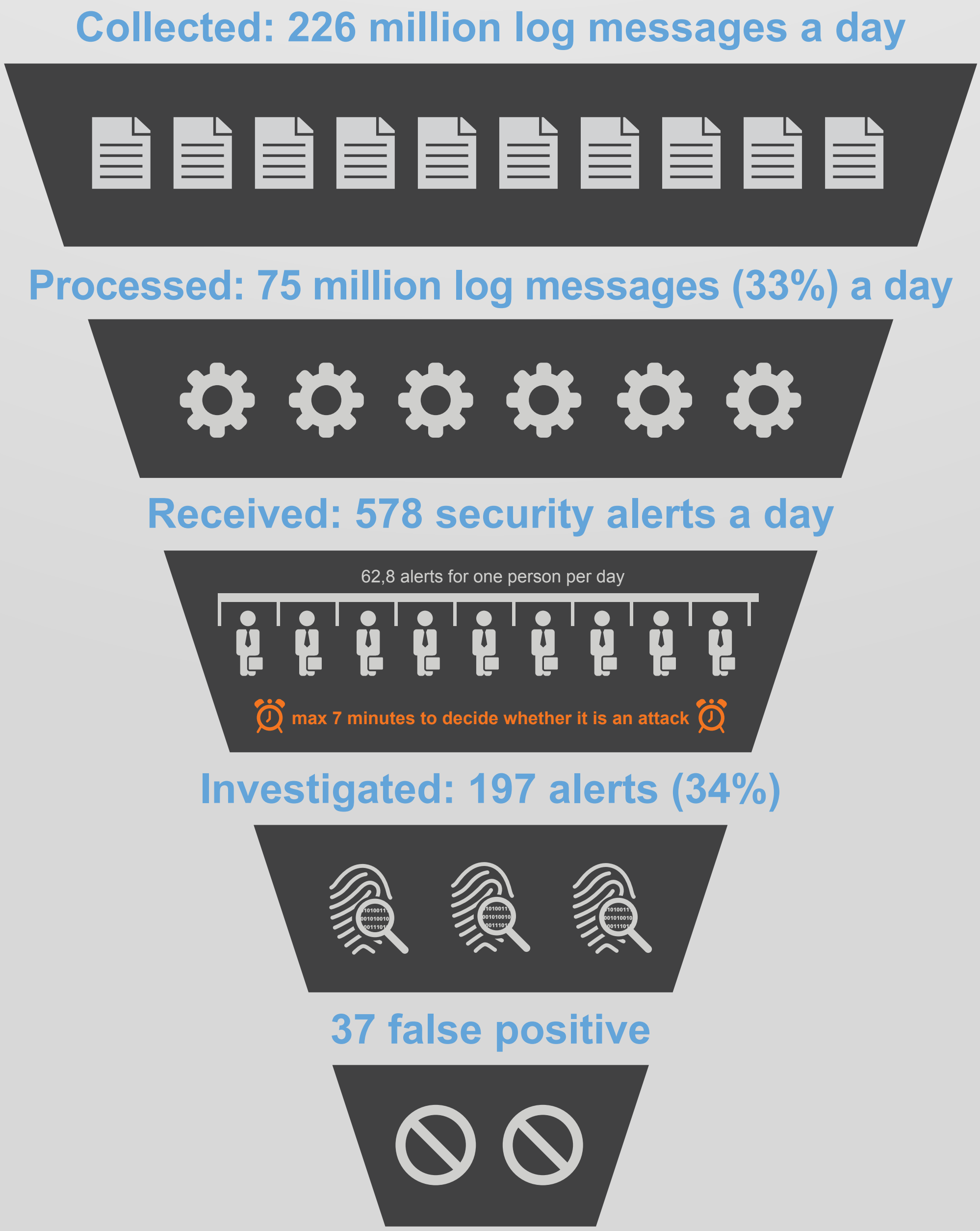
Balabit CSI Report

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Wondering why we are hearing about so many data breaches recently?

Organizations have an average of 7 minutes per security alerts to decide whether they are under an (APT) attack.



Collected: 226 million log messages a day

Processed: 75 million log messages (33%) a day

Received: 578 security alerts a day

62,8 alerts for one person per day

max 7 minutes to decide whether it is an attack

Investigated: 197 alerts (34%)

37 false positive

BalaBit surveyed 550 conference attendees on RSA Conference in San Francisco, Cyber Security Expo in London, IT-SA in Nuremberg, Les Assises in Monaco, and ITBN in Budapest. IT executives, CIOs, and CISOs participating in this survey represented organizations including the telco, finance, government and manufacturing sectors that need to comply with several regulations. Size of the organizations broke down as follows: 24% over 5000 employees, 25% between 500-5000 employees, 52% under 500 employees.

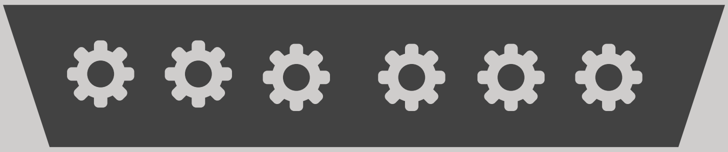
1

Collected: 226 million log messages a day

Log files record events that occur in an operating system or other software runs, or messages between different users of a communication software. Organizations collect hundreds of millions of log messages a day: on the average 226 million log messages per day. As your analysis can be only as good as the data you work from, it is essential to collect all the relevant logs from all possible platforms, than structure and classify them for further analytics. Collecting logs with high-speed, on a reliable way with "zero message loss" is a must in this process.

2

Processed: 75 million log messages (33%) a day



There are many log messages containing business critical information, and of course plenty of log messages with low relevancy. The bad news is that you need to collect and store ALL of them to be able to provide it for forensics investigation, in case it is necessary. Of course, processing (analyzing) 100% of your logs would be an extremely huge waste of money and efforts, so you need to decide which log message belongs to which group (relevant or not relevant). Organizations we surveyed are able to process 33 percent of their log messages – on the average. This result looks like a healthy rate, if this 33 percent really belongs to the relevant logs. The filtering process depends on your network and for what further purposes you use the logs.

3

Received: 578 security alerts a day

62,8 alerts for one person per day
max 7 minutes to decide whether is is an attack

An average **578 security alerts a day** – what our survey participants receive on a daily basis –is an extreme huge number (for these size companies, having such a small IT security teams). They receive alerts from firewalls, IPS, IDS, SIEM and user monitoring systems, to prevent potential malicious activities.

Organizations need to decide WHERE they put bigger efforts:

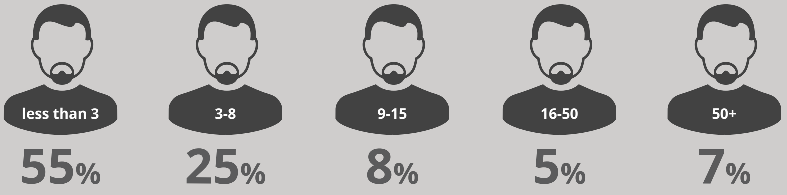
a) to **well configure their prevention systems**, continuously update the rules and patterns and have less but relevant security alerts, in this case it is easier to investigate them

b)or having a bit more alerts, which means more false positive (but less chance for a false negative) alerts, in this case the big effort should be taken to **investigation**.

Both approach can be good until the whole process is well balanced.

4

How many people are dedicated to investigate these security alerts?



Our survey results highlight that an average 9.2 people on the IT Security Team need to examine those 578 security alerts a day. It means that theoretically (if no one is on holiday from the team and all of them works on the alert investigation) one person would have received **62,8 security alerts a day**, and one person receives 7,8 security alerts per hour. Calculating with a 10 min. break per **1 person has an average maximum 7 minutes per security alert to decide** whether it is a sign of an attack (for instance, a sophisticated APT attack) and needs further investigation or not. This result highlights that IT Security Teams need to dramatically improve their efficiency by prioritizing the security alerts based on the real risk factor. The more efforts they can allocate to the high priority alerts with relevant risk, the more their network would be protected.

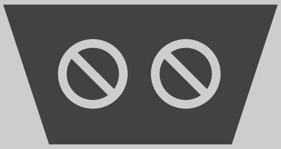
5

Investigated: 197 alerts (34%)

What to do, when time and efforts are not enough to investigate all the security alerts? According to our survey results, an average of **34 percent of the security alert scan be investigated** by organizations. Which could be enough, but the question is how to decide which security alerts are the top priorities? Rules and pattern based alerts are useful but can be costly and not enough to protect against the latest threads. We suggest automating the priority selection -- let the machines do the majority of the job to select usual activities based on pre-defined rules and self-learning business intelligence algorithms, and only involve – but always involve – humans to handle the unusual activities.

6

37 false positive



Our survey reveals that organizations have an average **18,8 percent false positive alerts** from those investigated. Having false positive alerts means that organizations keep security alerting balanced. It is even better “to waste” a certain time for false positives investigation than ignoring a suspicious activity and not having any alerts (false negative) about that. BalaBit suggests that organizations request alerts on the unusual activities, and help organizations to prioritize alerts based on the potential risk it poses to the corporate IT network by adding contextual information in addition to logs and analyzed by big data algorithms.

i

Finding 578 security alerts a day from 226.000.000 log messages is something like turning 60 GB (13 DVD) data into 1 MB (less than an 8-inch floppy disk) valuable information.

Be an early adopter of Blindspotter and visit our website.
https://www.balabit.com/network-security/blindspotter