About me:

* Hi my name is Harman, I’ve got a background in vineyard and property management,
* I’ve completed my Bachelors in computer science in 2019 but never really got into the field and instead helped with family business.
* This spring lighthouse’s cybersecurity course caught my eye and I saw it was being funded by upskill Canada and I thought it would be a good opportunity to get back into tech.
* Want to be involved in tech, but coding isn’t my thing so I’ve been liking cyber security
* Areas I’m most passionate about I cyber: threat detection, vulnerability detection, monitoring, analyzing logs or other data…want to work with datadog, siem or Ids

Questions:

* Is there an specific cybersecurity challenges you are facing?
* What is your guys top priorities during the next 4 weeks in regard to cyber security?
* What do you expect from us during the course of this internship?
* How does cybersecurity fit into their overall vision
* Short term and long term security goals
* How do you currently monitor the performance and security of your infrastructure and applications?
* What tools or platforms are you using for real-time monitoring of your systems?
* Do you conduct regular vulnerability scans on your network and systems? If so, what tools do you use?
* What is your process for setting up alerts for potential security incidents or system failures?
* Do you have a centralized log aggregation system in place? If so, what tools are you using?
* I see on project scope page on rippen you guys are looking to implement centralized logging using something like Datadog, which is a monitoring, log management, alerting tool. Do you guys you currently monitor the performance and security of your infrastructure and applications?

Suggestions:

- look at current security posture, identifying gaps and vulnerabilities. This includes reviewing access controls, network architecture, and existing security policies.

- Set up dashboards in Datadog to visualize key metrics and create alerts for specific events, such as unauthorized access attempts or abnormal network traffic.

- Use Datadog to collect logs from various sources, ensuring they are centralized for easy analysis and correlation.

- Identify critical systems and applications that require logging, including databases, web servers, and network devices.

- Conduct a gap analysis comparing current security measures against industry best practices and relevant regulatory standards

- Based on the analysis, offer actionable recommendations for improving security measures, such as implementing multi-factor authentication (MFA), encrypting sensitive data, or updating firewall rules.

- Use tools like Nessus or OpenVAS to scan the network and systems for vulnerabilities, documenting findings and recommending remediation steps.

- Explore advanced security solutions like Intrusion Detection Systems (IDS), and SIEM to enhance detection capabilities.

* **Datadog:** A cloud monitoring and analytics platform primarily for performance monitoring, log management, and alerting. It includes some security features but is not specialized for security.
* **SIEM (Security Information and Event Management):** A dedicated security tool for collecting, analyzing, and correlating logs from various sources to detect and respond to security incidents.
* **IDS (Intrusion Detection System):** A security tool focused on monitoring network traffic or system activities to detect and alert on suspicious behavior or potential intrusions.

-that was a lot, they have very ambitious goals. Virgina you did a good job trying to guide her to practical tasks though, but they are still kind of fuzzy. The two I can recall is ai detection for registration process, setting up datadog and maybe a system review?

-set up app…I looked at it an felt overwhelmed last night