

RSA SURVEY REVEALS 44% OF ORGANIZATIONS REGULARLY FAIL TO INVESTIGATE AND REPORT DATA BREACHES IN TIME



Do you have fixed time limits in which you need to investigate a potential incident?

40% IN A FEW HOURS!
14% by the end of business day
11% in a few days
5% in a few weeks
5% in a few months

75% YES
they have fixed time limit

25% NO
there is no preset time limit for that

Have you missed any of these deadlines (investigating or reporting) in the last 12 months?

6% always miss
38% sometimes miss

44% YES

56% NO

CAN KEEP DEADLINES

Are you required to report these incidents to external authorities or other entities within a predefined time limit?

HAVE TIME LIMIT TO REPORT
11% in a few hours
13% by COB
11% in a few days
7% in a few weeks
3% in a few months

45% YES

25%

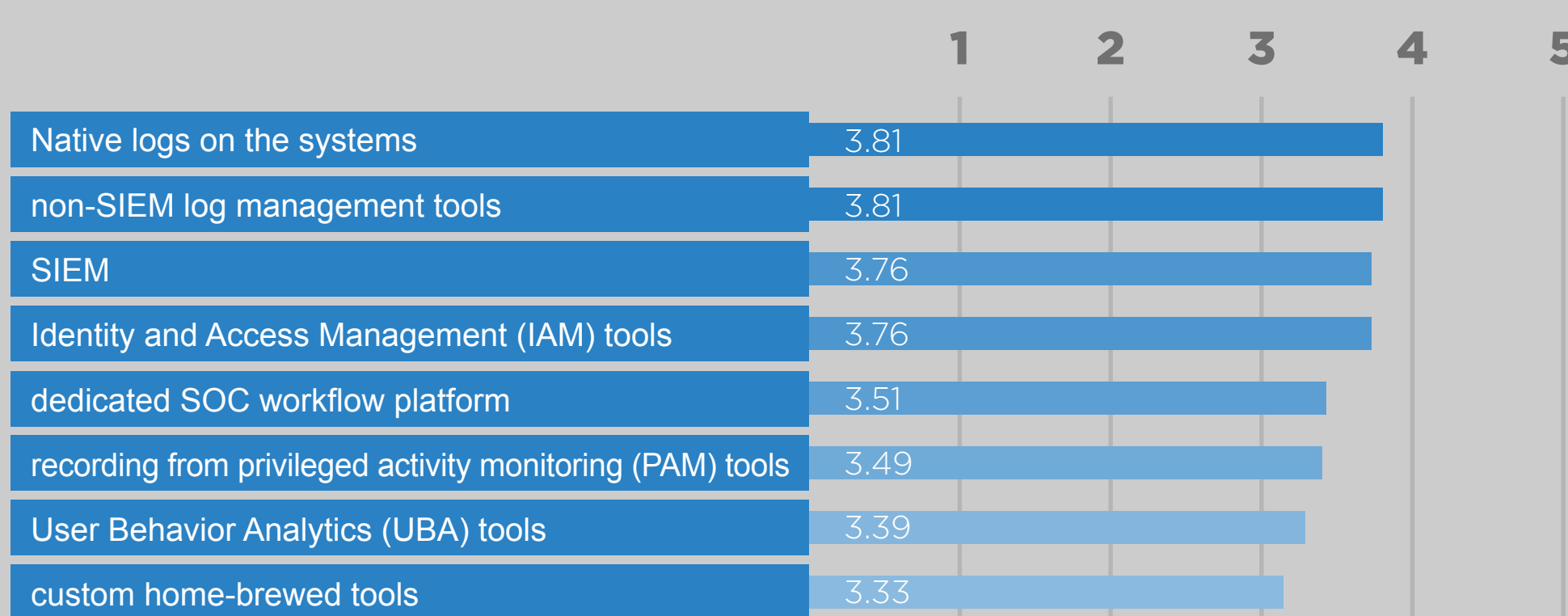
30%

NO TIME LIMIT FOR REPORTING

DO NOT NEED TO REPORT

How important role do the following tools play in the security investigation process?

On a scale 1-5 where 1 is least important and 5 is most important



Most important aspects of the investigation process

SATISFACTION

1

easy access to all relevant information

2

ability to ad-hoc drilldown

3

fast data access

4

see differences of actual user actions and normal baseline

5

have a single point of starting including all relevant details

6

see how users compare to their peers

7

turn data into understandable information

IMPORTANCE

2

harmonized

5

more satisfied than its importance

3

harmonized

6

more satisfied than its importance

4

harmonized, could be slightly improved

7

harmonized

1

MUST BE IMPROVED

It would be the most important aspect but IT professionals are least satisfied with understanding their own data.

About the survey

Balabit's Contextual Security Intelligence (CSI) Report market analytics are created on a regular base. CSI is a new information security concept for preventing data breaches without constraining business. This time Balabit asked 108 IT and security professionals including CIOs, CISOs, and auditors from Computer Security-, Financial-, Governmental-, Healthcare- and other sectors at RSA Conference 2016 USA in San Francisco, about the current status of their security investigation processes. The survey aimed to map what aspects they consider the crucial part of their investigation processes, and whether they are satisfied with those aspects or should be improved. Security tools' effectiveness in forensics investigations were also examined, as well as organizations ability to detect, respond, investigate and report about data breaches in time.