The Role of Baselines in Network Monitoring

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity

November 2, 2025

Instructions:

System monitoring and the use of network traffic log files are extremely important for gauging baseline performance and observing events. Why does identifying abnormal behavior first require having a baseline? What can a log file show that lends insight into abnormal behavior?

The Role of Baselines in Network Monitoring

Identifying abnormal behavior requires a **baseline** because, without one, an organization has no objective definition or standard for "normal" behavior (NIST, 2012). A baseline is a snapshot of a system's or network's standard operational state. For example, obtaining and recording typical CPU usage, memory consumption, network traffic patterns, user login times, and running processes looks like over a period.

Without an objective reference point, it is impossible to distinguish a genuine threat from routine activity, creating either false positives or false negatives (or both). For example, a spike in network traffic at 2 AM may be a malicious data exfiltration attempt, or it could be the normal start time for scheduled nightly backups or business activity in different geographical locations of the world. Only a "normal" baseline can provide the context needed to distinguish between them (Chen et al., 2017; McDonald et al., 2022).

Log files help track and provide granular, time-stamped records of events (Cichonski, 2012). When an alert triggers because activity deviates from an organization's baseline, the log file is the first place an analyst will look for more insight into the matter. A log file can show:

- **Failed authentication attempts:** A massive string of failed logins from a single IP address (a brute-force attack).
- **Impossible travel:** A single user account logging in from two different continents simultaneously (a compromised account).
- **Unusual port access:** Firewall logs showing scans across multiple ports from an external source (reconnaissance).
- **Anomalous data movement:** A server that normally receives only data suddenly sends gigabytes to an unknown external address (data exfiltration).

Thus, baselines help an organization determine whether network traffic and behavior are normal or anomalous. Anomalies may warrant further investigation, and log files provide additional information to support conclusions and help the organization appropriately respond if needed.

References

Chen, Qian, & Bridges, Robert A. (2017). *Automated behavioral analysis of malware: A case study of WannaCry ransomware*. In X. Chen, B. Luo, F. Luo, V. Palade, & M. A. Wani (Eds.), Proceedings of the 16th IEEE International Conference on Machine Learning and Applications (ICMLA 2017) (pp. 454–460). Institute of Electrical and Electronics Engineers Inc. https://ieeexplore.ieee.org/document/8260673

Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). *Ransomware: Analysing the impact on Windows Active Directory domain services*. Sensors, 22(3), 953. https://www.researchgate.net/publication/358119298_Ransomware_Analysing_the_Impact_on_Windows_Active_Directory_Domain_Services

National Institute of Standards and Technology (NIST). (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30, Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1