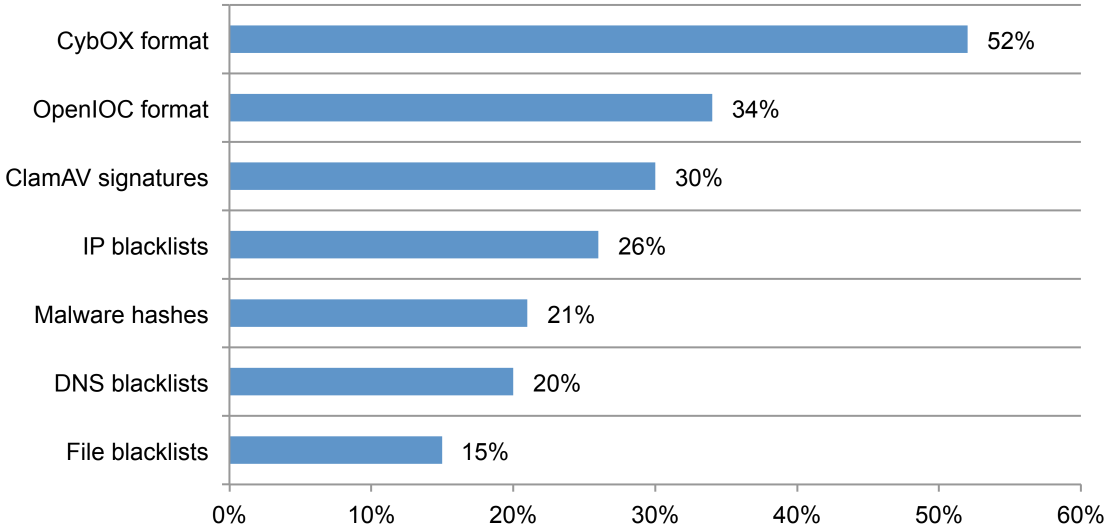


Figure 4 shows the threat intelligence data types organizations are able to import across their existing security products.

Figure 4. Imported threat intelligence data types currently utilized
More than one response permitted

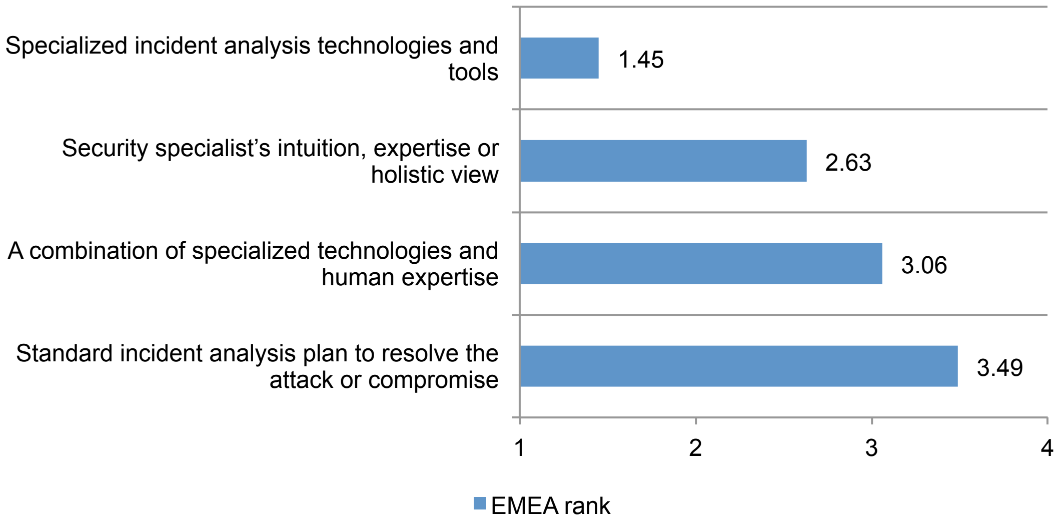


The current state of incident response

Incident analysis technologies and tools have the greatest value when a cyber attack occurs. As shown in Figure 5, respondents rank the quantitative approach offered by specialized incident analysis technologies and tools as most important when analyzing and remediating a cyber attack. This is followed by a security specialist's intuition, expertise or holistic view.

Despite the use of these technologies or processes, 51 percent of respondents do not feel their security team has sufficient skills to effectively investigate and remediate sophisticated cyber attacks.

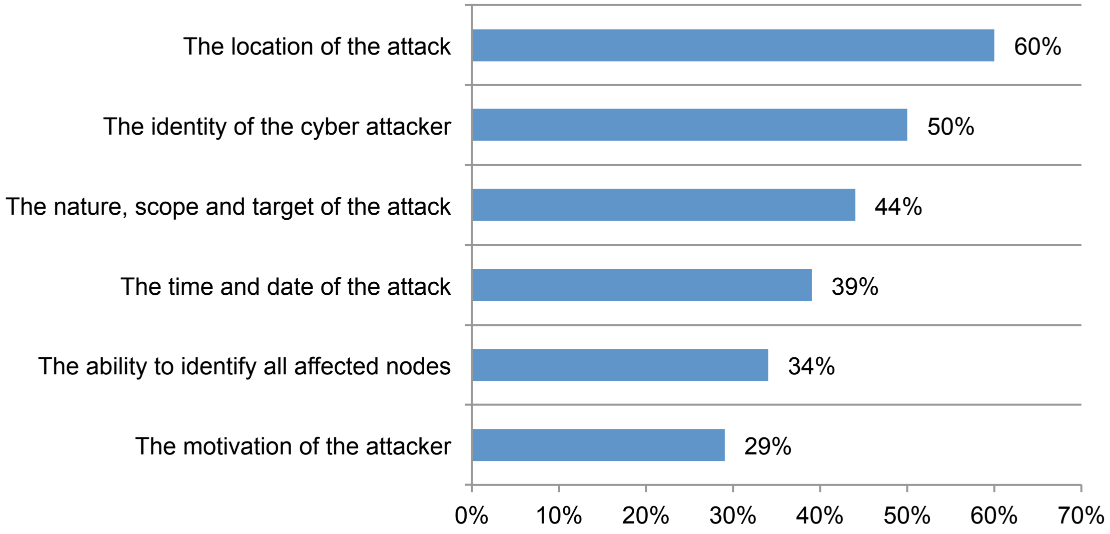
Figure 5. Important factors in analyzing and remediating a cyber attack
1 = most important to 4 = least important



Many companies succeed in knowing the location and identity of the cyber attacker. Sixty percent of respondents say they are able to know the "where" of the attack and 50 percent say they know the "who", according to Figure 6. They are not as good at identifying all affected nodes and the motivation or purpose of the attacker.

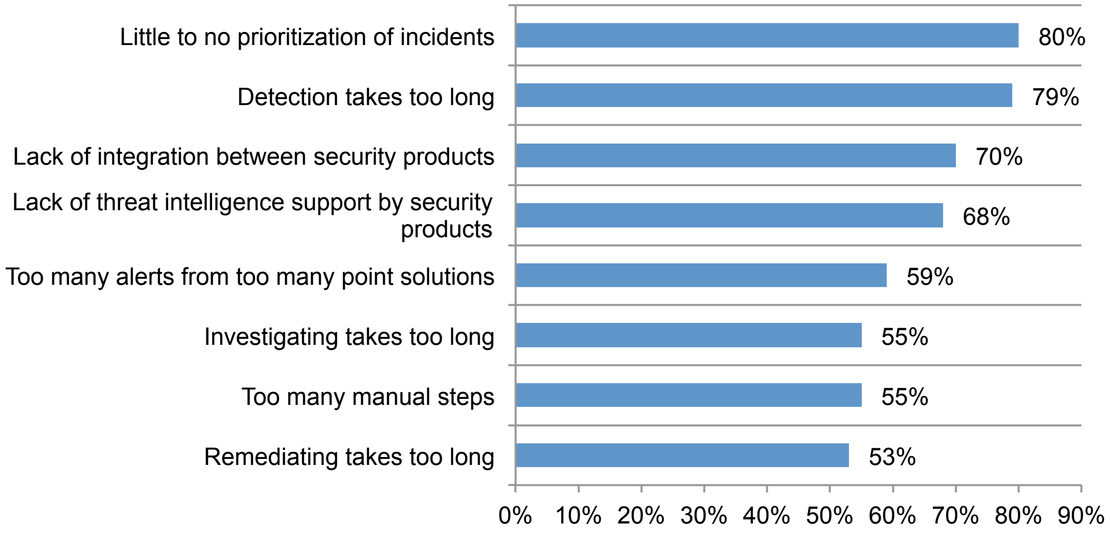
On average, respondents say 44 percent of all security incidents and alerts are capable of being handled automatically without human intervention and an average of 16 percent of all security incidents and alerts are considered high priority by the security team.

Figure 6. Ability to determine the "who, what, where, when and why" of security alerts
Very strong and strong response combined



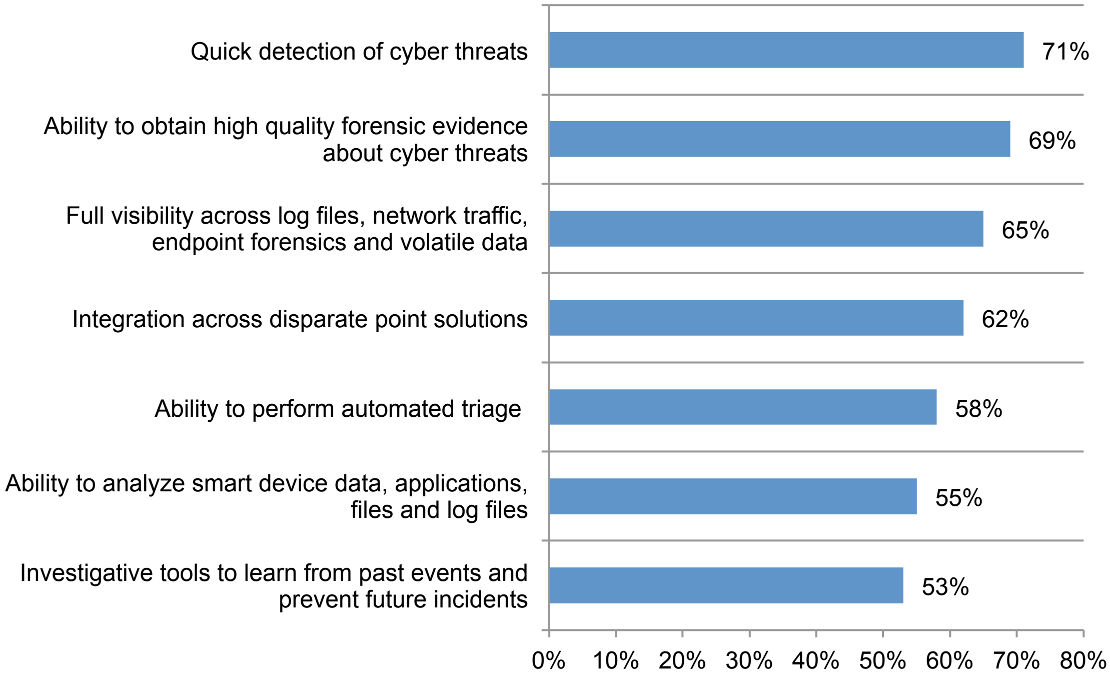
Detection takes too long to enable a quick and thorough incident response. Figure 7 shows all the factors that negatively impact the ability to respond to security incidents quickly and thoroughly. By far the biggest problems are the lack of prioritization of incidents and the time it takes to detect an incident. Other negatives are lack of integration between security products and lack of threat intelligence support by security products.

Figure 7. Factors that negatively impact the ability to respond to security incidents
Very significant and significant response combined



High quality forensic evidence about cyber threats is essential. Respondents consistently say that detection is not happening fast enough (71 percent). As a solution, 69 percent would like the ability to have high quality forensic evidence about cyber threats, as presented in Figure 8.

Figure 8. Solutions important to incident response
Essential and very important response combined

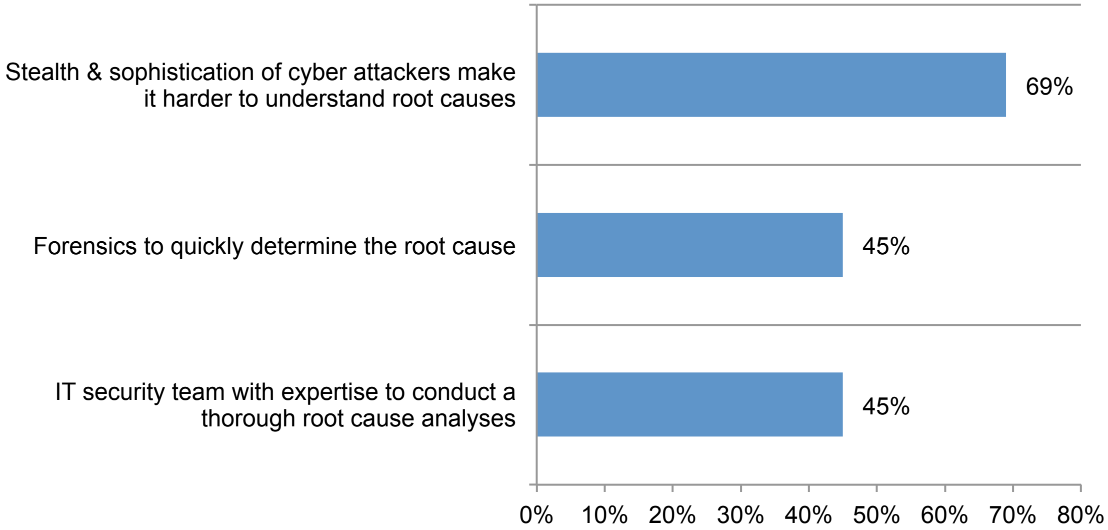


Also important is full visibility across log files, network traffic, endpoint forensics and volatile data (65 percent of respondents). This is followed by the ability integrate across disparate point solutions (62 percent of respondents).

Getting to the root cause is critical to stopping future attacks

Organizations cannot know with certainty the root causes of security alerts and cyber attacks. Forty-three percent of respondents say their organizations will never know with certainty what caused the security incident and 36 percent say it could take a year. The main barrier to understanding the root cause, as shown in Figure 9, is the increasing stealth and/or sophistication of cyber attackers.

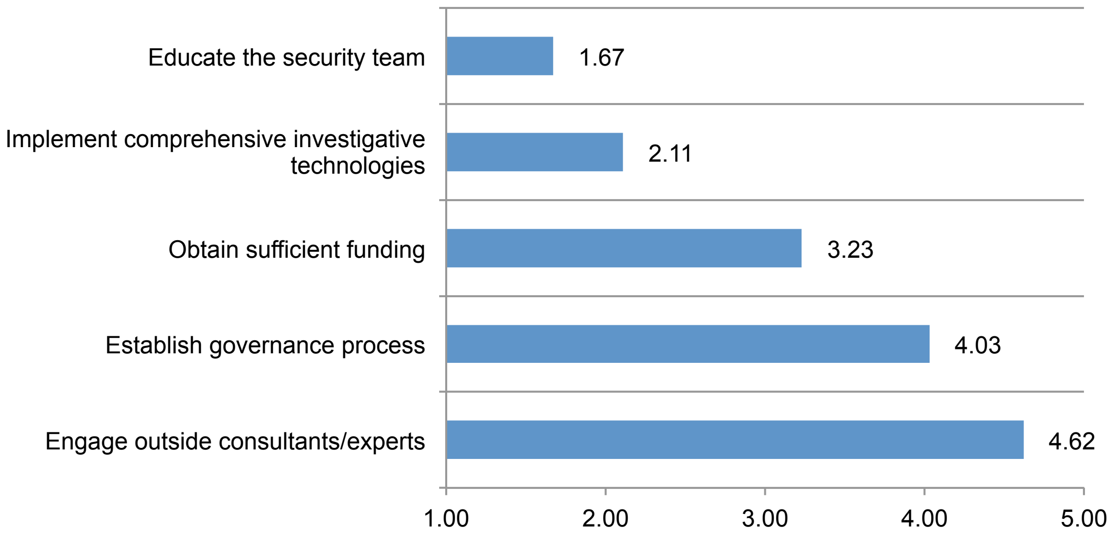
Figure 9. Perceptions about understanding the root cause of security incidents
Strongly agree and agree response combined



Less than half of respondents say their organizations have the forensic technologies or tools to quickly determine the root cause of most cyber attacks it experiences (45 percent of respondents) or a security team that has the forensic skills, knowledge and expertise to conduct thorough root cause analyses (45 percent).

An educated security team can improve the certainty of root cause. Understanding the root causes of cyber attacks increases an organization's ability to respond to future attacks, according to 65 percent of respondents. To achieve this objective, respondents rated education and the implementation of comprehensive investigative technologies as most important followed by having the funding to invest in these solutions, according to Figure 10.

Figure 10. Steps to strengthen the ability to determine root causes of security incidents
1 = most important to 5 = least important

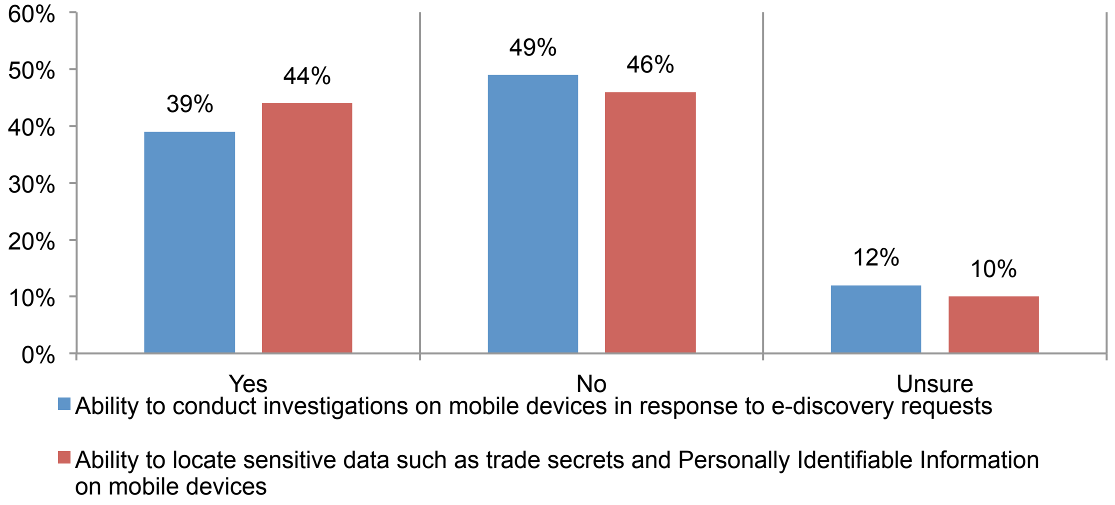


Mobility and e-discovery

Mobile devices are really hard to investigate after a security incident. Eighty-five percent of respondents rate the investigation of mobile devices as difficult. The level of difficulty to investigate mobile devices averages about 8 on a scale of 1 = not difficult to 10 = very difficult.

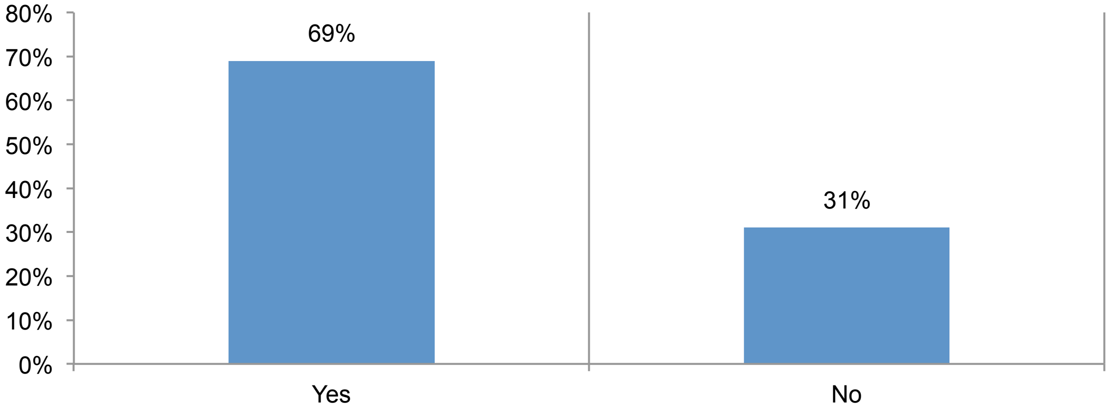
According to Figure 11, 61 percent say they are not able to conduct investigations on mobile devices in response to e-discovery requests or they are unsure (49 + 12 percent). In the case of being able to locate sensitive data such as trade secrets and personally identifiable information (PII) on mobile devices, 56 percent say they are not able to or are unsure (46 + 10 percent).

Figure 11. Are you able to respond to e-discovery requests and locate sensitive data on mobile devices?



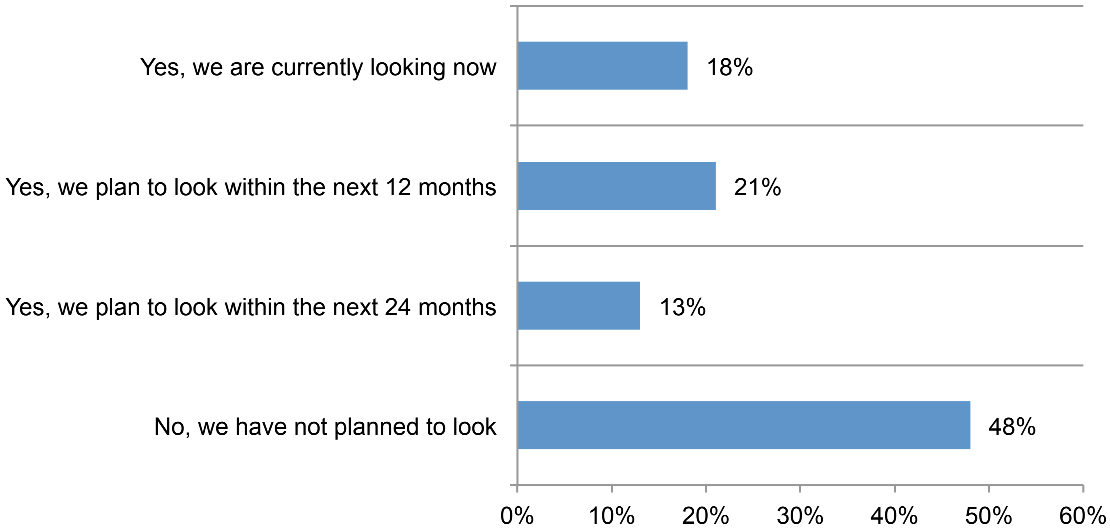
Most security teams would like to include e-discovery capabilities. Sixty-three percent of respondents say their organization's security team responds to e-discovery issues**.** As shown in Figure 12, because of this level of involvement, 69 percent say they would find value in a combined security, internal investigation and e-discovery platform that works seamlessly across business units.

Figure 12. Is a combined security, internal investigations and e-discovery platform valuable?



Fifty-two percent of respondents (18 + 21+ 13 percent) say they are expanding their current incident response products to include e-discovery capabilities.

Figure 13. Will you expand current incident response products to include e-discovery capabilities?



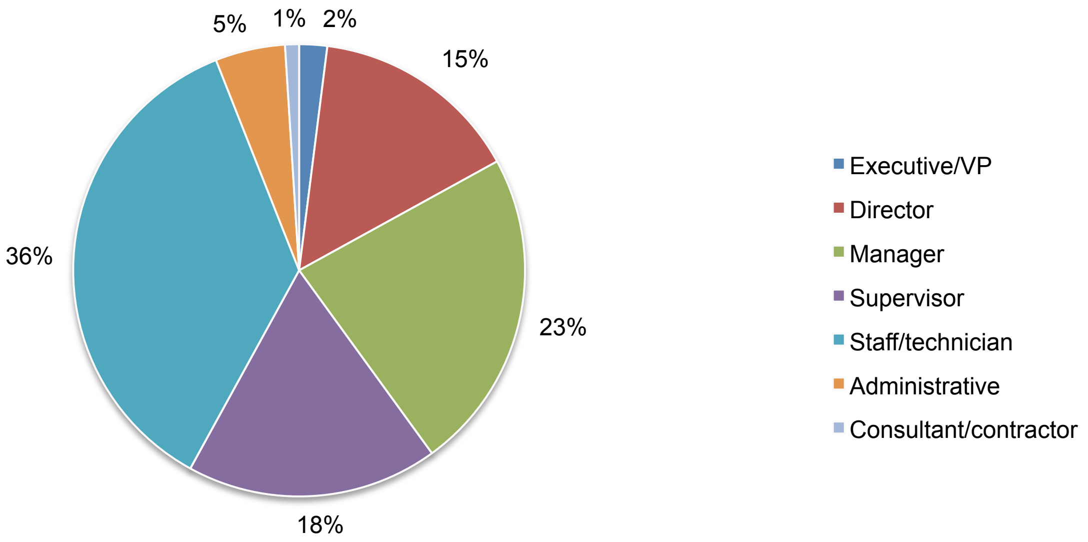
Part 3. Methods

A random sampling frame of 14,595 IT and IT security practitioners located in the EMEA were selected as participants to this survey. As shown in Table 1, 597 respondents completed the survey. Screening and failed reliability checks removed 76 surveys. The final sample was 521 surveys (or a 3.6 percent response rate).

Table 1. Sample response	Freq.	Pct%
Total sampling frame	14,595	100.0%
Total returns	597	4.1%
Rejected and screened surveys	76	0.5%
Final sample	521	3.6%

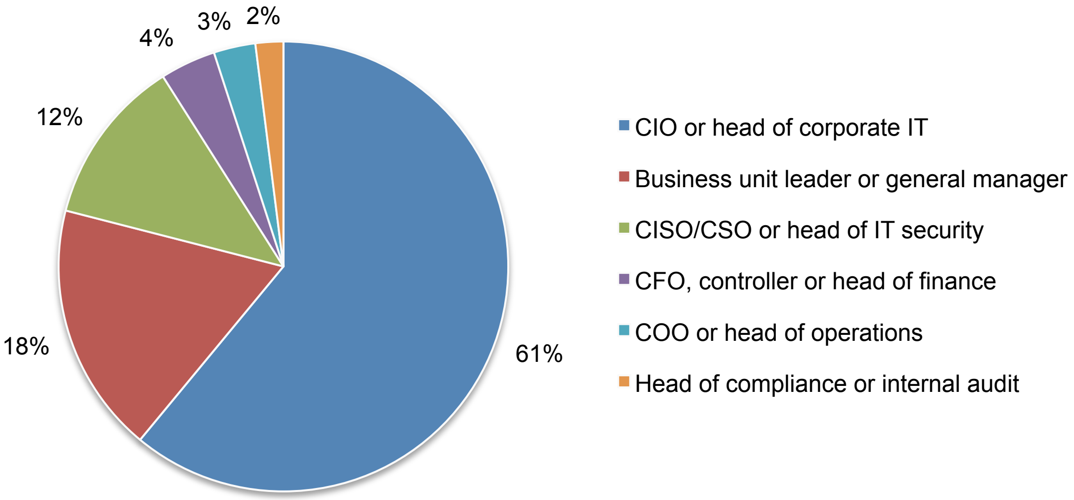
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 58 percent of respondents are at or above the supervisory levels.

Pie Chart 1. What organizational level best describes your current position?



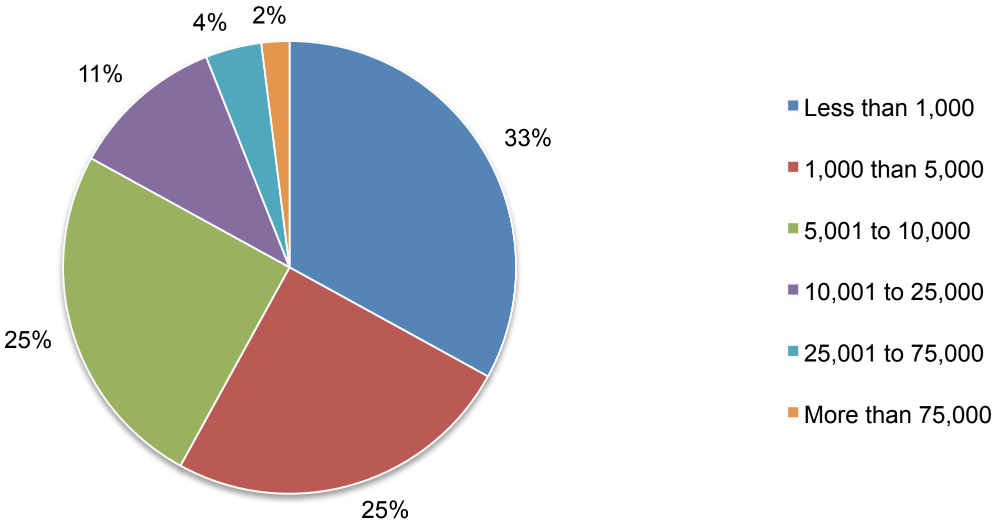
Pie Chart 2 reports the respondent's direct reporting channel. Sixty-one percent of respondents report to the CIO or head of corporate IT and 18 percent report to the business unit leader.

Pie Chart 2. What best describes your direct reporting channel?



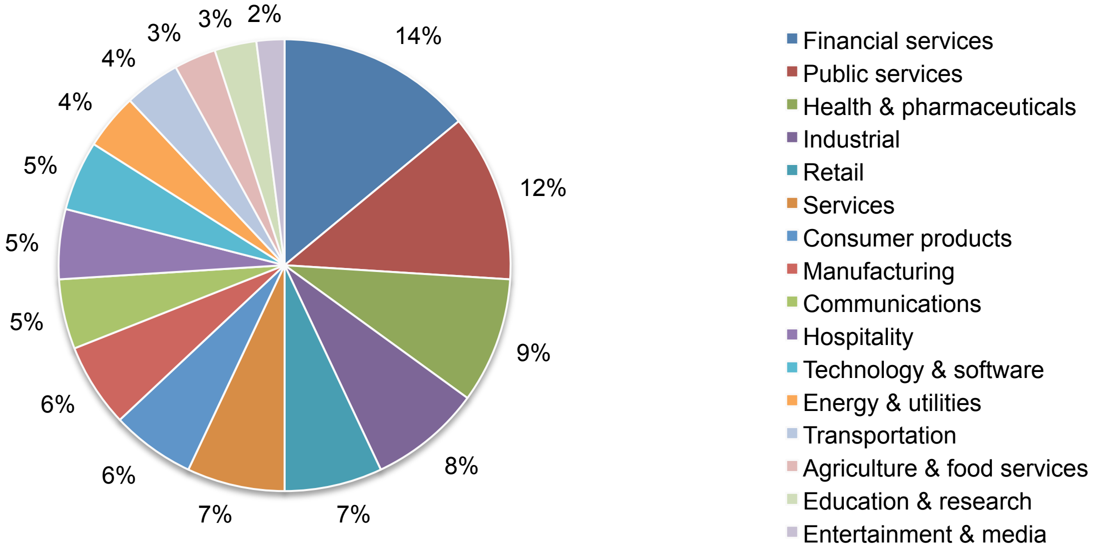
As shown in pie chart 3, 67 percent of respondents are from organizations with a worldwide headcount of 1,000 or more employees.

Pie chart 3. Worldwide headcount of the organization



Pie Chart 4 reports the industry segments of respondents' organizations. This chart identifies financial services (14 percent) as the largest segment, followed by public services (12 percent) and health & pharmaceuticals (9 percent).

Pie Chart 4. Industry distribution of respondents' organizations



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 in the EMEA who are involved in handling security and incident response for their company. 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 holdout 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 a truthful response.

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 January 2014.

Sample response	EMEA*
Total sample frame	14,595
Total returns	597
Rejected and screened surveys	76
Final sample	521
Response rate	3.6%

*EMEA sample contains respondents located in 21 countries within this region

Screening

S1. What best describes your level of involvement in handling security and incident response for your company?	EMEA
Very significant involvement	26%
Significant involvement	36%
Some involvement	38%
Minimal or no involvement (stop)	0%
Total	100%

Part 1. Threat intelligence & incident resolution

Q1a. Do you investigate the majority of security alerts **thoroughly to your satisfaction**?	EMEA
Yes	55%
No	45%
Total	100%

Q1b. If not, why? Choose only one primary reason.	EMEA
Lack of reliable products	36%
Lack of in-house expertise or knowledge	26%
Pressure to remediate quickly	29%
Rely on automated remediation (e.g. Antivirus quarantining)	9%
Total	100%

Q2. Do you feel that your security team has sufficient skills to effectively investigate and remediate sophisticated cyber-attacks and compromises?	EMEA
Yes	49%
No	51%
Total	100%

Q3. How important are the following factors in analyzing and remediating a cyber attack? Please rank the choices below from 1 = most important to 4 = least important.	EMEA rank
Standard incident analysis plan to resolve the attack or compromise (one size fits all)	3.49
Specialized incident analysis technologies and tools (quantitative approach)	1.45
Security specialist’s intuition, expertise or holistic view (qualitative approach)	2.63
A combination of specialized technologies and human expertise	3.06
Average	2.91

Imagine this. An organization had a cyber-attack. The CEO and board of directors want the CISO to brief them on the details and how it impacts their company. Unfortunately, the CISO does not have the necessary facts in time for the meeting.

Q4. What do you think CISOs at **most companies** would do in this situation? Please select one best response.	EMEA
Take a best effort guess based on initial information they do know	41%
Tell them it's still too early to understand what happened and more time is needed	22%
Take immediate action on what is known and tell the CEO it's been taken care of	33%
Tell the CEO that due to the lack of people and internal resources, it's best to bring in incident response consultants to investigate	4%
Total	100%

Q5. What would **you and your** security team do? Please select one best response.	EMEA
Take a best effort guess based on the initial information I/we do know	15%
Tell them it's still too early to understand what happened and more time is needed	43%
Take immediate action on what is known and tell the CEO it's been taken care of	36%
Tell the CEO that due to the lack of people and internal resources, it's best to bring in incident response consultants to investigate	6%
Total	100%

Q6. When providing this update to the CEO, would CISOs at **most companies** have the results modified, filtered or watered-down?	EMEA
Yes, almost always	16%
Yes, some of the time	34%
No	50%
Total	100%

Q7. How important is comprehensive endpoint, network and logfile visibility to your organization's defense against cyber-attacks? 1 = low importance to 10 = high importance.	EMEA
1 to 2	2%
3 to 4	3%
5 to 6	15%
7 to 8	23%
9 to 10	57%
Total	100%
Extrapolated average	8.10

Q8. Please rate your organization's ability to determine the "who, what, where, when and why" of security alerts or cyber-attacks experienced. Percentage of respondents who rate their ability as strong or very strong.	EMEA
Who: knowing the identity of the cyber attacker	50%
What: knowing the nature, scope and target of the attack	44%
Where: knowing the location of the attack	60%
When: knowing the time and date of the attack	39%
Why: knowing the motivation or purpose of the attacker	29%
What: knowing the ability to identify all affected nodes	34%

Q9. What percentage of all security alerts and cyber-attacks experienced by your organization are you able to know with certainty the root causes? Percentage of respondents who say they can reach a definitive conclusion in a given timeframe.	EMEA
Within one day	8%
Within one week	15%
Within one month	24%
Within one year	36%
Never know with certainty	43%

Q10. What percentage of all security incidents and cyber-attacks experienced by your organization do you think are never detected? Please provide your best estimate.	EMEA
Zero/None	8%
1 to 10%	30%
11 to 25%	25%
26 to 50%	13%
51 to 75%	11%
76 to 100%	13%
Total	100%
Extrapolated percentage values	29%

Please rate the following seven (5) statements using the five-point scale provided below each item. The combined strongly agree and agree response is shown.	EMEA
Q11. My organization has the forensic technologies or tools to quickly determine the root causes of most cyber attacks it experiences.	45%
Q12. My organization's IT security personnel possess the forensic skills, knowledge and expertise to conduct thorough root cause analyses.	45%
Q13. Understanding the root causes of cyber attacks strengthens my organization's readiness to future attacks.	65%
Q14. Determining the root causes of cyber attacks is becoming more difficult because of the increasing stealth and/or sophistication of cyber attackers.	69%
Q15. Determining the root causes of cyber attacks is becoming more difficult because of the trend for employees to use their personally owned mobile devices in the workplace (a.k.a. BYOD).	48%

Q16. How does your organization's security team normally detect security incidents? Please respond to this question by allocating points in the following table. Note that the sum of your allocation must equal 100 points.	EMEA points
Antivirus	32
Next-gen malware detection	15
Indicators of compromise	4
Network Intrusion Detection System	16
Data Loss Prevention	7
User awareness	21
External notification	5
Total	100

Q17a. Does your organization use a next generation security solution to contain or remediate cyber attacks?	EMEA
Yes	24%
No	76%
Total	100%

Q17b. If you use a next gen malware detection solution what does it accomplish? Please select all that apply.	EMEA
Detects cyber attacks	88%
Prevents cyber attacks	81%
Contains cyber attacks	21%
Remediates cyber attacks	12%

Q18. Are your most valuable threat intelligence from internal or external sources?	EMEA
Internal	41%
External	55%
Don't Know	4%
Total	100%

Q19. Are you able to **efficiently and effectively** utilize threat intelligence with your existing security products?	EMEA
Yes	43%
No	57%
Total	100%

Q20. Which best describes your ability to import and utilize threat intelligence with your existing security products?	EMEA
Threat intelligence is automatically imported and utilized by all our existing security products	15%
Threat intelligence is automatically imported and utilized by only some of our existing security products	38%
None of our security products support imported threat intelligence	45%
Don't know	2%
Total	100%

Q21. Which of the imported threat intelligence data types are you able to import and utilize across your existing security products? Please select all that apply.	EMEA
OpenIOC format	34%
CybOX format	52%
ClamAV signatures	30%
Malware hashes	21%
IP blacklists	26%
DNS blacklists	20%
File blacklists (e.g. file name and size)	15%
Total	198%

Part 2. Mobile and e-discovery issues

Q22. Detail the mix of company owned vs. BYOD mobile devices used across your company. Allocate the proportion of phones used by each segment, which must total 100 points.	EMEA points
Company provides mobile devices (tablets, smart phones and standard mobile phones) for work use	34
Employees use their personal mobile devices for work use (BYOD)	66
Total	100

Q23a. Are you able to conduct investigations on mobile devices in response to security incidents?	EMEA
Yes	61%
No	37%
Unsure	2%
Total	100%

Q23b. If yes, are you able to investigate mobile devices as part of an enterprise-wide live incident response investigation (review multiple running endpoints simultaneously)?	EMEA
Yes	40%
No	56%
Unsure	4%
Total	100%

Q23c.If yes, are you able to review mobile applications and social media activity?	EMEA
Yes	44%
No	52%
Unsure	4%
Total	100%

Q24. Do you find the investigation of mobile devices difficult to conduct? Please rate level of difficulty using the following 10-point scale. Not difficult = 1 to Very difficult to 10.	EMEA
1 to 2	1%
3 to 4	3%
5 to 6	11%
7 to 8	35%
9 to 10	50%
Total	100%
Extrapolated average	8.10

Q25. Are you able to conduct investigations on mobile devices in response to e-discovery requests?	EMEA
Yes	39%
No	49%
Unsure	12%
Total	100%

Q26. Are you able to locate sensitive data such as trade secrets and Personally Identifiable Information (PII) on mobile devices?	EMEA
Yes	44%
No	46%
Unsure	10%
Total	100%

Q27. What steps could your organization take **to strengthen its ability** to determine the root cause of security incidents? Please rank the following list from 1 = most important to 5 = least important.	EMEA Rank
Implement comprehensive investigative technologies	2.11
Educate the security team	1.67
Engage outside consultants/experts	4.62
Establish governance process	4.03
Obtain sufficient funding	3.23
Average	3.13

Q28. How has your organization's spending level on security incident analysis changed over the past 12 months?	EMEA
Increased	39%
Stayed at the same level	53%
Decreased	8%
Total	100%

Q29a. Do you believe your organization is in a state of "continuous compromise" to at least some degree including mass malware and botnets?	EMEA
Yes	63%
No	30%
Unsure	7%
Total	100%

Q29b. Does continuous compromise affect security policies and procedures employed within your organization?	EMEA
Yes	65%
No	31%
Unsure	4%
Total	100%

Q29c. If yes (Q29b), how has it impacted the approach taken by your organization? Please select all that apply.	EMEA
Increases the need for experts	55%
Increases the need for investigative technologies	68%
Changes the composition of security team members	47%
Raises the need for employee awareness	45%
Increases the need for resources/budget	55%
Other (please specify)	5%
Total	275%

Q31. What factors negatively impact the ability to respond to security incidents quickly and thoroughly? Please rate the following items using the five-point scale from very significant impact to no impact . The combined very significant and significant impact is reported.	EMEA
Too many alerts from too many point solutions	59%
Too many manual steps	55%
Detection takes too long	79%
Investigating takes too long	55%
Remediating takes too long	53%
Little to no prioritization of incidents	80%
Lack of integration between security products	70%
Lack of threat intelligence support by security products	68%
Average	65%

Please rate the following capabilities in terms of importance to your overall incident response needs using a five-point scale from essential to irrelevant. The combined essential and very iimportant response is reported.	EMEA
Q32. Full visibility across log files, network traffic, endpoint forensics and volatile data	65%
Q33. Ability to integrate across disparate point solutions	62%
Q34. Ability to quickly detect of cyber threats	71%
Q35. Ability to obtain high quality forensic evidence about cyber threats (low false positive rate)	69%
Q36. Investigative tools that learn from past events and prevent reoccurrences	53%
Q37. Ability to perform automated triage for cyber threats	58%
Q38. Ability to analyze smart device data, applications, files and log files	55%
Average	62%

Q39. In your opinion, what percentage of all security incidents and alerts are capable of being handled automatically (without human intervention)?	EMEA
None (0%)	5%
Less than 10%	6%
10 to 25%	19%
26 to 50%	30%
51 to 75%	23%
76 to 99%	17%
All (100%)	0%
Total	100%
Extrapolated average percentage	44%

Q40. In your opinion, what percentage of all security incidents and alerts are considered high priority by your security team?	EMEA
Less that 1%	16%
1 to 5%	21%
6 to 10%	25%
11 to 25%	19%
26 to 50%	13%
51 to 99%	5%
All (100%)	1%
Total	100%
Extrapolated average percentage	16%

Q41. In your opinion, are the security products used for security incident investigations appropriate for e-discovery as well?	EMEA
Yes	32%
No	55%
Unsure	13%
Total	100%

Q42. Is your organization’s security team involved in e-discovery operations?	EMEA
Yes	63%
No	36%
Unsure	1%
Total	100%

Q43. Would you find value in a combined security, internal investigations and e-discovery platform that works seamlessly across business units?	EMEA
Yes	69%
No	31%
Total	100%

Q44. Are you looking at expanding your current incident response products to include e-discovery capabilities?	EMEA
Yes, we are currently looking now	18%
Yes, we plan to look within the next 12 months	21%
Yes, we plan to look within the next 24 months	13%
No, we have not planned to look	48%
Total	100%

Part 3. Organization and respondents’ demographics

D1. What best describes your position level within the organization?	EMEA
Executive/VP	2%
Director	15%
Manager	23%
Supervisor	18%
Staff/technician	36%
Administrative	5%
Consultant/contractor	1%
Other	0%
Total	100%

D2. What best describes your direct reporting channel?	EMEA
CEO/executive committee	0%
COO or head of operations	3%
CFO, controller or head of finance	4%
CIO or head of corporate IT	61%
Business unit leader or general manager	18%
Head of compliance or internal audit	2%
CISO/CSO or head of IT security	12%
Other	0%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	EMEA
Less than 1,000	33%
1,000 than 5,000	25%
5,001 to 10,000	25%
10,001 to 25,000	11%
25,001 to 75,000	4%
More than 75,000	2%
Total	100%
Extrapolated global headcount	8,447

D4. What best describes your organization's primary industry classification?	EMEA
Agriculture & food services	3%
Communications	5%
Consumer products	6%
Defense	0%
Education & research	3%
Energy & utilities	4%
Entertainment & media	2%
Financial services	14%
Health & pharmaceuticals	9%
Hospitality	5%
Industrial	8%
Manufacturing	6%
Public services	12%
Retail	7%
Services	7%
Technology & software	5%
Transportation	4%
Other	0%
Total	100%

Countries in samples	EMEA
Austria	11
Belgium	21
Croatia	6
Czech Republic	8
France	51
Germany	74
Greece	7
Ireland	26
Israel	16
Italy	20
Netherlands	36
Poland	10
Russian Federation	34
Saudi Arabia	30
Scandanavia (Sweden, Denmark, Norway and Finland)	17
South Africa	16
Spain	33
Switzerland	12
Turkey	5
United Arab Emirates	20
United Kingdom	68
United States	-
Total	521

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.