Logging and Log Management and How Useful Are They

"Tech-IT-Easy: 1st Cyber Defense Community Meetup"

Content

- Overview
- What we want to do? (Plans)
- Leverage Coverage
- Collect, Store & Analyze
- Active Response
- Improvement
- Sample popular use case used in SIEM

Overview

What Is Log Data?

Log data is the **intrinsic meaning** that a log message has. Or put another way, log data is the information pulled out of a log message to tell you why the log message generated. For example, a Web server will often log whenever someone accesses a resource (image, file, etc.) on a Web page. If the user accessing the page had to authenticate herself, the log message would contain the user's name. This is an example of log data: you can use the username to determine who accessed a resource.

First off, the typical basic contents for a log message are the following:

- Timestamp.
- Source.
- Data.

Logs Can Be Useful

- Logs can tell you a lot of things about what is happening on your network and operating system, from **performance information** to **fault detection** to **intrusion detection**.
- Logs can be a good source of "**forensic**" information for determining "what happened" after an incident.
- And logs can make an audit trail for (what else?) **auditing purposes**.

What we want to do? (Plans)

- Leverage Coverage
- Active Response
- Improvement

Leverage Coverage

Collect

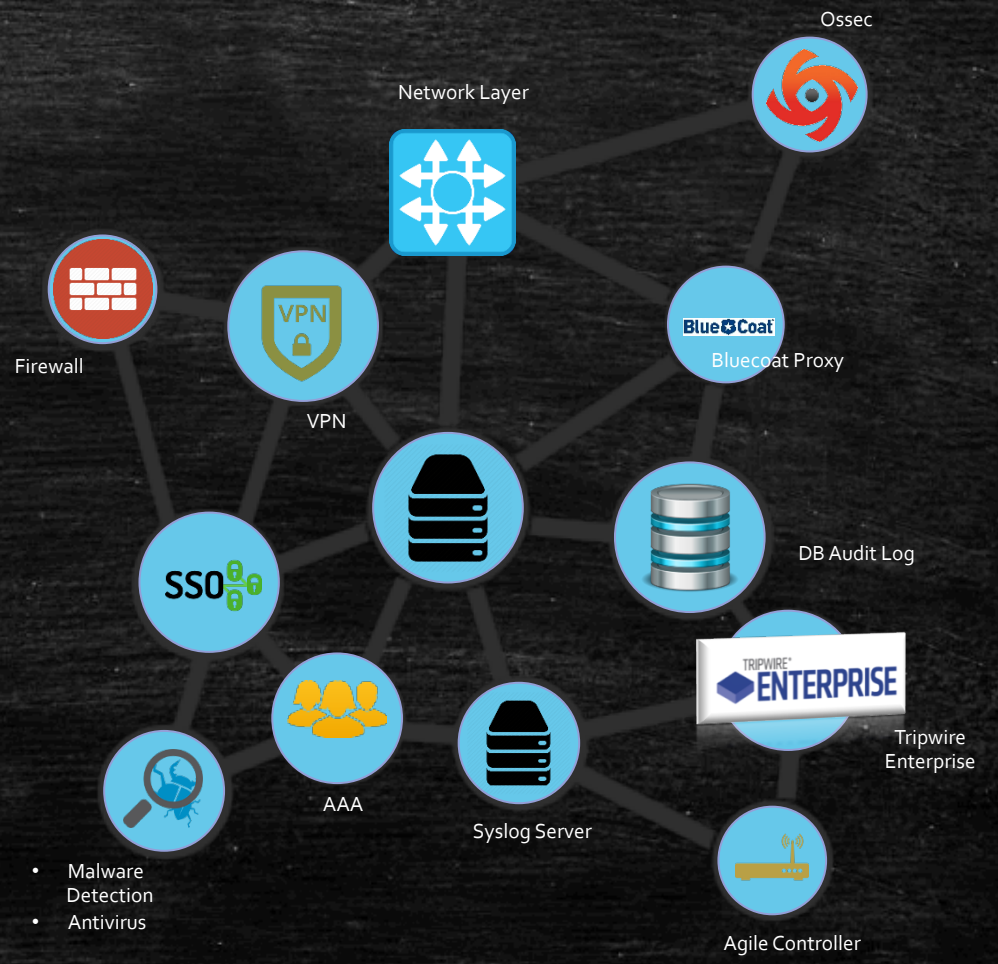
Collect alerts and log records based on the policies defined in the Plan phase.

Store

Collected data must be stored for future access, for both compliance and forensics

Analyze

The collected data is analyzed to identify potential incident



Collect, Store & Analyze

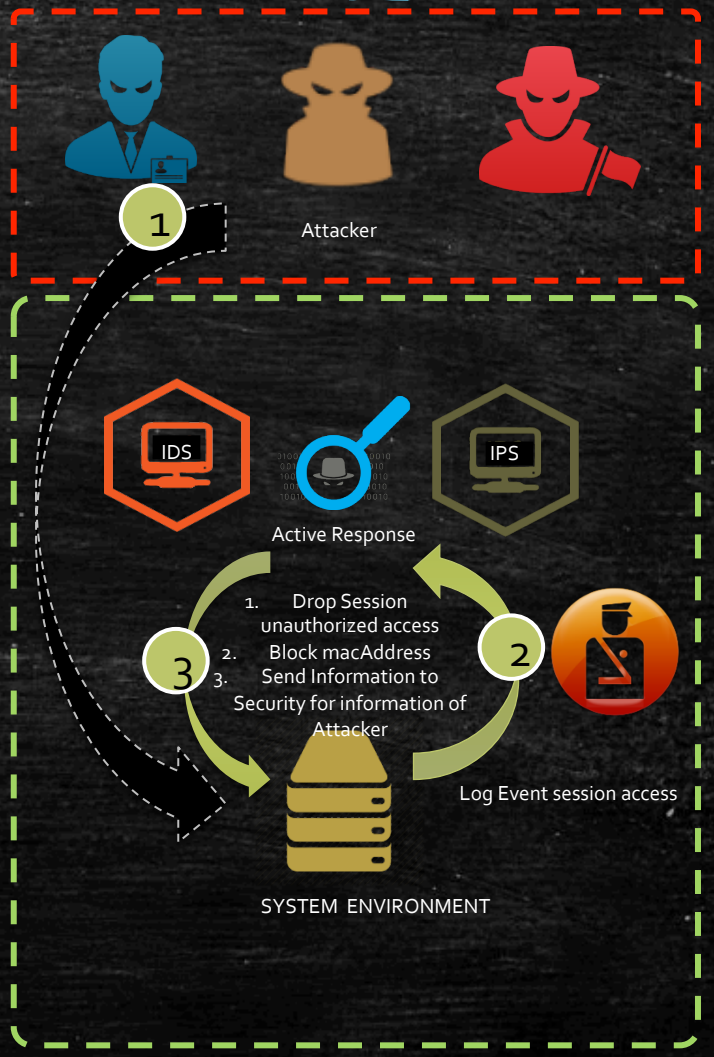
Baseline	Problem	Recommendation
Collect All logs system environment should be collected.	Bottle neck in system environment which cannot generate output log.	Recommendation to enabled logging in our system or applications.
Store There are many logs system data stored.	License Max Space	Upgrade license and using another log management. Log Management development.
Analyze Integrated log must be analyze to enhancement and enrichment use case currently used.	Active response not implemented yet. Depend in policy	Implementation Active response using SIEM. IPS & IDS Improvement.

Active Response

Active Response is a mechanism in intrusion detection systems (IDS) that provides the IDS with capability to respond to an attack when it has been detected. There are two methods that the IDS can take to circumvent an attack.

Method 1- Session disruption
If there are illegitimate user **successfully** compromised any system, active response should be drop session this user. Then automate tracking IP Address Source and to do method filter rule manipulation (IPS)

Method 2- Filter rule manipulation
If there are IP address brute forcing any system, active response should be **disabled** this mac address in our network.



Improvement

1. Implementation Active Response
2. Research and max SIEM capability.
3. Decrease False Positive using Alert Analytic with use case & Active Response
4. Research and compare another Log Management (GrayLog ,Splunk, ArcSight Logger etc)

Collect : Splunk Forwarder, Syslog-ng, rsyslog, Arcsight agent, Beats
Store : Splunk Indexer, Syslog Server, Arcsight Logger, Logstash
Analyzer : Splunk SIEM, Arcsight ESM, Elastic

Sample popular use case used in SIEM :

1. Warn if 5 failed logon attempts are tried with different usernames from the same IP to the same machine in 15 minutes and after that, if a successful login occurs from the same IP to any machine.
2. Warn if a host scan is made by an IP and then if a successful connection is established by the same IP and then backward connection is established from connected IP to connecting IP.
3. Warn if more than 100 connections are established from the different external IPs to the same destination IP in one minute.
4. Warn if 100 connections are established from the same external IP through different ports to the same destination IP in one minute.
5. Warn if the same user tries more than three failed logon attempts to the same machine in an hour.
6. Warn if a user can’t log into any server and caused failed authentication and in two hours if that user can’t log into the same server.
7. Warn one if more than 100 packets are blocked by UTM/FireWall from the same source IP and don’t warn within an hour. (Millions of packets are blocked in case of DDOS attack. If email is sent for each, you are exposed yo yourself DDOS attack.)

Bibliography

"Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management" published in 2012 by Syngress Publishing (ISBN 9781597496353).

Thank You

Nice to see you
everybody