Logging and Monitoring

Call to Action

After learning about logging and monitoring, let's put it to action using this Call to Action document.

In this document you can find actionable tasks that will help you implement logging and monitoring in your system.

1. Make sure there's a central logging service in your system

   Every microservices system must have a central logging service to collect the logs generated by the various services. This service can be a product, such as the ELK stack, or an in-house developed service. This service should be able to receive a large amounts of log records, store them, and allow running analysis on them

   The central logging service in the system is ________________

2. Make sure services log security related incidents

Having logging libraries in place is not enough. Make sure, via code review, that the services actually log potential security incidents, such as unauthorized access, exceptions, SQL injection attacks, excessive loads and more.

Service name	**Logs security related events?**

3. Connect the logs to the organizational SIEM tool

If the organization has SIEM tool in place, make sure security logs are streamed to it.

Is there an organizational SIEM tool? __________

Are the system’s logs streamed to it? _________

Print this document and use it for running the security tasks.

Good luck!

Memi