ISTANBUL TECHNICAL UNIVERSITY
Faculty of Computer Science and Informatics

CYBERSECURITY ENGINEERING INTERN

INTERNSHIP PROGRAM REPORT

HAKAN DURAN
150200091

SUMMER / 2023

Table of Contents

1 INFORMATION ABOUT THE INSTITUTION

Intertech is an information technology company providing financial software solutions. Their customer base consists of banks, electronic payment services, and other financial institutions. Intertech is one of the dominant companies in Turkey in the sector of financial software solutions. The company has six branch offices, including its central office located in Istanbul. Intertech's other offices have a presence in Ankara, İzmir, and Vienna [1]. My internship is affiliated with the central office located in the Pendik district.

Within Intertech, numerous departments operate cohesively, each employing the Agile methodology to streamline their operations. A remarkable 85% of product development teams within the company have embraced Agile transformation practices. The company has 1,400 employees. Among the employees, there are software developers, business analysts, system, network, and cybersecurity experts. At the helm of the institution, Ömer Uyar serves as the General Manager, with Hakan Ateş acting as the Chairman of the Board [1].

Intertech has projects in fields of cloud services and financial systems. They have more than 100 products. Examples of notable projects include the development of anti-fraud systems, stable cryptocurrency production, and various financial applications [1].

One of the notable projects undertaken by Intertech is the provision of security solutions for Deniz Bank, involving the use of SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) applications — an area closely aligned with my internship experience.

2 INTRODUCTION

In my internship, I had the opportunity to gain hands-on experience in using Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) technologies to investigate playbooks, analyze logs, respond to security incidents, and access servers to address alerts and other security-related issues.

3 DESCRIPTION AND ANALYSIS OF THE INTERNSHIP PROJECT

My job during the internship was mainly on improving the stability and security of company servers. Among the cybersecurity solutions of companies, SIEM and SOAR tools are mostly used [2]. SIEM and SOAR tools are mostly used in Intertech for the following purposes:

- Ensuring the security of servers in Deniz Bank and Intertech
- Providing retrospective information by collecting logs from servers
- Creating routines for server security using playbooks
- Providing necessary notifications to cybersecurity teams by creating incidents in abnormal situations

During my internship, I used SIEM and SOAR tools to examine the logs and events coming from the servers at Layer2 level. Intertech uses Humio and Arcsight software as SIEM. XSOAR software is used as SOAR. The XSOAR creates more celebratory incidents using artificial intelligence from logs created by SIEM application. What we do as L2 employees are:

- To examine whether the incidents reported within XSOAR are true positive or false positive.
- Performing necessary routines using playbooks
- Providing information to teams in order to respond to external requests which comes from other teams.

3.1 INCIDENT REVIEW

XSOAR subjects the logs from Arcsight and Humio software to certain artificial intelligence algorithms and reports an incident when it detects anomaly. Which of the L1, L2 or L3 teams this incident will go to is determined according to predetermined playbooks. For example, if the incident is critical, it can be investigated directly by L1 teams. Thanks to the playbook, we know what we need to do when the incident reaches us. We may be asked to examine some places in the playbook and write down the results we reach to the specified place in the playbook. As a result of the incident investigation, we examine whether the incident is a false or true alarm. If it is true, we label it as true positive, if it is false, we label it as false positive incident. If it cannot be determined exactly, we forward it to the L1 teams.

Incidents are breaches that are detected by cybersecurity software and require investigation. Software transmits some incidents to experts thanks to the algorithms they contain. It is essential for experts to evaluate these incidents correctly, because if they are not evaluated correctly, it may cause a compromise of corporate information.

Logs are collected from enterprise devices to create an incident. Logs collected from all devices, with priority given to devices such as Firewall, IDS and IPS, are collected on a selected server. The manager software connects to this server and makes the logs readable by performing correlation and aggregation on the logs. SIEM software used within Intertech are ArcSight and Humio. While Intertech has had ArcSight software for a long time, they have just purchased Humio and started testing it. While Arcsight products are widely used in Intertech and Denizbank servers, i will firstly introduce Arcsight product.

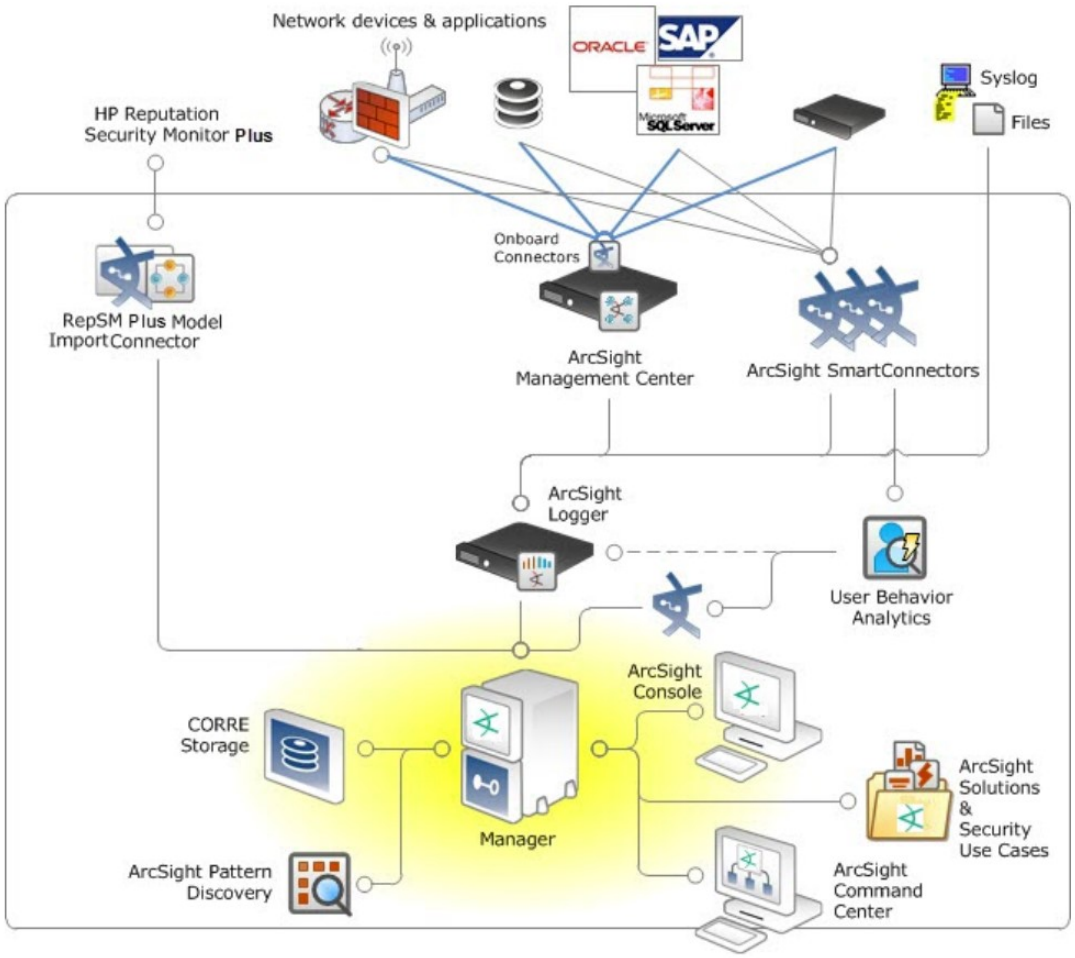

Figure 1: ArcSight products and components creates a management system for enhancing security for enterprises [3].

Arcsight products are deployed and configured in a lot of servers. SmartConnectors, ArcSight Management Center, ArcSight Logger and Manager can be seen from figure 1.

There are Arcsight connector devices on network, which named as SmartConnectors. SmartConnectors are interface for devices whose logs will be gathered. SmartConnectors are parsing logs and normalize them into a common schema. Aggregation and categorization process is also happening here. In the end, it passes events to the Manager after they have been processed.

A management center application has been developed to manage ArcSight software located in many locations from a single interface. ArcSight Management Center (ArcMC) is a centralized security management center that manages large deployments of ArcSight solutions such as ArcSight Logger, ArcSight Connectors through a single interface. ArcMC is a hardware device that consists the SmartConnectors in a single device with a web-based interface for centralized management. ArcMC can control hardware or software-based SmartConnectors or remote ArcMCs.

ArcSight Manager is the most important area for the ArcSight enterprise security system. Manager comes with default configurations. However; rules and network models can be reconfigured. Manager can be thought of as the administrator and adjuster of the system. It also has correlates logs using CORR-engine (Correlation Optimized Retention and Retrieval Engine).

ArcSight Logger is an event data storage device which is optimized for extremely high event throughput. Logger device stores security events in compressed form. Using multiple Loggers to work together leads to scale support high input rates. In each logger, Arcsight Management Server Agent should be installed in order for logger server to provide log data to ArcMC [3].

By using this security management system:

- Logs from network devices are normalized, correlated and aggregated.
- Incidents created and ready to be investigated with the help of ArcMC.

Correlated data shows itself as an incident in SIEM application, in our case they are ArcSight ESM (Enterprise Security Management) or Humio. Humio is not a system but using Arcsight loggers for his input data. Intertech has started to use Humio because they find hard to use ArcSight log search console.

SOAR applications has some differences with SIEM software in context of incident review:

- Using artificial intelligence to detect unnoticed incidents
- Using playbooks for incident review

Incident review and handling can be done manually, but using predetermined playbooks is an innovation because it makes easier and faster to handle possible security attack. Intertech has selected XSOAR software for its SOAR solution. XSOAR gathers its data by using Arcsight products.

In the XSOAR application, there is dashboard and incidents tabs. Dashboard gives a general information about security of enterprise network. Incident tab lists all incidents to be investigated. An incident can be thought of as a SQL entry. Each incident has ID, Name, Type, Severity and a lot of other attributes which makes incident information detailed and unique.

In order to investigate an incident, one should select the incident and follow the playbook. Playbook says what should be done with the incident and asking questions about the incident. XSOAR can want SIEM search console data about the related incident. It can ask if the incident should be investigated by Layer 1 team. After all predetermined questions are resolved, we should determine what is the final mark of the incident. There are some options for that:

- Forward incident to Layer 1 team
- True positive incident
- False positive incident

If the capability of Layer 2 team members are not enough to resolve incident, then incident is forwarding to Layer 1 teams. Layer 1 team has the most skilled experts of cybersecurity, and they cannot forward to anywhere since there is not more skilled team in the Intertech Security Center.

If incident is reviewed and it is thought as a true positive incident, that means there is possible attack to the enterprise network. All the cybersecurity handling teams are alerted to quick handling of the threat. They can suspend some servers, reach risked devices or ban the attacker from system by using firewalls.

If incident is reviewed as false positive incident, that means SIEM and SOAR applications were wrong, or there is a problem with correlated log data, leads SIEM and SOAR to interpret data wrongly.

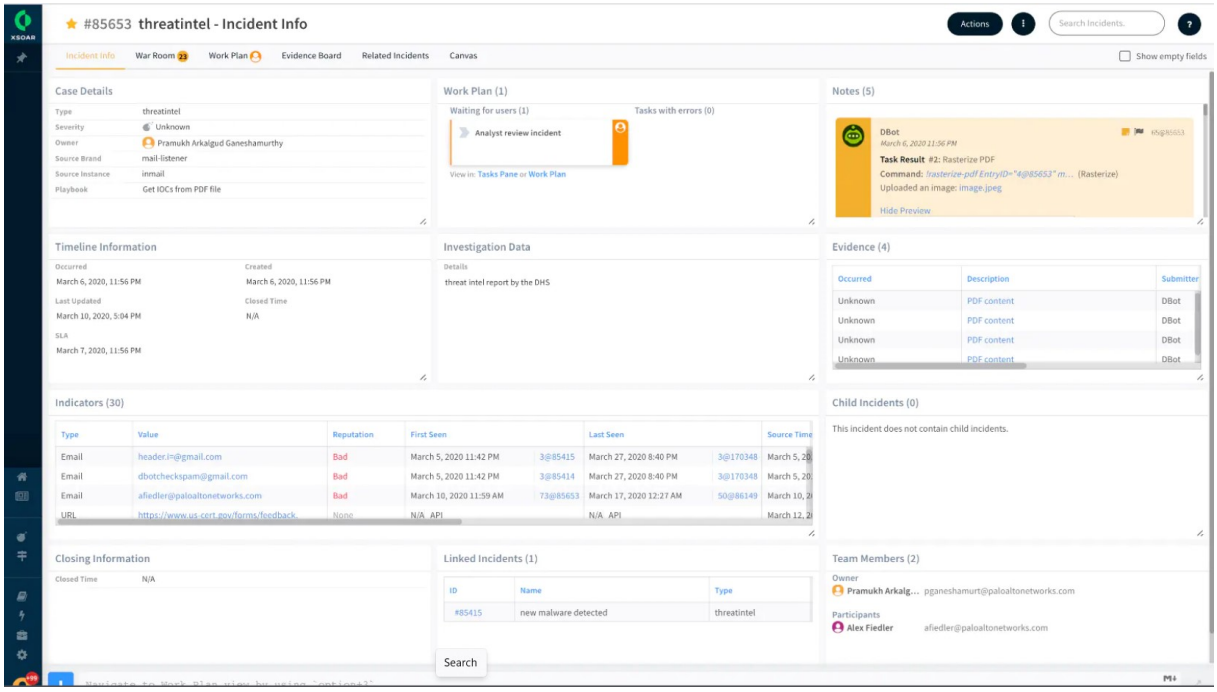

Figure 2: An example of incident can be investigated. This screenshot is not from Intertech, since they do not let me to share any picture.

In the figure 2, it can be seen there is a lot of information about the incident. I dealt with these kinds of incidents while doing my internship at Intertech. By following the Work Plan, the incident can be resolved. In this figure, work plan is waiting for an analyst to review incident. There is also another type of information like timeline and indicators.

If playbook wants us to investigate log data from SIEM, SIEM console should be opened and necessary input should be given to SIEM console. By using that, we manually looks correlated log data and arrives some conclusions about the incident.

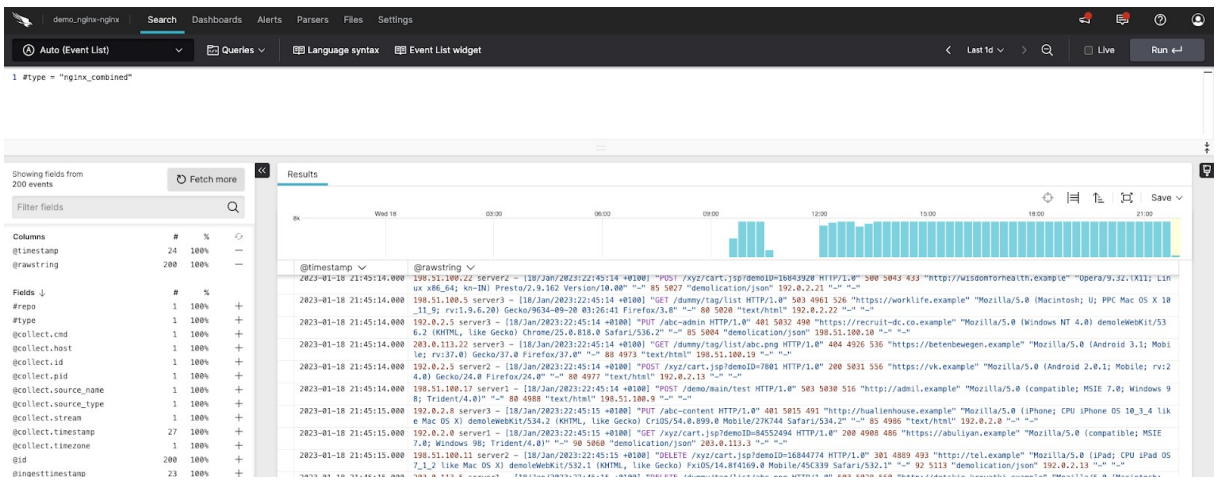

Figure 3: Humio SIEM shows logs related to input query. This screenshot is not from Intertech, since they do not let me to share any picture.

In figure 3, of all the logs, only events which has a type of ”nginx_combined ” listed. By using SIEM for our search, we can manually investigate all logs one by one. But we also have the chance for reaching number of events.

In the left, we can see there are 200 events which has the type of ”nginx_combined”. In those events, only 24 of 200 events has timestamp. In the upright, it can be seen when the logs

came by looking time chart. There were no events until 9 am. Events start coming a little after 9 o'clock, but around 11 o'clock the events do not come again. Events start coming again after 12 o'clock. This could tell us that the server was turned on on January 18th, and after it was turned on, there was an outage between 11 and 12 o'clock.

In the downright, logs can be investigated one by one. The lowest event says that the event has happened when the time is 21:45:15. Since it is a log from the unknown network, guessing what happened is hard, but using some intuition can help. It happened to server2, which can be predetermined server name in the network which Humio SIEM gathers the logs. And server's IP is probably is 198.51.100.11. It was probably a HTTP request which has method "DELETE". That request has been send to "http://tel.example", by probably using an iPad.

By manually investigating of logs, we may detect a suspicious event. It happens when there is a problem about acquiring logs for SOAR. For example, a malicious http request as "GET http://example.com?id=1 OR 1=1;–" can come. If the network has been crushed and there were issues with capturing or transferring logs between SIEM and SOAR, this type of event may not be captured from SOAR software. By manual investigating, we can say that an external threat actor is trying to reach database.

When using playbooks for incident review, SOAR can also want screenshots about investigation of logs in SIEM.

Another process can be wanted is that reaching the actual servers. It can be done by using SSH or RDP. mRemoteNG is an application which stores enterprise network devices and provides a login display. By using mRemoteNG, we can login into necessary device and analyze what happened with the help of local logs. While ArcSigth collects logs from almost any device, communication between SmartConnectors and devices can be failed and unfortunately, it is common. Investigating the reason of disconnection is a crucial part of a layer 2 team member.

Throughout my internship, I have investigated logs manually with the usage of SIEM search consoles. I have taken a lot of screenshots of SIEM application in order to provide necessary pictures for XSOAR playboooks. My another job was login into devices and searching the reasons of disconnection of end-devices with ArcSight SmartConnectors. Sometimes the disconnection do not only happen between the end-devices and SmartConnector, disconnection between SmartConnectors and Loggers, Loggers and ArcMC or SmartConnector and ArcMC can be happening.

Thanks to incident review, i have learned about how a security incident is created and alerted. By analyzing incidents and logs, i can say that i gained experience on logs, incidents and identifying patterns of messages whether they are malicious or not.

3.2 USING PLAYBOOKS

Playbooks tell you what to do when an incident is reported, but there are other areas where they can be used.

An example can be given that there is a routine called health check every Monday. During this routine, Intertech layer 2 team checks the log history of all its Logger servers using ArcSight. Loggers are event data storage devices and they are crucial part of the enterprise security system.

There are many loggers in Arcsight. Each of these loggers collects logs from certain servers and creates graphs that gives insights about these logs and the network area which the logger is responsible.

The routine is being executed by the help of consulting company. Consulting company provides necessary knowledge and guidance. But more important thing is security team should follow predetermined playbook. In the playbook, how a routine should be carrying out is determined.

The health check playbook follows those steps:

- Log in ArcMC firstly, since they have all the logger server's IP addresses.
- Log in each server using IP address and the password.
- Investigate graphs and check if there is any anomaly.
- If there is anomaly, find the reason.
- If there is not, start to investigate another logger.

If there is an anomaly in the graph, we look at the logs in SIEM to detect it. We use the search software installed in SIEM to retrieve the logs we want from all the logs.

For example, we can use the following code snippet to list all logs that include Microsoft among all logs, whose device product is Microsoft Windows, and whose Event Class ID is 4625:

```
Microsoft and deviceProduct = "Microsoft Windows"
and deviceEventClassId CONTAINS "4625"
```

The reason of using this query as a search in SIEM console is Windows events whose ID is 4625 are so common that it shows for the logger if it was active for the checked period time. By using this query, we can understand the anomalies like getting no logs for a certain period of time. If the problem is valid, we can check which time we have started to getting no log.

It was one example of playbook, and those playbooks can be thought of as if-else conditions on what should be done. Playbooks can be triggered manually or something occurs (like an incident shows up).

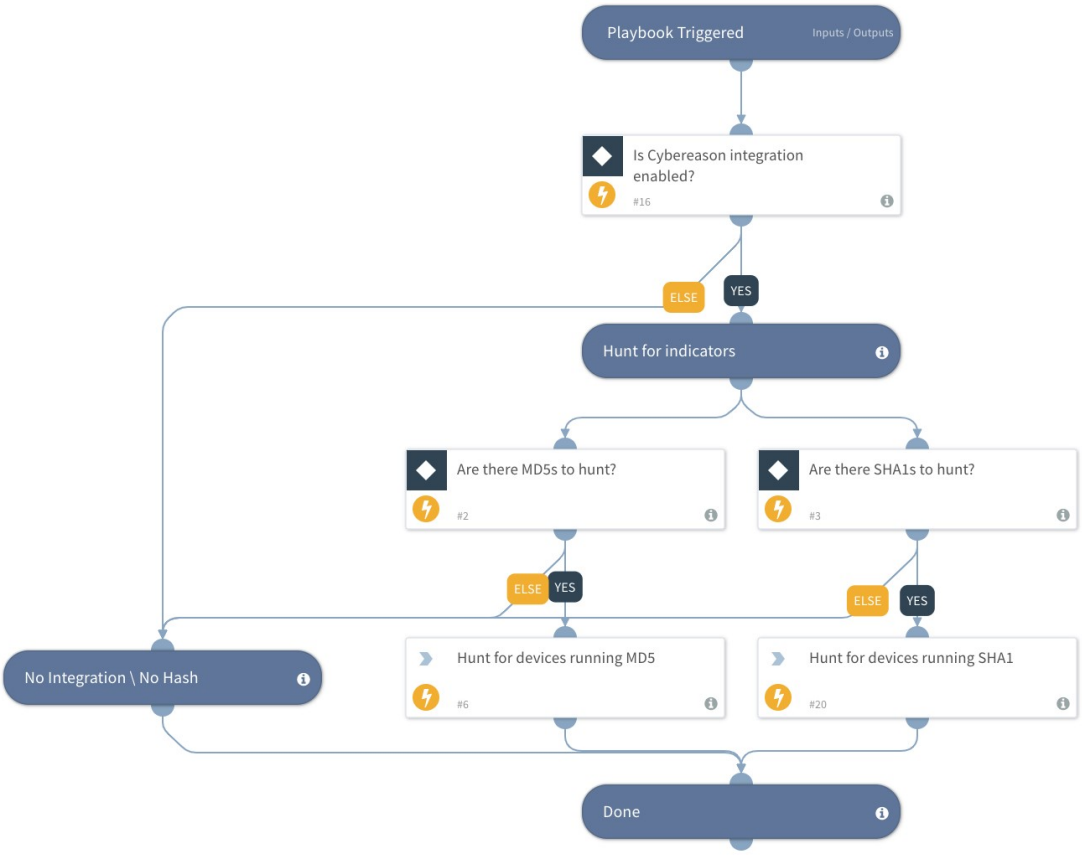

Figure 4: An example of a playbook for hunting endpoints based on their MD5 or SHA1 values.

An example of playbook can be seen from figure 4. This playbook takes input values as MD5 and SHA1 values. Then it searches among endpoints which has that values. [4]

The first question is ”Is Cybereason integration enabled?”. Cybereason is endpoint detection and response solution. In order to use this playbook, Cybereason should be integrated into the endpoints. Otherwise, ELSE will be used and as an output, playbook will give ”No Integration / No Hash” as output. If there is Cybereason integration, then it will give a comment on starting for hunting for indicators. It will look if we have provided any MD5 or SHA1 value. If we did, then hunting for devices will be started. Playbook output is endpoint’s hostname name as type of string. [4]

Another use cases for playbooks can be listed as:

- Creating tasks for another employees
- Blacklisting or accepting a user or IP for the whole network
- Carrying out authentication, authorization and accounting operations
- Ensuring that tasks that involve forgettable processes are completed accurately

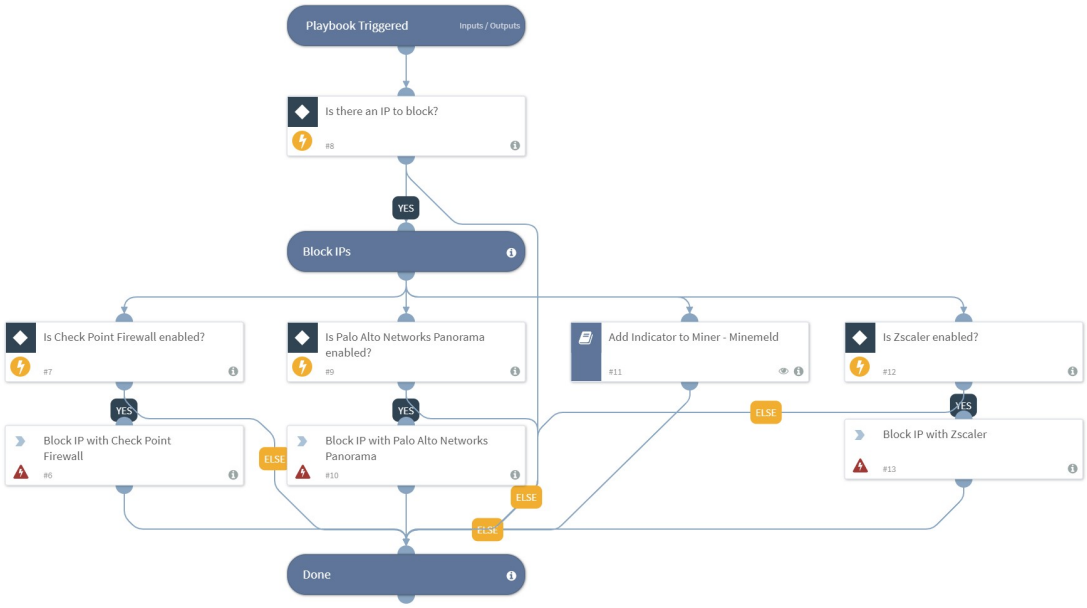

Figure 5: The playbook which ensures that IP has blocked from all the network [5].

As it can be seen from the figure 5, an IP block operation has completely done for all the network devices. If a person would try it manually, may be it can block IPs for firewall, Panaroma and Zcaler. But there is a chance for forgetting blocking IP for Miner - Minemeld. Using playbooks gives precise completion of the task.

A playbook can consists of another playbooks. For example, when an intruder has been detected, there may be a lot of playbooks to be triggered. Firstly, network can be scanned if there is any harm. Scanning whole network can be done easily with usage of one playbook. But, scanning network is not enough. Intruder should be detected with the help of SIEM and SOAR applications. Detecting IP is another playbook, and banning this IP from the whole network is another playbook which can be seen from figure 5.

XSOAR software comes with already existing playbooks, but of course one can create a new playbook. Playbooks have some necessities like inputs, scripts and flow of the chart.

In my internship, I have dealt with some playbooks. Thanks to those playbooks, I was aware of what should be done. Also, investigating playbook is giving a new insight of what a malware can do or what can be defense ways of an attack. Reading playbooks’ blocks and their scripts gave me invaluable skills for my future career.

3.3 TECHNICAL CHALLENGES

During my internship, our team has encountered some technical problems. I can give an example of a problem in the issue of communication between Humio and XSOAR software.

Humio was storing names of the software from which it collected logs in capital letters. However, in XSOAR, software names were stored differently. The first letter is capitalized, other letters are lowercase. This situation was creating incoherent communication.

For example, while XSOAR was storing Windows software as ”Windows” itself, but Humio was storing it as ”WINDOWS” after correlation. Since XSOAR is gathering their data from SIEM’s correlated log data, XSOAR was convinced that because there was no log from machines with Windows, these machines were down, or there may be possible DOS or DDOS attacks to the Windows machines. This problem was solved with support from an external consultant company.

Another problem was from a logger. ArcMC is storing the list of loggers. But one logger seems that it does not give any log to any ArcMC. And that logger server was on. As a team, we couldn’t understand the reason why ArcMC and the logger could not reach each other.

Firstly, we have thought that SmartConnectors and logger server cannot reach each other. That would be simply because logger cannot accept the logs from connectors. Because there is no chance for all the connectors become broken. But then we saw that logger accepts logs and storing them.

After that, we have thought may be it was because logger does not give logs to their external interface. We have decided to observe the output signals from logger whether it is forwarding logs. After observation, we saw that logger give logs to his external interface.

As a final solution, we have decided to change port for logger output signals, but again it did not work. Although port changes, we still couldn’t achieve it to work, that may mean there may be some rules in routers or firewalls. After some tests on firewalls, we saw that new configurations has been added by network teams. We have created a ticket to network teams to let us using that port.

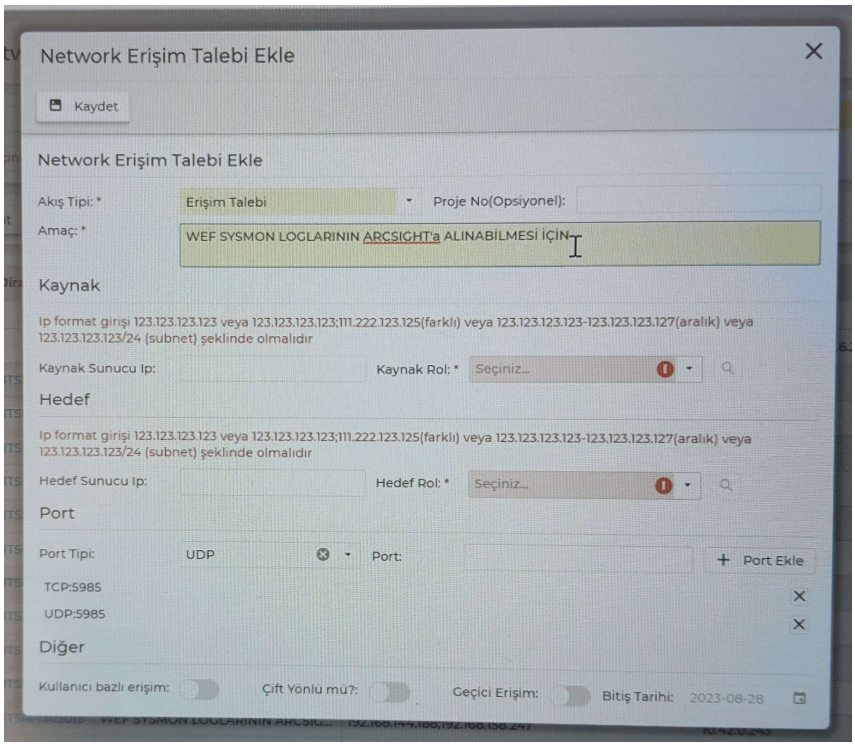

Figure 6: The ticket to network teams in order for letting logs to arrive to ArcMC

Intertech usually have more stringent security policies due to their clientele, primarily consisting of banks. And this situation leads to having so much closed ports.

4 CONCLUSIONS

Working with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) applications, I gained experience in incident response, log analysis, and server management.

From an engineering perspective, I would like to offer some suggestions for institution's engineering capabilities. They should deploy much more management servers in order to reach servers' configuration or software/hardware data. It consumes time and effort to log in each server and pull the relevant data. SOAR and SIEM communication should be better configured and structured. False positive incidents due to broken configuration reduce employee motivation and work time. The process of writing and using scripts is less than necessary. From time to time, I observed performing operations manually instead of using more efficient time and effort with the use of scripts.

In conclusion, this internship has offered insights and knowledge that have enhanced my understanding of the engineering landscape within the organization. It provided me technical skills and a deeper understanding of the intersection of cybersecurity and finance. However, I have also learned that becoming professional in cybersecurity requires effort.

5 REFERENCES

[1] Intertech. (2023, Nov. 5). *Intertech Annual Report 2021* [Online]. Available: https://www.intertech.com.tr/Faaliyet-Raporu/2022/TR/Intertech-2022-Faaliyet-Raporu.html

[2] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, pp. 15–16, July, 2021, doi: 10.3390/s21144759

[3] Micro Focus Security. (2021) *ArcSight ESM 101*. [Online]. Available: `https://www.microfocus.com/documentation/arcsight/arcsight-esm-7.5/pdfdoc/ESM_101/ESM_101.pdf`

[4] Palo Alto Networks, "Search Endpoints By Hash - Cybereason," *Palo Alto Networks*, 2023. [Online]. Available: `https://xsoar.pan.dev/docs/reference/playbooks/search-endpoints-by-hash---cybereason#!`

[5] Palo Alto Networks, "Block IP - Generic," *Palo Alto Network*, 2023. [Online]. Available: `https://xsoar.pan.dev/docs/reference/playbooks/block-ip---generic`