IT Capstone Topic Approval Form

The purpose of this document is to help you clearly explain your capstone topic, project scope, and timeline and to ensure that they align with your degree emphasis. Without clearly addressing each of these areas, you will not have a complete and realistic overview of your project, and your course instructor cannot accurately assess whether your project will be doable for the purposes of these courses.

Of course, if this a project that you have already completed at work or elsewhere, this should be easy to fill in! Most students use a project that they have already completed in the past year or two. In that case, you will write the proposals (Tasks 1 and 2) as if the project has not been done yet, and Task 3 as the complete post-implementation report.

Complete this form and send it (via UGCapstoneIT@WGU.edu) to your course instructor for approval. Once approved, you will receive a signed document in PDF format that you can upload as part of Task 1.

DEGREE EMPHASIS: Bachelor of Science, Cybersecurity and Information Assurance

ANALYSIS:

Project Topic – Installing and configuring a security information and event management (SIEM) system for Wayne Enterprises.

Problem Statement or Project Purpose – Wayne Enterprises is a modest-sized company with a small technical infrastructure. They currently do not monitor any logs for any security events or specific information. They had a security scare when an angry employee added themselves to the domain admin group in Active Directory and changed the CEO's display name to a bad word. They would like to take a more proactive approach to their security, so they hired my company Gutz Sec to install and configure a security information and event management (SIEM) system for them.

DESIGN and DEVELOPMENT:

Project Scope

a. Project Goal(s) and Supporting Objectives –

1. Conduct an inventory of technology that needs logging and monitoring.
2. Provision virtual servers needed for the SIEM.
3. Install and configure the SIEM infrastructure and software.
4. Feed the logs of current infrastructure into the SIEM; this includes installing any forwarders on the servers that the SIEM will monitor.
5. Configure SIEM alerts, reports, and dashboards for Wayne Enterprise's IT security team.
6. Handover documentation and management of the SIEM to the IT security team and provide training.

b. Project Outcomes and Deliverables –

1. Improve security posture by implementing alerts, dashboards, and log reports of the current infrastructure.
2. Centralized management of all infrastructure logs will bring more eyes to any notable events currently going unseen.

3. Prevent potential security breaches by providing close to real-time alerts.
4. Increase efficiency by having dashboards organized with relevant metrics.
5. Trained IT security staff will be more proactive by managing and responding to alerts.

c. Projected Project End Date – The project end date is about two weeks from its start date. Approximately November 19, 2021. Two weeks will give Gutz Sec sufficient time to inventory the existing infrastructure, build and configure the SIEM, feed all logs into the SIEM, create alerts, reports, and dashboards. This timeframe includes the time needed to train the IT security staff.

IMPLEMENTATION and EVALUATION:

Describe how you will approach the execution of your project – I will deal with this project in a few stages. My steps are as follows:

1. Inventory the current infrastructure by going over Wayne Enterprise network diagrams and speaking with IT staff while noting what systems provide valuable logs.

2. Provision the Windows servers needed by the SIEM using Hyper-V. Wayne Enterprises has provided a host for these virtual machines. We will build two servers to serve as indexers, one for a search head and one for a master server—a total of four virtual servers.

3. Configure the SIEM software once the infrastructure is in place.

4. Feed all necessary logs into the SIEM; this includes making sure all times are synchronized and installing the forwarding agent on servers that the SIEM will monitor (for example, Domain Controllers).

5. Configure relevant alerts, dashboards, and reports to benefit the Wayne Enterprise IT staff.

6. Train IT staff to manage and respond to logging and alerts.

☒ **This project does not involve human subjects research and is exempt from WGU IRB review.**

COURSE INSTRUCTOR SIGNATURE:

COURSE INSTRUCTOR APPROVAL DATE: