Project Proposal – Internship

Version: 7
Period: Spring 2023

Goal and use of this document

The proposal is used to describe a practical research internship which is carried out in semester 5 of the study program. Through this form the student requests approval for the assignment from the internship coordinator. This document is also used to receive feedback from client and coordinator and should lead to all three parties having one single view of the assignment. The student is responsible for writing the content, based on input of the organization and feedback of the coordinator. This document may be written in Dutch.

Student details

Student number	: 4252802
First name + Family name	: Mohammed Alshukaili
Location	: Eindhoven
Profile Semester 3	: M
Specialisation Semester 4	: ICS
Internship choice	: ICS
Dutch-speaking?	: No

Internship period

Start date	: 6-2-2023	(official start date: Monday FHICT-week 1)
End date	: 23-6-2023	(official end date: Friday FHICT-week 18)

Organisation details

Name	: Eindhoven University of Technology (TU/E)
Visiting address	: https://goo.gl/maps/ENKJ9ocrwNvDmXwD7
Zipcode + City + Country	: 5612 AZ, Eindhoven, The Netherlands
Phone	: 0402472381
Website	: https://www.tue.nl , https://security1.win.tue.nl
Own Company ("Eigen bedrijf")?	: No

Company mentor

(The person who guides the student on a regular basis)

First name + Family name	: Peter Boosten
Department	: ESH-SOC
Position	: Assistant Professor
Background (highest education)	: SOC Manager
Background URL (e.g. LinkedIn)	: https://www.linkedin.com/in/peterboosten/
Phone	: +31 (0)40 2474971
Email	: p.i.j.boosten@tue.nl
Assignment in ASAM?	: Yes

1. Context & Problem/Opportunity

1.1 Context & Background

The ESH-SOC at TU/e is a SOC monitoring IT security events run by the Eindhoven University of Technology. The ESH-SOC is a new project starting on the 30th of June 2020, to which several commercial partners are affiliated. These commercial partners enrich the service portfolio provided by the ESH-SOC, as well as providing professional expertise contributing to running its monitoring operations. These commercial partners are all operating in the Eindhoven region and provide consultancy, IT management, and cloud services to their clients. The ESH-SOC operates in the highly technological sector of security monitoring, at the intersection between network security, data analysis by means of machine and deep learning techniques, and operational aspects such as incident detection, and reporting and communication to the customers.

1.2 Current situation & Stakeholders

The current situation regarding the activities, problems (or opportunity) is described. The relevant stakeholders within the organization are provide with an explanation why they (possibly) are stakeholders. The scope of the project must become clear at this point.

The stakeholders is the head of the SOC at TU/E.

1.3 Problem/opportunity description

The student working on this project can evaluate security problems in a real, operational environment and to engage in the feedback loop between SOC operations and SOC development by participating in the fine-tuning and refinement of (technological/process) aspects of its operation. The student will get experience with state-of-the-art security monitoring technologies in the larger context of security operations and contribute to their development by critically matching customer requirements with technological implementations and limitations

To ensure a timely and accurate detection of threats and attacks against our customer base, the ESH-SOC focuses on two main activities:

Development and improvement of state-of-the-art detection tools and techniques. This involves, for example, development of attack signatures for Zeek/Suricata threat detection; development of Kibana dashboard and security playbooks; platform tuning (ELK) and threat intel integration.
Security monitoring. This activity concerns the employment of the aforementioned technologies to support the detection and investigation of security incidents in the monitored environments. This includes the (live or forensic) analysis of security events, identification of affected assets, reconstruction, and reporting of attack development and (system) impact.

2. Assignment

2.1 Desired project result

Below it should be clear what the desired result of the internship is. What situation should be reached at the end of the internship?

Project goal

A clear and as concrete as possible description of the intended results and what value they should have for the organization. A (concept) project goal can be formulated and products to be delivered are indicated.

To be up to date with the latest network designs and how to build them. To develop in-depth knowledge and expertise on security monitoring of IT & IoT technologies. To become a substantial expertise as a security analyst capable of analyzing, recognition, investigation, and reporting security incidents.

"The student working on this project has the opportunity to evaluate security problems in a real, operational environment and to engage in the feedback loop between SOC operations and SOC development by participating in the fine-tuning and refinement of (technological/process) aspects of its operation. The student will get experience with state-of-the-art security monitoring technologies in the larger context of security operations and contribute in their development by critically matching customer requirements with technological implementations and limitations."

is all a team effort. The monitoring happens individually but the analysis and escalation is a team effort in collaboration with the different tiers. Working on the technological backend to match customer requirements/operational limitations is also something that can only happen by joining in a team effort.

Project IT-deliverable

Specifically indicate the IT-products (proof-of-concept) that will be developed. Describe the end product as well as any intermediate products or other deliverables that are already known. For each IT-deliverable, specify the technology(s) to be used.

The student will be working mainly on Security Onion to analyze traffic for our clients. Then, they will discuss the alerts with their mentor.

2.2 Research aspects

Research questions
As it is important that all results are based upon (also practical) research: Which research questions are going to be relevant in order to achieve the desired project result? Provide (sub)-research questions and possibly a main research question.

As an intern, I will apply research strategies for developing networks and improving intrusion detection and prevention tools.
I will need to own research in the field of cyber security.

TU/E offered me research that will require me to talk about:

1- A modern strategy to design and deploy networks. (individual)
2- Compare my design to other designs and why did I choose it. (individual)
3- Test the performance to my network. (individual)
4- Launch Security Onion to monitor the network. (individual)
5- Design the best suitable Dashboard for me. (individual)
6- Monitor all the alerts on the network. (Group)
7- Lower the amount of false-positive and false-negative. (Group)
8- Discuss the suspicious alerts with the team and get feedback from the mentor (Group)
9- Come up with a solution for the problem and ensure that it never happens again. (Group + individual)

Infrastructure (30%)
My mentor will require skills to configure and deploy servers.
I will also work on designing networks that will be monitored by me after.
The mentor will make sure that the network design is appropriate and secure.
I will need to prove why my design is good and professional.
I will conduct a performance session to test my network.

Monitoring the infrastructure (70%)

After deploying the network. I will be using Security Onion to monitor the network and analyze the traffic.

I will gather all the log files as alerts in the Security Onion Dashboard and Hunts.

Kibana will also help me to display the data. However, I would need to add more configuration for Kibana to only show the correct alerts and not the false-positives and false negatives.

All the alerts can be monitored by all the group members. Whenever someone finds a suspicious alert, they will send the alerts to Cases section.

All the group members, including me, will conduct a meeting to discuss and analyze the suspicious alert.

The mentor requires that all the group members come up with:

- How the alert happened
- How long did the activity take
- What will we do to fix the problem.
- What measure will we take to ensure it never happens again.

All this will be done using the DOT framework https://ictresearchmethods.nl/Methods.

Research approach
Regarding the DOT Framework: give a first indication of which research strategies and methods will be used and/or will be the most important ones. Think of the possibilities your internship environment specifically has or lacks and how you can in any case ensure you have enough methods and strategies to use.

3. Guidance & Expertise

Coach/Mentor

What background does your company mentor have? Think of education (Bachelor/Master/Phd) as well as experience in (internship) coaching or mentoring. How many hours of guidance will there be per week and will you be coached?

BSc, 20 yrs of experience on Security Monitoring, manager of the ESH-SOC. Soc Manager as well as senior team leads are avaialble at all times for guidance and coaching. Students work closely together with the team.

Expertise / Guidance

What expertise is available in the company and who has that expertise? What kind of support does the company provide on IT skills related to your domain? Describe the people and/or teams or departments where you are able to go to and who will help and guide you with (IT)-domain related questions, advice and review.

Security monitoring, security research and development, networking. Technical guidance from ESH-SOC personnel. Contact with research aspects from TUe faculty.

4. Personal & Professional goals

Which aspects on personal or professional development will you further develop? Focus on soft-skills. Select a realistic three to five aspects to work on. Use previous feedback received from others (e.g. semester coaches and teachers as input).

Personal goal	Describe what exactly you want to achieve and how to work on this.
To become a security analyst	**I will get to know the difference levels of alerts and what deserves to be discussed about and what deserve to be dropped.**

Development of skills to writing IDS rules	**I want to get familiar with writing IDS/IPS rules depending on where the detection tool is being used.**
Development in visualizing of alerts and using dashboards to make analyzing easier.	**I will develop a dashboard that shows alerts and information depending on the type of detection tool is selected.**
Improving my team skills.	**I will be working in a Security Operation Center with a team full of ambitious students and experts. Therefore, the job for me becomes more challenging.**
Proficiency of working inside a SOC.	**I tend to have a job that allows me to work in a SOC. Therefore, this is going to be the beginning of my career and will teach me everything about working in a SOC.**

5. (Optional) other important remarks