Homelaber Brasil

Homelab & Virtualização

Virtual Design Master - 2016

Challenge 2

Valdecir Carvalho | Homelaber Brasil | homelaber.com.br | @homelaber | July/2016

Table of Contents

I. Executive Summary 2

II. Challenges 2

III. Assumptions 2

IV. Prologue 3

V. Security Software 4

VI. Challenge Explanations 7

Executive Summary

We've been talking about how fantastic humanity has been over the last few years, and how everyone has worked together to save humanity...but what if that's the view through rose colored glasses? We think we know what we've been dealing with, but what if we really don't?

There is one person on Earth, who has survived the apocalypse deep in the bowls of the SuperNaps, and they have managed to rig up satellite capabilities. One of our brand new datacenter, the closest drop and go datacenter for Earth has been taken over.

While it has not disappeared from any monitoring it is no longer in anyone's direct control. In addition, the black market for goods, services, etc. is accelerating, using your own network against you.

All you know at the time of discovery is that a shipping manifest you created has been changed to include some interesting components, and the shipment has been rerouted to go someplace else. However, you notice this after the shipment has left, there is no time to change anything.

Your challenge is to

A. find the extent of the changes anywhere within the system, what are the prereqs to make this happen

B. be notified of other changes, not just to files but to attack(s), what is the steps of an attack, how fast can you detect an attack and changes?

C. prevent the changes; can you prevent the attack or just detect the attack. If only detection how fast can you make this happen.

D. determine the root of the attack, can we find the culprit, is there any forensics data, where did the 'bad actor' leave his/her fingerprints. Is it the black market or something else?

Challenges

A. find the extent of the changes anywhere within the system, what are the prereqs to make this happen
B. be notified of other changes, not just to files but to attack(s), what is the steps of an attack, how fast can you detect an attack and changes?
C. prevent the changes; can you prevent the attack or just detect the attack. If only detection how fast can you make this happen.
D. determine the root of the attack, can we find the culprit, is there any forensics data, where did the 'bad actor' leave his/her fingerprints. Is it the black market or something else?

Assumptions

- Earth Datacenter has been compromised
- The attacker is an INSIDER and is based on Earth
- I am on Moon
- Someone of the Earth Datacenter lost valuable and sensitive information
- The attacker is in possession of the lost information
- There is a SIEM system running on Moon Datacenter collection data from the Earth Datacenter

- There is a Syslog system running on Moon Datacenter collection log data from the Earth Datacenter
- All SIEM and Syslog systems data is stored ONLY on the Moon Datacenter and are not replicated to the Earth Datacenter,
- There is a full system in place to prevent EXTERNAL attacks and it´s working (i.e.: Firewall Systems).
- The Identity Manager system (LDAP) is based on Moon DC and replicated to Earth DC where it´s read only
- The attacker has access to the HumanityLink software and all the systems on the Earth Datacenter
- I still have access to the physical access control software on Earth

Prologue

After we have setup our shine new Datacenters both on Earth and on Moon, things are going very well to the Human Race.

One night two of the DC staff, João and Marcio were at a Pub having some HEMPBeers celebrating the birth of Marcio first child. They left the Pub around 01:00am and head home. The Pub was almost empty at this time, but they didn't notice a strange sitting alone in a dark corner.

In the following morning, João noticed that he had lost his access badge at the Pub, but didn't report to the DC security manager, as the procedure demands. What he didn't remember is that with his badge was also his flash drive.

This strange was nothing less than Pablo, a hacker who has survived the apocalypse and now became an interplanetary gangster who controls the black market of goods and services.

One week later, in possession of João´s access card and his flash drive, Pablo find his way (using social engineering tactics to lure the security staff) to get inside the datacenter and then have access the VPN firewall and to the HumanityLink system. He now has full remote access in the datacenter systems using João´s credentials.

Pablo now is using the HumanityLink software and the Datacenter network to contraband goods outside the Earth using our ships, changing the shipping manifests without no one notice.

A few months after Pablo´s datacenter invasion, I have noticed that one of the shipping manifests I imputed in the HumanityLink system has been changed and the ship is rerouted to Mars instead of Moon,

I started to look at all the monitoring systems the logs and realize that the systems on Earth Datacenter has been compromised and someone had taken control of it. I was running out of time and the only chance to find out who was the invader was to intercept the ship as soon it arrives on Mars. But

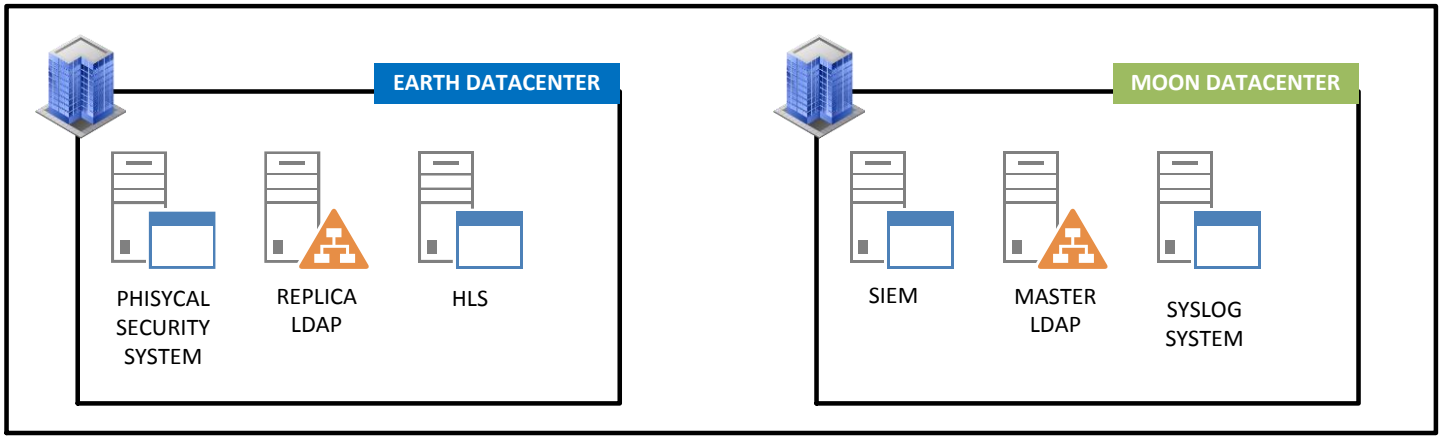
I could not use our communication system, because it was compromised too and the invader should be monitoring everything we did.

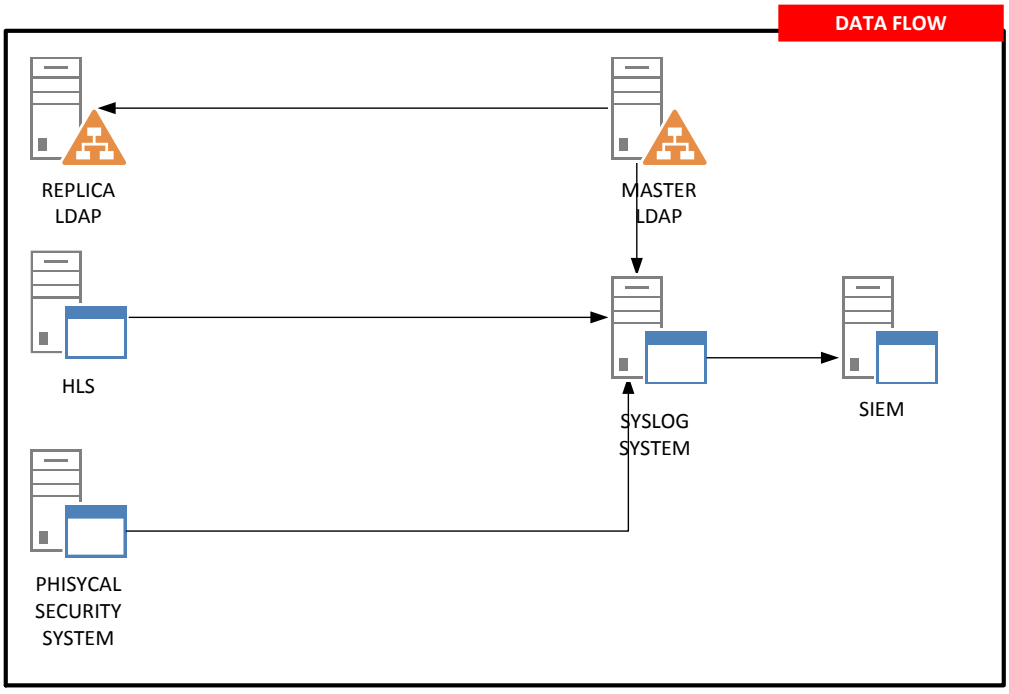
The solution was to use an analogic communication system based in radio signals and not detected by our monitoring systems to reach Mars before the ship arrives.

Security Software

The security soft wares utilized in this design will be the following:

Note: This document is strongly focused keeping in mind the concepts and data security aspects, so the hardware requirements of the software chosen will not be described.





Log System:

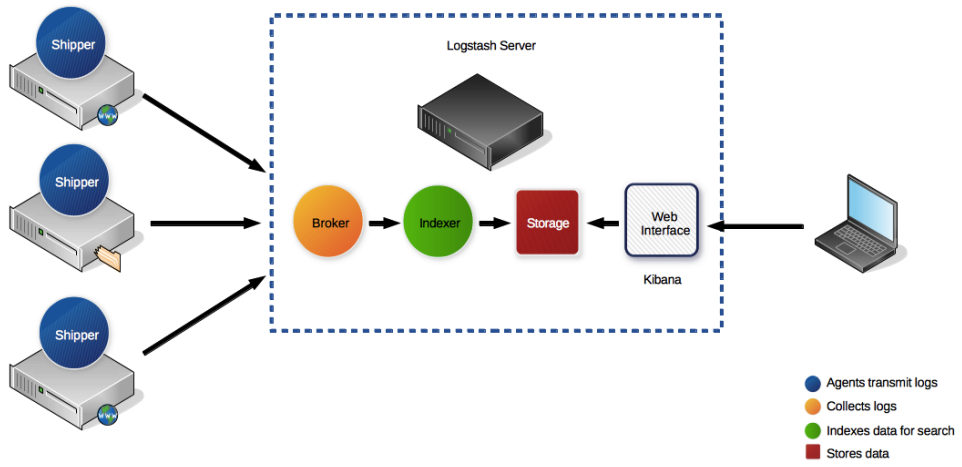
The Log and monitoring system used in this design will be the ELK stack will be use, ELK is an acronym for a collection of three open-source products: Elasticsearch, Logstash, and Kibana.

Elasticsearch is a NoSQL database.

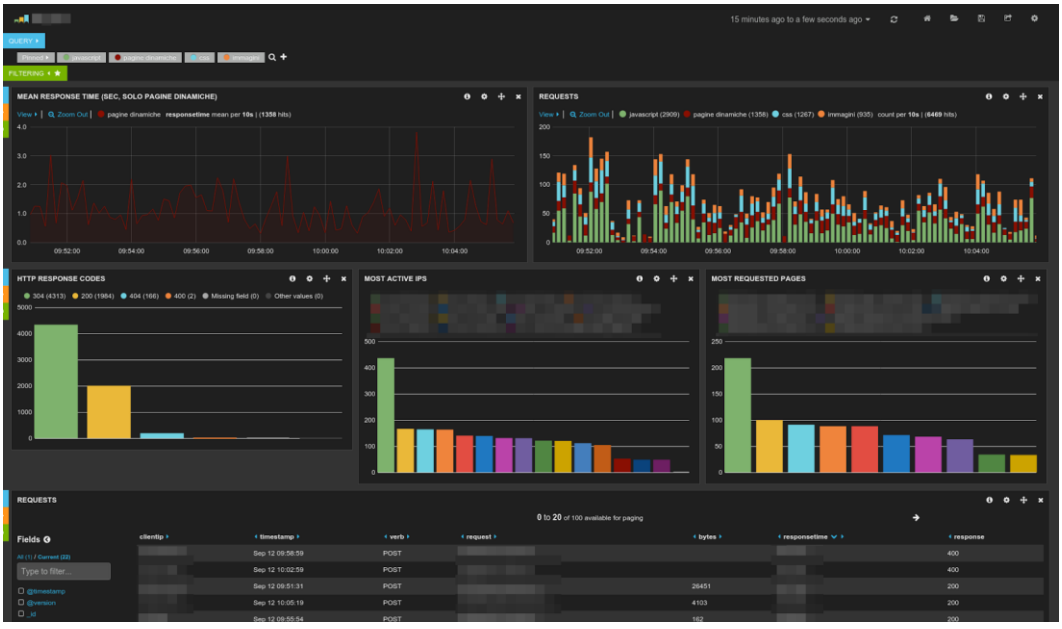
Logstash is a log pipeline tool that accepts inputs from various sources, executes different transformations, and exports the data to various targets.

Kibana is a visualization layer that works on top of Elasticsearch.

Together, these three different open source products are most commonly used in log analysis in IT environments (though there are many more use cases for the ELK Stack starting including business intelligence, security and compliance, and web analytics). Logstash collects and parses logs, and then Elasticsearch indexes and stores the information. Kibana then presents the data in visualizations that provide actionable insights into one's environment.



Graphical representation of how the ELK stack works

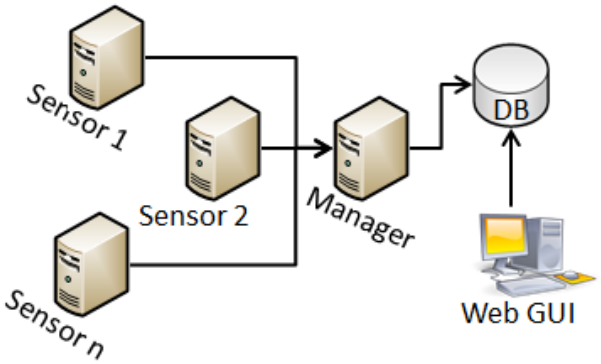


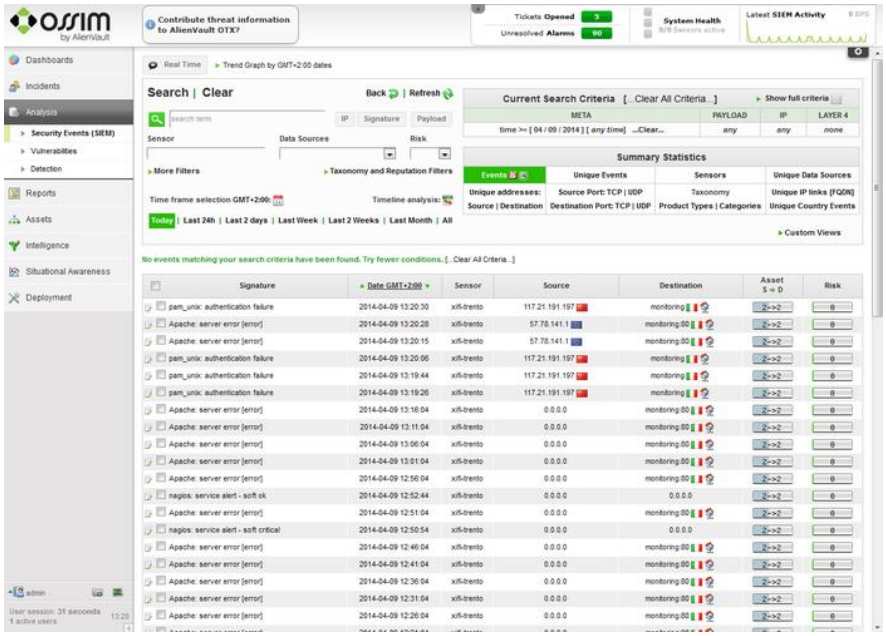
Example of a Kibana dashboard

SIEM System:

The SIEM system used in this design will be the OSSIM from Alien Vault (https://www.alienvault.com/products/ossim)

OSSIM, AlienVault's Open Source Security Information and Event Management (SIEM) provides a feature-rich open source SIEM complete with event collection, normalization and correlation, providing one unified platform with many of the essential security capabilities such as Asset discovery, Vulnerability assessment, Intrusion detection, Behavioral monitoring and SIEM (Security Information and Event Management). It also supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources.





Challenge Explanations

A. The extensions of the changes in the systems only happened on the shipping module of the HumanLink Software. The hacker did not make any other changes based in the forensic analysis results and later investigation interviews with all DC staff members. And the main prereq to the system hack was the human error, when one of the Earth Datacenter staff member lost his access credential key and flash drive at the Pub.

B. Before the attack there was a lack of security procedures and monitoring. The monitoring system was there, but no one was really paying attention to it for three main reasons:
1) The SIEM software was no well setup and was generating too many false alerts, so everybody just ignores the real threat.
2) The staff was not trained to report events to the security team.
3) There are no strict policies and rules applied to prevent data loss,

If Marcio have had reported his access key lost to the security team and did not have been able to transfer sensible data to his flash drive, probably the attack did not happen.

C. After the attack the following procedures were taken to prevent security breaches on the systems:

- Review and improve all the security polices
- Review and improve all the security process
- Train and educate the staff to follow the security policies
- Improve the SIEM system to reduce the number of false alerts to a minimum

- Improve the SIEM system to send automatic alerts and notification regarding system invasions/attacks/treats.
- Improve the security of all the servers, workstations, etc. by implementing strict polices to prevent data loss. I.e.: Disable copy of sensible data to flash drivers and implement an encryption system if the copy is really necessary, Force user to change password expiration in X number of days, etc.
- Create a NOC in the Moon DC to have focus on monitoring the infrastructure to fast detect and treat any anomalies in the system.

D. The root cause of the attack was the data loss/human error. The culprit of the invasion was Pablo who had access to sensitive lost information and used it to gain physical access to the Earth DC and to the systems.

He left traces of his actions but was only discovery after an extensive analysis and correlation of the data on the SIEM system and other data like the security cameras in the DC.

Investigations indicate that he "invade" the Earth DC on a day that João as off duty and all his remote connections happened when João was locally connected to the system, so there were two simultaneous connections of the same user at the same time from different locations. All these traces have led to identification of attacker.