SOC/MDR Platform Engineer

Job Description:

Reporting to the Platform Manager, the MDR Platform Engineer is responsible for testing and building new, or updating existing, automation within MDR Centre technologies and integration between such technologies and the larger set of systems and applications within True Digital. The role involves designing, developing, testing and deploying automation and integration using toolsets provided by various MDR Centre technology vendors. The role is also involving in planning and supporting the operational security team with required security technologies to fulfill their day-to-day operations. The role will support new platform engineering, updating the existing environment as well as implementing any new requirement.

Key Responsibilities:

- Evaluating and selecting appropriate technology solutions to meet MDR Centre consumer needs.
- Preparing, testing, staging and deploying new MDR Centre technology platforms.
- Preparing, testing, staging and deploying major releases and major changes to existing MDR Centre technology platforms.
- Analysis of automation and integration within the current MDR Centre technology stack to identify areas for improvement.
- Working with other MDR services to design automation and integration that meets their needs.
- Developing, testing and deploying new automation and integration via custom code and scripts.
- Working with the MDR Architect to test and fine tune the technical design of the use case to be implemented in the SIEM.
- Documenting MDR Centre technology platform architecture and deployments

Qualifications:

- Bachelor degree in a related field such as information security, management or computer engineering.
- Platform-specific certifications are desirable.
- Good working knowledge of security concepts for both Windows and Unix related operating Systems.
- Good working knowledge of network concepts.
- Familiar with well-known SIEM tools (e.g. Splunk and ELK) and dashboard/analytic tools (e.g. Grafana).
- Familiar with SOAR and UEBA tools.
- Working experience in a MDR Centre, Security Operations Centre (SOC), Managed Security Service Provider (MSSP) or enterprise network environment preferred