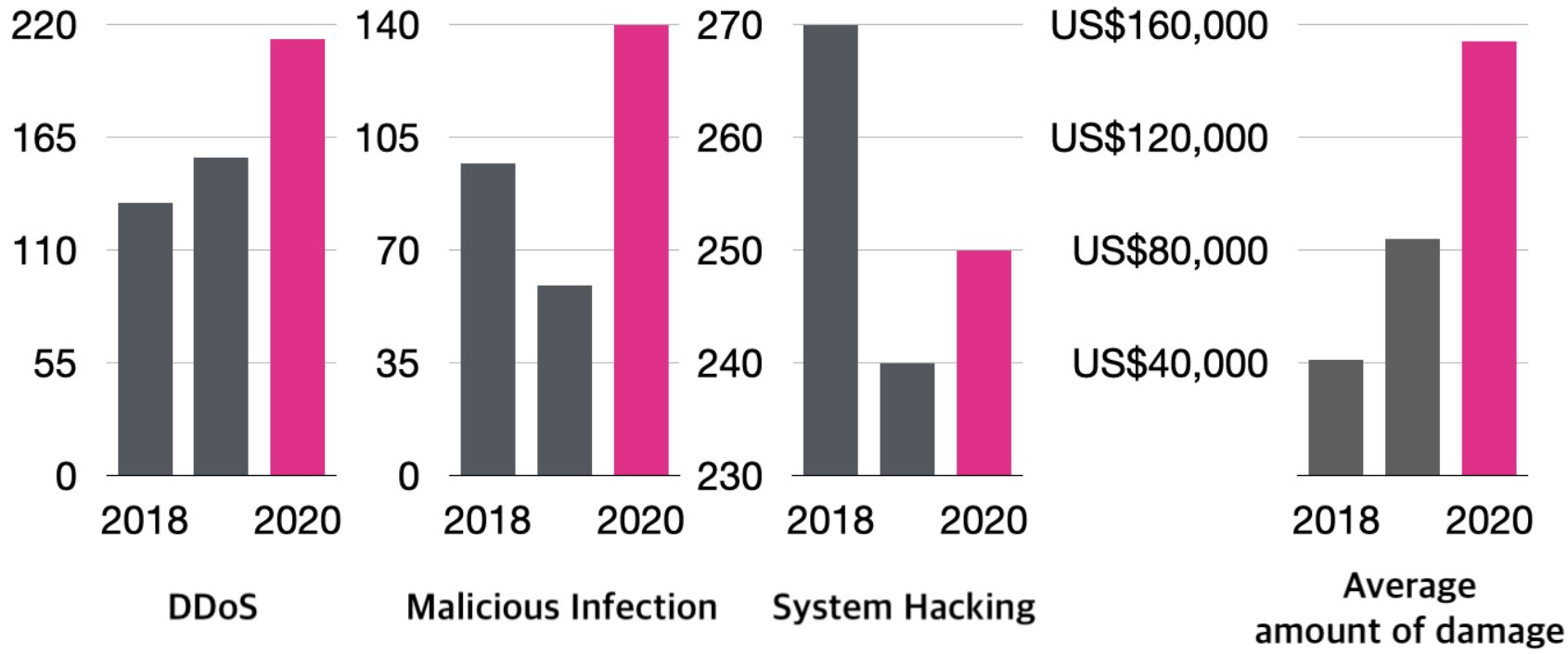
Project proposal

---

1. Title : Trinity(SIEM using ELK Stack)

2. Objectivity and Necessity : Centralized log system and response service using Elastic stack

From the past to the present, automation and digitalization are progressing across all industries. Accordingly, it is necessary to avoid intrusions that can affect the security of personal information and the inside/outside assets of the organizations. If problems such as cyber-attacks on important industries or information theft due to vulnerabilities occur, global problems may occur beyond individual infringement problems. Therefore, the demand for cybersecurity skills will become more demanding over time and will grow in importance in organizations.
It is necessary to properly judge and recognize the risk factors inside and outside the individual and organization. Set the risk tolerance threshold level, and take appropriate actions when a certain threat occurs. We can also create recovery plans after incidents to maintain continuity of service delivery, increase, reliability, and maximize value to the organization



▲Report and amount of damage by type of incident [source=KISA]

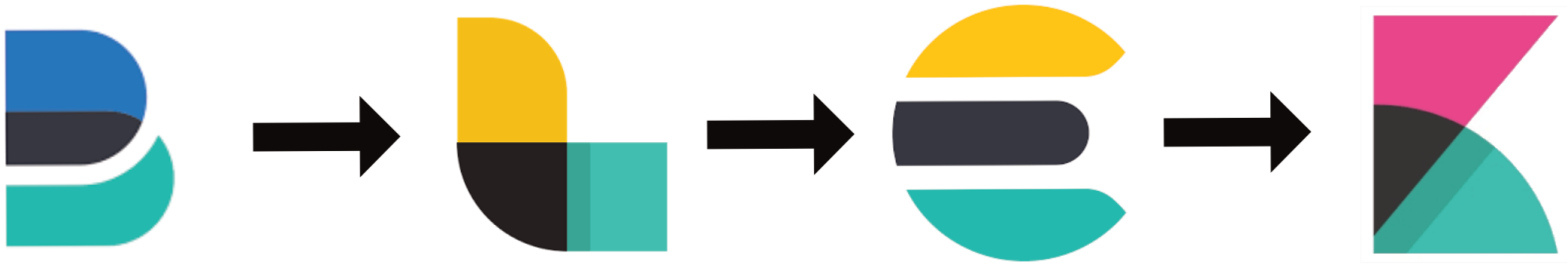
A total of 1,819 reports of cyber incidents occurred: 500 in 2018, 418 in 2019, and 603 in 2020, and An increase of 185 cases in 2020 compared to 2019. Cyber incidents are continuously increasing rapidly, and the scale of damage is also extremely increasing.
Therefore, if you have vulnerabilities that can be damaged by cyber security incidents, we need ways to identify and prevent them in advance and respond appropriately in the event of the incidents. The starting point of this project started with this thought, and the goal is to prevent the threats with advanced technologies in line with the evolving threats.

3. Content and Skills :

By using Elasticsearch, Logstash, Kibana (Elastic Stack), we build a centralized logging system to provide services for preemptive and follow-up action on suspicious signs.

1. Collect, process, and refine clients' logs using beats and logstash.
2. The preprocessed logs are sent to the central server for management.
3. Use Elasticsearch installed on the central server to analyze those logs for signs of intrusions and threats.
4. Based on the identified threats, the service and connection are quarantined, blocked, and will be restored.
5. Check the service quality of the server and perform log analysis through Kibana's data visualization on the monitoring host.

SIEM System
Configured using Beats, Logstash, Elasticsearch, Kibana.



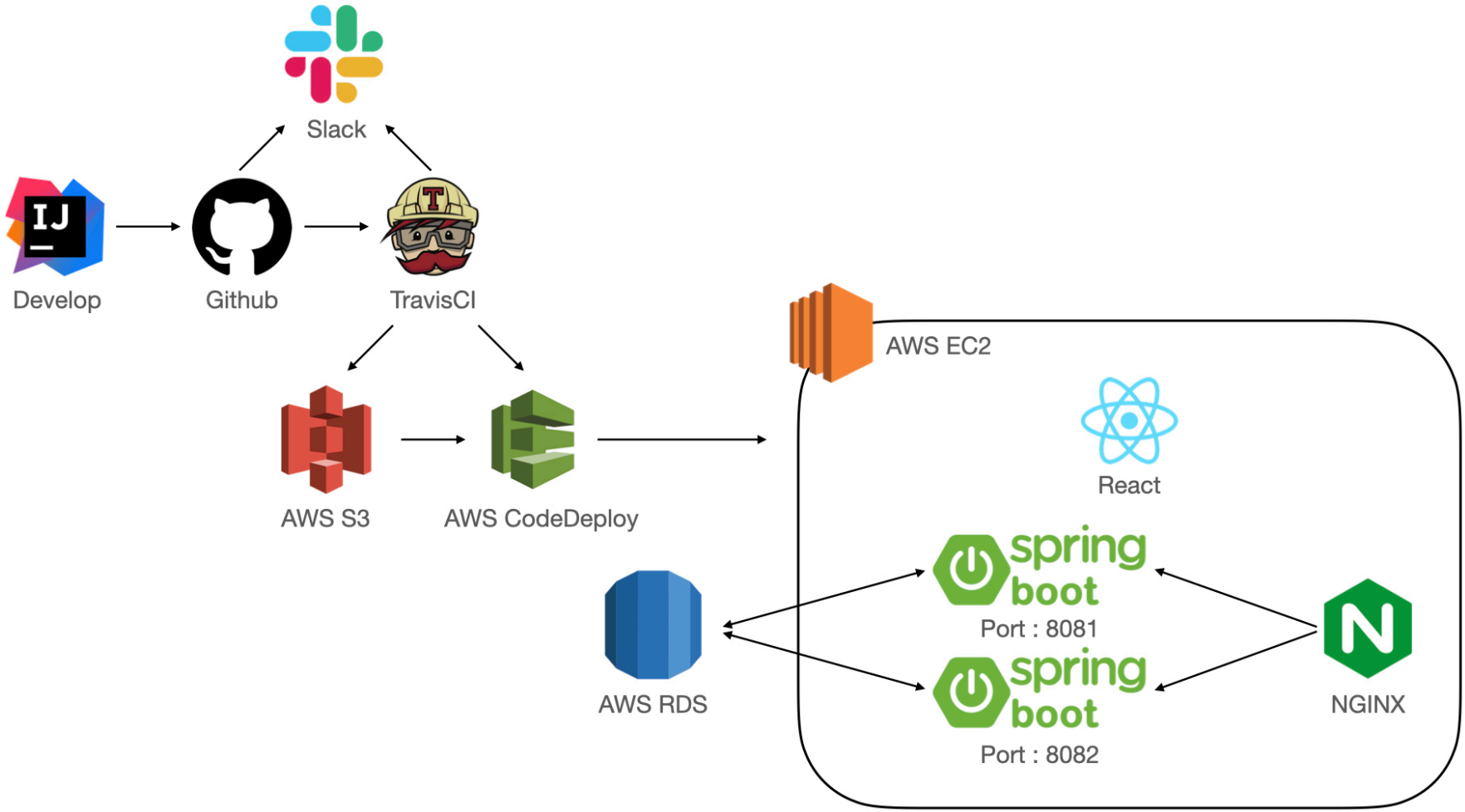
Beats - Collect logs and extra files and send to Logstash server to process
Logstash - Collect and classify, process logs
Elasticsearch - Store and analyze logs through HTTP RESTful API provided
Kibana - Visualize and analyze intuitively through log visualization

Elasticsearch is a search engine based on Apache Lucene. We can store unstructured or structured data in the indices in the HTTP web interface and JSON format and analyze it through documents, filtering, sorting, and statistics on field contents within documents.

Kibana analyzes indices stored in Elasticsearch, visualizes data, and makes it easy to configure and manage the Elastic Stack through functions within the UI.

Web Service

We will build web service for test to detect and prevent threats using Spring boot(Backend) and React(Frontend)



4. Conclusion :

The Elastic Stack is used to collect, refine, and analyze various, large capacity logs and visualize data to increase the efficiency of incident response and improve network security within the organization through pre-blocking, post-response, and recovery of internal/external threats in the future. and this improvement can be expected. By collecting and analyzing all logs generated by clients through the provision of SIEM service, large-volume log analysis can be used for automation and pre-, middle-, and post-intrusion detection and prevention.
Existing systems such as Splunk and IBM's Qradar have difficulty implementing high-cost, leading technologies. However, by using the Elastic Stack, which uses the Free and Open model as a license, we can use relatively low-cost and optimized services, and we can implement additional functions on our own in our organizations and connect them with the Elastic Stack.
Logs are diverse and are currently characterized by large volumes that cannot be analyzed only with the naked eye. Therefore, it is possible to respond quickly in security analysis if we use big data analysis technology to recognize, block, and recover cyber threats in advance. In addition, since there are limitations in signature-based detection with vaccines alone, it can be supplemented by anomaly analysis.
In the event of an abnormal threat to the client's normal service, we will provide incident response services by detecting signs in advance through correlation analysis.

Plan

Period	Plan
1-2 week	Select a project idea and write the project proposal
3-4 week	First configuration base pipeline of ELK Stack and Backend
5-6week	Second configuration base pipeline of ELK Stack and Backend, Frontend
7-8 week	First Test log collection, processing and analysis. Backend, Frontend implementation
9-10 week	Interim check. Second log analysis, backend configuration, frontend implementation
11-12 week	Log analytics visualization with penetration testing and correlation analysis
13-14 week	Final check and build and run