www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 12 December 2018, Page No. 24430-24432
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i12.03

Network Security Enhancement using CTI and Log Analysis

Ravi Kumar[1], Parvesh Kumar Chaudhary[2]

[1]ICERT, New Delhi
[2]ECIL, Hyderabad

Abstract:
Cyberattacks, ever increasing in severity, complexity and frequency are impacting the functioning of citizens, government, and businesses around the world. Protecting valuable intellectual property, business and personal information in digital form against theft, misuse, is an increasingly critical concern for everyone in the present digital era. The financial and reputational loss incurred due to Cyber-attacks motivate organizations to improve defensive measures to protect their organizational networks and information stored. This paper proposes a Cyber Threat Intelligence (CTI) collection, log analysis and automated Threat alerting platform capable to analyze and respond to incidents that can lead to cyberattacks. The proposed system makes use of CTI received from Open Source intelligence (OSINT), Elasticsearch and Logstash to analyze, observe and generate alerts for malicious traffic/ activity in organization based on log analysis. At the same time an easy to understand visual representation can be made by the use using Kibana.

Keywords: Log analysis, Network Security, Vulnerabilities, ELK, CTI, OSINT

I. Introduction

A. *Cyber Threat Intelligence*

[1] defines Threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to information assets that can be used to take informed decisions for tackling the menace or hazard". STIX is an international cybersecurity community effort developed by members of community from industry, academia, and government organizations from around the world to represent Cyber Threat Information (CTI) in a standardized structured manner in terms of incidents, cyber observables. Incidents are represented using Indicator Exchange eXpression (IndEX) language which uses Cybox for representing cyber observables.

Cyber Observable eXpression (CybOX) is a standardized schema for the specification and characterization of events or stateful properties developed to standardize the transfer of Cyber threat information across the entire spectrum of security activities, tools and services. STIX standard is still evolving with the recently released STIX 2.0 has moved from XML representation to JSON format.

In Fig. 1, STIX feed for malicious domain is displayed collected using a Taxii client written in Python using Taxii client library (Cabby) and parsed using Stix library available in python. The CTI feeds can also be fetched from Taxii servers using several taxii clients available like cabby which can be stored in XML files.

Fig. 1. STIX for Malicious Domain.

In the SANS 2018 Cyber Threat Intelligence Survey [2], it was concluded by the author that CTI has proved to be useful to operations teams who are monitoring events in the environment, looking actively for threats and responding to incidents due to the early detection and response, managing discovered vulnerabilities, as well as preventing when possible.

B. Introduction to ELK stack

Elasticsearch, Logstash, and Kibana a collection of three open source projects often termed as "ELK" stack, offers end-to-end solution delivering actionable insights in real time for any type of structured/unstructured data. Elasticsearch is a readily-scalable, enterprise-grade search engine partitioning documents across an arrangement of distinct shards that resides across nodes in a multinode cluster, duplicating each shard to provide data redundancy and failover. Logstash is a server-side data processing pipeline allowing users to push data from multiple sources, parse unstructured data (logs) and structure it using its grok plugin and then send it to different indices on the elastic search server.

C. Utility of ELK stack in Log Analysis

In [3] authors have discussed the utility of ELK stack in log analysis and compared its performance with its commercial rival systems. They have come to the conclusion that for small and medium sized organisations with financial constraints, ELK stack proved to be powerful tool, easily adaptable to user's requirement for log analysis with acceptable performance.

II. Proposed System

A. CTI Feeds Server

The CTI feeds available in the form of STIX from various sources is collected, parsed and classified into feed for malicious domain, malicious IP, malicious email and stored on different indices in Elasticsearch feeds server. These feeds will be used for blacklisting malicious traffic originating from organisations network / systems. The following TAXII servers were used for pulling STIX feeds

- https://otx.alienvault.com/taxii/poll
- http://hailataxii.com/taxii-data

B. Log Analysis

The OWASP Top 10 - 2017 [4] mentions Insufficient logging and monitoring as one of the most critical security risks exploited by attackers to achieve their goals without being detected and

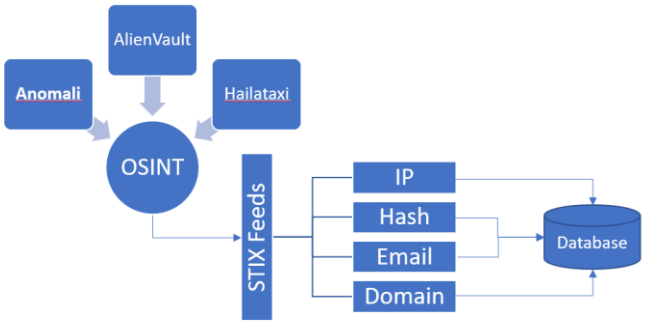

Fig. 2 Stix Feeds Server

preventing organisations from doing in time incident response.

In [5] authors are of the view that Analysis of logs from peripheral network devices, important servers can reveal the gap in safeguards, vulnerabilities or weaknesses that exists in the systems helping to mitigate any potential threats during or before any incidents happened.

The importance given by OWASP to proper logging and monitoring makes it imperative to have a automated log analysis system in organisations. The proposed solution envisages a centralized logs server depicted in Fig. 3, where logs from all the peripheral devices like Proxy servers, Dns Server, Firewalls, Database Servers are pushed to a log server. Logs from Proxy servers, DNS servers are sent using RSYNC to different locations. Firewall like CISCO ASA has the feature to sends syslog on UDP port 514, but protocol and port can be changed depending on needs. Filebeats is configured to monitor any changes in the logs of all the folders where logs are pushed by RSYNC and sends all the updates in logs to different ports. Logstash, an open source product used to send, parse logs with predefined filters for most of log formats and support for custom filters written in basic regular expression which parses these logs and sends these parsed logs to different indices of Elastic Search ex firewall log is sent to IP index.

Multiple pipelines are defined in Logstash through a configuration file called pipelines.yml. Each pipeline is used to listen to a different port / file to get logs as input, grok pattern used / defined to parse logs and send the parsed output to a index in Elasticsearch from a different category of device. Configuration of pipeline is shown in Fig. 3. Here the system is listening for System logs on port 5044

```
input {
    beats {
        port => "5044"
    }
}
filter {
    grok {
        match => { "message" => "%{SYSLOGLINE}"}
    }
}
output {
    elasticsearch {
   hosts => ["192.168.4.125:9200"]
   index => "System-loganalysis-%{+YYYY.MM.dd}"
```

Fig. 3. Pipeline Configuration for Logstash

and sending the parsed log fields to elastic search server running over port 9200 into a index name System-log analysis followed by date of the log event.

Considering the data generated due to the near real time logs pushed from the perimeter devices, the compute power required to search in the indexed log fields will be huge, a cluster of Elasticsearch running systems having minimum two master nodes, and 4 data nodes was created thus overcoming the performance issue.

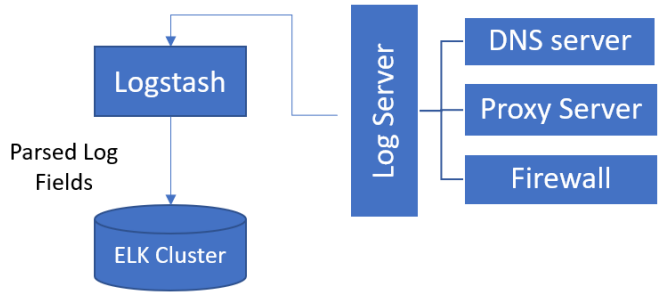

Fig. 4. Elasticsearch Server with parsed logs

As per trend, most of organizations have some level of cyber-attack detection and incident handling capabilities. But building capabilities to take a proactive measure against an evolving threat landscape often need a lot of technical expertise and huge expenses.

challenging. The CTI aids in decision making thus improving the response time. At regular intervals, an Elasticsearch query is done to compare the requests for all domains, IPs and other resources made from organisations network / systems in the last interval duration with the respective collection of STIX feeds stored in another instance of elastic. If a match with any of the STIX indicators from recent and previous cyberattacks, various resources used for the attack (IP, domain, hash of malicious code, vulnerable software, CVE) is found in the events collected from logs, At a configurable defined interval, a comparison is done for all the requests to domains or IP address from the logs in last interval and if there is a entry in a log which matches a blacklisted entry, an alert indicating a event / compromise of a system in the network is raised via an email / telegram message to the respective administrator of system in organisations network or an ongoing attack.

C. Challenges

The STIX feeds are still evolving and building trust is one of the most crucial obstacles amongst CTI stakeholders. There is a need for a Trust Measuring Model for the CTI feeds which assigns a Trust score to each source in the proposed system.

III. References

[1] R. McMillan, “Definition: threat intelligence,” Gartner, 2013, 2013.

[2] D. Shackleford, “Cti in security operations: Sans 2018 cyber threat intelligence survey,”

[3] S. J. Son and Y. Kwon, “Performance of elk stack and commercial system in security log analysis,” in 2017 IEEE 13th Malaysia International

[4] T. OWASP, “Application security risks 2017,” 10.

[5] I. Y. M. Al-Mahbashi, M. Potdar, and P. Chauhan, “Network security enhancement through effective log analysis using elk,” in Computing Methodologies and Communication (ICCMC), 2017 International Conference on. IEEE, 2017, pp. 566–570.