7 THINGS UEBA DETECTS

A survey by analyst firm Enterprise Strategy Group of more than 400 cyber security pros reveals that an overwhelming majority—94%, in fact—plan to deploy machine learning/AI technologies for security analytics and operations, which would include UEBA.

If you're considering deploying UEBA technology, familiarize yourself with these top seven threats that UEBA can detect and stop before it's too late.

Symantec.

1

Slow and Low Attacks

Bad guys, outsiders and insiders alike, know that traditional security tools work on basic thresholds and understand repetitive attempts to steal sensitive data raises red flags.

They keep their activity slow enough with low volume, exfiltrating small amounts of data over time, to stay under the radar.

UEBA identifies these types of reoccurring behaviors and notifies investigators immediately!

2

Collusion

A group of people who work closely together want to leave their current employer and start their own company.

They conspire, each one stealing bits of sensitive intellectual property data, hoping to avoid detection.

UEBA detects changes in each employee's behavior, validates those behaviors as unusual compared to their team and business unit, and alerts investigators.

3

Hiding in the Noise

Someone assigned to a specific role or group accesses data that's not necessary for them to do their job.

The person attempts to mask the activity within the noise of the group, hoping to go unseen.

UEBA detects those behaviors and alerts investigators.

4

Persistent Exfiltration Attempts

If an individual tries to exfiltrate sensitive data using one method and they're blocked, they will try another way to get around the system, until they extract what they're looking for.

UEBA flags several failed attempts, quickly pieces the actions together, and prompts an investigation.

5

Door Jigglers

Many people are curious or like pushing the limits, but the truth is these are the people who are most likely to open that file that they know they shouldn't.

These types of people visit blocked websites and keep on trying, assuming nobody is really looking. They are also likely to be a soft target for a phishing attack.

UEBA detects their persistent attempts, and warns door jigglers about their risky behavior. Evidence suggests 80% will stop doing it right then and there just by giving them notice.

6

Checking out/Preparing to Exit

When employees are preparing to leave a company, they may take large amounts of sensitive data with them.

UEBA spots behavioral changes consistent with people preparing to leave their jobs and prevents large amounts of data from slipping out the door.

7

Gold Prospectors

Unlike door jigglers, gold prospectors are true bad actors, scouring file systems, trying to log into whatever they can find, looking for any golden nuggets.

These people have big dreams and keep looking until they find that golden sensitive data.

UEBA technology easily identifies individuals trying to steal sensitive data for their own gain and stops them dead in their tracks!

Symantec.

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.