Fine-tuning your Microsoft® Sentinel platform means a stronger security profile, fewer manual tasks, reduced alert “noise,” and an empowered security team. Here are six ways to optimize the platform once you’ve deployed and begun to ingest logs.

**6 Ways to Make the Most of Microsoft Sentinel**

1. **Check log forwarders and ingestion rates.**
   Make sure logs are forwarding correctly and that your VHL log directory is not at or beyond capacity. Over time, look back at your ingestion rates to forecast your needs more accurately.

2. **Minimize false positives to control noise.**
   Out-of-the-box rules may not be properly aligned to your needs. Use the WatchList feature to bake queries into analytics rules and reduce false positives and alert fatigue.

3. **Use a centralized tenant.**
   Establish a baseline for thresholds, running frequency, and other settings by using Azure® Lighthouse to monitor multiple Azure tenants and manage workspaces in a single location.

4. **Perform out-of-the-box detuning.**
   The Microsoft Sentinel platform has alerts with default frequencies that may not work for your organization. Detune to minimize non-urgent alerts and make your team more efficient.

5. **Automate to improve security.**
   From automating storage per compliance and retention requirements, to controlling access based on user behavior, Microsoft Sentinel can support a wide range of automation use cases.

6. **Expand and enhance.**
   Keep your eyes out for new ways to leverage Microsoft Sentinel. Bring Your Own Machine Learning (BYO ML) and advanced visualization are a couple of areas to look into.

For the most effective and targeted approach, consider Insight’s Managed Security Services (MSS). We orchestrate Microsoft Sentinel with other advanced tool sets, the latest technologies, and a proven methodology to help businesses amplify their security.

Learn more about Insight’s security practice and Managed Security Services.