10 compelling reasons why log file based security monitoring sucks

Over recent years many enterprises have invested much of their cyber security budgets in Security Information and Event Management (SIEM). The companies offering SIEM solutions are spending millions marketing their solutions, and the promises SIEM makes - you only have to look at the F1 lineup to see their names!

“Managed SIEM” or as it’s sometime s referred to “Next Generation SIEM”, is what Bluedog offers via it’s MDR solutions, but whereas SIEM uses log files to try and find the bad guys, MDR is much more proactive and investigates the actual real time risk and threats across the network and can help pinpoint the full spectrum of attacker activity much faster.

Here we look at the drawbacks of using a SIEM solution which relies on Log Files, and why it’s a seriously poor quality yet ironically rich billioniare cousin of MDR!

1. You miss devices which are connected to the network under Bring Your Own Device (BYOD) policies, as these haven’t been configured to send log files. You therefore miss all that activity which can easily allow malware and attackers to hide under the radar.
2. You miss IOT devices like printers and VOIP phones, which are used by attackers to hide their tracks. We all remember the internet connected fish tank thermostat story!
3. If an attacker is on your server, the first thing they will wipe are the log files and there goes your trail! You have no clue where, how and when you were attacked; are you still being attacked?
4. From an OSI layer perspective: log files are on layer 7, and network monitoring is on layer 2. This means network monitoring is getting much more detail.
5. Log files don’t contain the proof data you need to confirm or convict the attacker, which network data does. Logs files are only the end result; there are no underlying proof data.
6. Log files don’t catch an attacker’s lateral movements through your network as this lateral movement doesn’t generate logs (SMB traffic).
7. Log files can only catch the easy attacks. It’s not possible for log files to be used to catch sophisticated attacks due to a lack of behavioural analysis capabilities.
8. Setting up and collecting log files is time consuming and very costly to do correctly and maintain properly. You need central log servers and loads of storage capacity
9. With all those log files and extra storage, guess what! You now have double security governance to prove the data integrity of your log files.
10. When using network monitoring, you have 95% coverage already. Adding log file monitoring adds 3% more coverage but triples the total cost of ownership.

To find out more about our services and our other solutions, email us at **sales@bluedogsec.com** or visit **bluedog-security.com**.