Why do companies need User Behavior Analytics?

"Only amateurs attack machines; professionals target people.
And any solutions will have to target the people problem, not the math problem."[1]
(Bruce Schneier)

Many companies' worst nightmare – a sophisticated external attacker or malicious insider – is already within its perimeter. Nowadays, attackers are intelligent, well-funded, and their attacks are increasingly complex and well targeted. The recent, high-profile breaches, such as the case of Sony, Target or Ashley Madison, were carefully planned and went undetected for some time, with the attackers moving freely inside the victim's IT environment. Malicious insiders hold an advantage over a company's primary security tools, because these tools are designed to protect against external threats, not against trusted employees. Targeted attacks by humans use a combination of IT vulnerabilities, social engineering, and ordinary crime to gain unauthorized access.

Statistics

Attacks are costly and widespread

50%

Almost half of organizations suffer at least one security incident in the last 12 months.[3]

1 BILLION

Almost 1 billion data records were compromised in attacks in 2014.[4]

256 DAYS

Malicious attacks can take an average of 256 days to identify.[2][5]

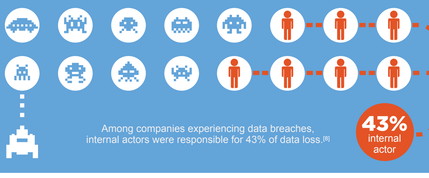
$21,155/DAY

The mean number of days to resolve cyber attacks is 46 with an average cost of $21,155 per day – or a total cost of $973,130 over the 46-day remediation period.[6]

People are dangerous

nearly 90% of all incidents are caused by people

"The common denominator across
the top four security incident patterns
(miscellaneous errors, crimeware,
privilege misuse, lost and stolen assets)
– accounting for nearly 90% of all incidents – is people."[7]



Among companies experiencing data breaches, internal actors were responsible for 43% of data loss.[8]

43% internal actor

75% of IT security experts consider insider threats and insiders' account misuse more risky than outsider threats.[9]

83% of IT security experts assume that attackers use social engineering methods – e.g. phishing – when they want to get sensitive data in the shortest time.[10]

Security Intelligence and more

Companies using security intelligence technologies were more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost savings of $1.9 million when compared to companies not deploying security intelligence technologies.[11]

37% of respondents indicated they face over 10k alerts/month. The low end of that range, (10k) translates to 300+/ day, and ~14/hr, so a nearly constant occurrence. The percentage of false positives were 52%, while the percentage of redundant alerts were 64%.[12]

Cyberattacks affect more and more companies, which suffer bigger and bigger losses due to these. Besides external attackers, malicious or cheated insiders became the most dangerous factors of IT security. It means the new perimeter, where companies have to focus, is users. But traditional defenses are not able to overcome the overwhelming number of alerts and find the "unknown unknown" threats that are lurking on them. User Behavior Analytics is the right answer to these problems. It is able to:

find external attackers and malicious insiders without disrupting the business

optimize security alerts by reducing their number and prioritizing the most important ones

improve the investigation of alerts by providing contextual information

[1] https://www.schneier.com/crypto-gram/archives/2000/1015.html#1
[2] 2015 Cost of Data Breach Study: Global Analysis - May 2015 – The Ponemon Institute

Sources:

[2] Experian, 2015 Second Annual Data Breach Industry Forecast
[3] Gemalto, 2014 Breach level Index
[4] Ponemon, 2015 Cost of Data Breach Study
[5] Ponemon, 2015 Cost of Cyber Crime Study
[6] Verizon, Data Breach Investigations Report 2015
[7] Intel Security, Grand Theft Data – Data exfiltration study: Actors, tactics, and detection
[8] Balabit CSI report
[9] Centrify, Corporate Perimeter Survey
[10] Ponemon, 2015 Cost of Cyber Crime Study
[11] FireEye, The Numbers Game: How Many Alerts is too Many to Handle?