CASE STUDY

Holistic view of Threat Intelligence

INDUSFACE™

ABSTRACT

- This case study reveals the implementation of SIEM done for an analytical company where they need an effective and feasible way to analyse real-time security alerts and patterns produced by our Apptrana Solutions.

  One of our Customer we known to be the most prominent analytical companies who is serving their business for more than 15 years and completed 1000+ projects. Their main business offerings are Data Science, Business analytics and Data Engineering. To serve this services, they are using large cloud-physical hybrid network & stores a huge amount of data.

KEY CHALLENGES

- As customer is using our Apptrana product to secure their web application and installed other Network layer devices in their infrastructure. Due to the ongoing zero day attacks, DDOS attacks, Slowloris attacks, downtime alerts from Apptrana Solution get missed, which is impacting their business in various ways such as:

1. During the incident handling, they don't have any proper steps to take forward because of insufficient data.
2. Continuously effecting the Business Compliance and regulations.
3. Difficult to analyse the huge humungous data when any incident occurs.
4. Difficult to find and react to security breaches, threats & downtime.
5. Their technical team fails to collect all the data to create a comprehensive reports.
6. They can't be detected any unplanned changes being made in real time and alerting mechanism to any unusual activities.
7. Apptrana helps them to block malicious activity on their application, but they fail to manage the alert coming through the Apptrana product.
8. Lost revenues as a result of avoidable downtime.

- Overall, Customer's requirement is to get a real time threat intelligence solution to safeguard their own and their customer's confidential data from threats and other attack vectors along with our Apptrana solution. Hence their security team restructure the technology squad where Apptrana keeps on blocking and alerting about the threats and they need to monitor those alerts through their internal security monitoring team to have a complete comprehensive security program.

  Even though, to deploy any SIEM within the infrastructure, the main challenges were:

1. They need to integrate the Apptrana solution with SIEM.
2. Out of many other devices and appliances in scope of implementation, which do not have the direct integration and the generated log formats were might be not supported by the SIEM Engine.
3. Customer needs the expert person who can manage and handle the outcomes of the SIEM.

STRATEGY & RECOMMENDED SOLUTION

- We recommend to integrate the SIEM solution with our Apptrana product which is compatible with top all SIEM solution provider and our team helps them to integrate the SIEM with our Apptrana solution.

IMPLEMENTATIONS

- After implementing the SIEM solution with our Apptrana WAF, client can retrieve the attack details from the SIEM services which enabled in Apptrana portal. As it's fulfilled the requirement of the customer to fetch the attack logs from the Apptrana in a proper format which helps them to analyse it easily and quickly. They can now view the following parameters as in a log format.

1. Time Frame: It specifies the start and end time of the incident.
2. Event Type: It specifies either the request get LOG or BLOCK.
3. Access Token: It is mandatory while requesting and should be passed in authorisation header.
4. Website name: Name of the Website for which details should be retrieved.
5. API Details: The API details which contain the endpoint, Header, Request Body without website, Success Response, Error Response.

RESULTS:

- This organization now has a secure, stable and PCI compliant IT Infrastructure that can detect unplanned changes in real time, alerting to any unusual activity that can be dealt with appropriately before any damage can be done. After our suggestion and helps in integrating the SIEM solution with our Apptrana WAF, they feel secure in various ways such as:

1. Drastically reduce the security incident investigate time.
2. Take proper steps when the alert of DDOS attacks being provided by the Apptrana solution through SIEM.
3. Gained ability to prevent lost revenue from unnecessary e-commerce and point of sale downtime.
4. Achieved cost savings by shutting down unnecessary Amazon web Services instances.
5. Their team can now constantly monitoring of their application and suspicious activities.
6. Their monitoring squad can prevent and react to security breaches, threats and any downtime alerts.
7. Identify the improvement based on the facts in the comprehensive reports.