Further Reading Material, SIEM

This lesson is designed to provide students with additional reading material on different aspects of SIEM platforms and usage in case you didn't fully understand a specific part of the course, or you just want to read more about this area of cybersecurity to strengthen your skills ready for the BTL1 practical exam. **We suggest that students come back to this lesson once they have completed this domain.**

If you have any resources you would like us to add to this list, please reach out to us via email at *BTL1@securityblue.team* with the subject line *"SIEM Domain Further Reading"*.

RESOURCES

- **What is SIEM Software? How it Works and How to Choose the Right Tool by CSO Online** // https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html
- **What is SIEM? A Beginners Guide by Varonis** // https://www.varonis.com/blog/what-is-siem/
- **SIEM Architecture: Technology, Process and Data by Exabeam** // https://www.exabeam.com/siem-guide/siem-architecture/
- **Top 6 SIEM Use Cases by Infosec Institute** // https://resources.infosecinstitute.com/top-6-seim-use-cases/
- **Standards and Best Practices for SIEM Logging by AT&T** // https://cybersecurity.att.com/blogs/security-essentials/what-kind-of-logs-for-effective-siem-implementation
- **SIEM Rules or Models for Threat Detection? by Exabeam** // https://www.exabeam.com/siem/siem-threat-detection-rules-or-models/
- **Tune Down the Noise: How to Effective Tune Your SIEM by RedLegg Blog** // https://www.redlegg.com/blog/how-to-effectively-tune-your-siem
- **Detecting a Security Threat in Event Logs by Netwrix** // https://blog.netwrix.com/2014/12/03/detecting-a-security-threat-in-event-logs/
- **Critical Log Review Checklist for Security Incidents by Lenny Zeltser** // https://zeltser.com/security-incident-log-review-checklist/
- **Reddit Thread: What Windows Server Events are you Monitoring and Why?** // https://www.reddit.com/r/sysadmin/comments/1sq955/what_windows_server_events_are_you_monitoring_and/