Security Enhancement

CHALLENGE 2: THIS IS WHY WE CAN'T HAVE NICE THINGS!

Katarina Wagnerova
katkaaw@gmail.com
@_KatkaW_
06.07.2016

Table of Contents

1 Mission objectives

What is going on?!

We were all happy about going back to Earth and saving humanity but it seems somebody has different plans. Our Earth datacenter has been taken over, black market is on the rise and they are even using our infrastructure.

Nobody knows what is happening…

What did they change?

Are they still attacking?

How can we stop them?

Most importantly, WHO are THEY?

We need to find answers!

1.1 Requirements

Following requirements have been derived from the mission objective:

#	Description
R01	Detect changes to physical infrastructure
R02	Detect changed to Virtual Machine OS
R03	Receive notifications for configuration changes
R04	Prevent configuration changes
R05	Revert unauthorized configuration changes
R06	Detect attacks
R07	Determine root of the attack
R08	Identify intruders

1.2 Constrains

#	Description
C01	Full control of Earth datacenter has been lost
C02	Someone else can operate Earth Datacenter
C03	There are not enough people to monitor all activities manually
C04	Earth datacenter location is unknown

1.3 Assumptions

#	Description
A01	Data collection tools have been set up prior to the incident and collecting data successfully
A02	We are able to deploy new components to the infrastructure
A03	Small closed group of trusted people exists
A04	Intruders do not know they were detected
A05	Intruders are still active in our network
A06	At least one intruder is an insider

1.4 Risks

#	Description	Risk mitigation
RI01	Intruders' identity not known	Implement Intrusion detection

RI02	Scale of Black Market operations is not known	Monitor Black Market operations to learn about its practices
RI03	Intruders can get suspicious	Carefully plan Intrusion detection techniques

2 Data Collection and Analysis

2.1 Log Insight

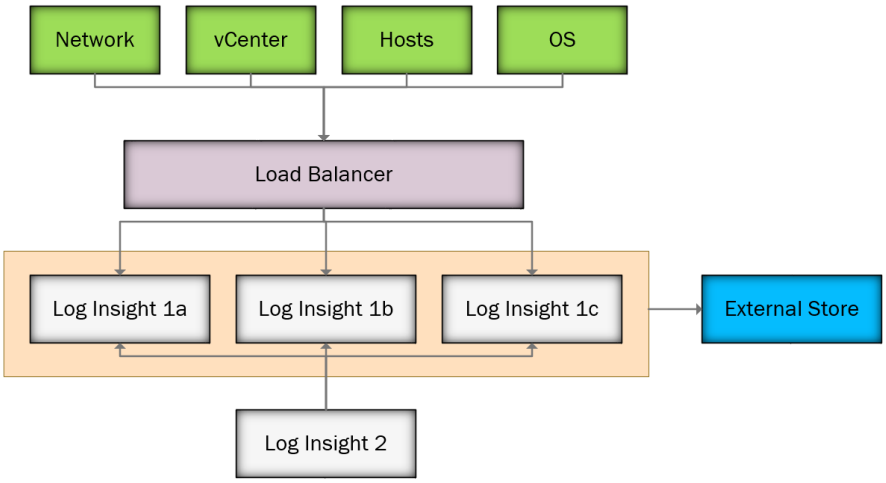
In order to provide a solution to review and manage logs, all infrastructure components will be configured to send logs to a centralized vRealize Log Insight 3.3 deployment. This will allow administrators to search through correlated events coming from all points of the infrastructure, whether it is network, ESXi host, vCenter or Operating systems, all in one place, and will also help to determine what was going on in the time of attack.

We will also enable notifications for certain types of events, such as logging into the infrastructure components. Once we determine who the intruder is, we will be able to set up alerts to notify us about his activity.

Log Insight will be deployed as a clustered solution, with one master node and two works, to allow for node failure. Traffic will be distributed through a Load Balancer.

All collected logs will be also forwarded to an external store for redundancy purposes in case of the Log Insight cluster failure. We do not want to lose all of our logs.

To log and monitor activity on Log Insight cluster itself, we have deployed an additional Log Insight appliance.



Log Insight will be integrated with Active Directory to provide authentication and authorization of users based on Access Policy.

Decision options	1. Leave logs in their default locations and review them manually 2. Configure all components to send logs to Log Insight
Option selected	2.
Requirement met	R01, R02, R03, R06, R08
Justification	Log Insight has been selected to provide a central point for log management and to enhance troubleshooting possibilities for both historical and real-time data.
Associated risks	RI01. Log Insight node failure RI02. Log Insight cluster failure RI03. Log Insight cannot monitor itself
Risk mitigation	RI01. Log Insight will be deployed in a 3 node configuration

	RI02. Collected logs will be forwarded to external store RI03. External Log Insight appliance will be deployed

2.2 Configuration Manager

vRealize Configuration Manager (5.8.2) will be used to control and manage configuration across all systems. Configuration templates has been created for ESXi hosts configuration, as well as OS configurations. This will help us easily check for security compliancy across all platforms, as well as provide us a list of configuration changes that have been implemented after the configuration standards have been created.

Compliancy checks will be scheduled to run every day, alert will be created and notification sent to administrators in case a non-compliant component would be detected.

For any non-compliant components, we will be able to enforce the compliancy and revert the settings to the desired state.

Configuration Manager will also be used for automated patch management for all managed machines. Report will be sent to administrators.

Access to Configuration Manager will be only granted to Trusted Administrators as defined in Access policy.

Decision options	1. Apply host configuration and check compliancy using Host Profiles, manage OS settings and compliancy using vendor provided tools (such as System Center Configuration Manager for Windows and UX management) 2. Deploy vRealize Configuration Manager
Option selected	2.
Requirement met	R01, R02, R03, R05
Justification	vRealize Configure Manager will provide us a central point of configuration management for ESXi hosts, Windows and UX based Operating Systems. It will also provide compliancy checks, settings enforcements, patching and reporting options.
Associated risks	RI01. Unauthorized access to Configuration Manager could have serious impact of the infrastructure as the intruder could enforce changes to all managed components.
Risk mitigation	RI01. Access will be limited to Trusted Administrators and all infrastructure components will be secured to prevent intrusion.

2.3 vROps

vRealize Operations 6.2.1 will be used to monitor performance of hosts and virtual machines running in our environment, with addition of management packs for VSAN and NSX.

Due to the recent events, vROps will be mainly utilize to look for anomalies in workloads. Alerts will be enabled to send out notifications in case an anomaly will be detected. This will allow the administrators to observe and troubleshoot the root cause of the problem.

vROps has been deployed as a 4 node HA cluster, with one master node, one replica node and two data nodes to provide redundancy in case of a node failure.

Decision options	1. Review performance manually using Performance Charts in vCenter and correlate events manually 2. Use vROps for performance monitoring, troubleshooting and alerting
Option selected	2.
Requirement met	R06, R07

Justification	vROps is a great tool for performance troubleshooting with its correlation of events and raised alerts on virtual machines and links to parent, child and sibling objects. It also provides a variety of predefined reports and ability to create custom reports that can be sent to administrators on regular basis. Integration with Log Insight and Configuration Manager is also possible.
Associated risks	RI01. vROps cluster failure
Risk mitigation	RI01. vROps HA cluster deployed to account for node failures

2.4 Notification systems

To allow our administrators to promptly act on events, we have implemented two notification systems. All alert notifications will be send by email to responsible personnel and will be also logged in a ticketing system.

2.4.1 SMTP

Two Microsoft Exchange 2016 will be deployed to provide email services. Database Availability Group will be created to provide high availability.

Both Internal and External SMTP relays will be configured.

Decision options	1. Use external SMTP providers (such as TurboSMTP) 2. Implement internal solution using Exchange
Option selected	2.
Requirement met	R03
Justification	Email notifications are important for alerting and reporting. By deploying an internal solution we will have full overview of all email activities, traffic flows and message tracking.
Associated risks	RI01. Exchange could fail RI02. Exchange could get compromised
Risk mitigation	RI01. Implement clustered Exchange RI02. Limit access to Exchange servers, secure all underlying infrastructure

2.4.2 Ticketing system

All configured alerts in our infrastructure will create tickets in an internal ticketing system.

Tickets will be handled in accordance with Incident and Change management policies.

3 Intrusion Prevention

3.1 Datacenter Security

Access to Datacenters will be limited to authorized personnel only. All visits to Datacenters will have to be approved in advance and documented, engineers will have to identify themselves and sign in upon arrival. Name of the engineer, date and time, brief action description, reference ticket number and signature will be required.

All rack cages will be locked. Security officers will open the cage once the change approval will be verified and will remain present with the engineer during the whole action. As soon as the change will be finished, security officers will lock the cage again and escort the engineer to the exit. Engineer will be asked to sign off before exiting the datacenter.

Video surveillance of premises will be available at all times. Motion detection systems will be installed in all premises. Full lockdown will be executed in case of a security breach.

Unfortunately, we do not have full control of Earth Datacenter. Same security principles will be applied as soon as we will take over control of the datacenter again.

3.2 Network Security

3.2.1 Physical Network

Access to physical network devices will be limited only to authorized administrators according to Access Policy. All devices will be secure with strong passwords following the Password Policy.

All unused ports will be disabled to prevent anybody from plugin in unauthorized devices.

Activity on network devices will be monitored and logged in Log Insight. Notification will be sent out as soon as somebody logs in into the devices. Alerts will be triggered in case of a configuration change. All changes will have to go thought the Change Management process.

3.2.2 Virtual Network

VLAN tagging will be enabled on all distributed switch port groups. All VLANs will be tagged using their respective IDs.

Number of available ports on the port groups will be limited.

In order to protect hosts against MAC impersonation, *MAC address changes* and *Forged transmits* options will be set to *Reject*.

3.2.3 Firewalls

Only allowed communication on predefined ports will be open. All remaining traffic will be blocked.

3.3 Host Security Hardening

All hosts will be properly patched with the latest updates.

Lockdown mode will be enabled, enforcing management through vCenter and preventing logins to the DCUI. Trusted administrators will be added to the exception list.

All hosts will be joined in Active Directory domain.

3.4 Virtual Machines

All unused devices will be disabled.

Access to VM management will be granted based on Access Policy.

Changes to VM configuration and state will be monitored.

3.5 OS Security Hardening

Windows and UX based Operating systems will be configured in accordance to vendor provided security standards.

OS patches will be applied by Configuration manager to maintain highest patch level.

Antivirus will be running and up to date.

4 Intrusion Detection and Response

Intruders do not know that we have detected them, yet. We will implement Intrusion Detection tools to monitor their activity to better understand their approaches, tools and find what they are after, before we shut them off. Black market uses our network for their operations which means that they can see everything we do. However, that also means that WE can see everything THEY do.

4.1 AlienVault Unified Security Management (USM)

Unified Security Management platform will help us with threat detection and incident response as soon as it happens. AlienVault Lab Threat Intelligence will identify threats targeting our network as well as provide remediation guidance.

Unified Security Management provides following capabilities:

1. Asset discovery – will provide asset inventory and overview of what's running in our network
2. Vulnerability assessment – provides vulnerability monitoring from both authenticated and unauthenticated standpoints, in our case insider and outsider intruders
3. Intrusion detection – network IDS, Host IDS and File Integrity Monitoring
4. Behavioral Monitoring – will collect logs and perform Netflow analysis, such as volume of Netflow traffic, which protocols are being used. It will also monitor service availability
5. Security information and event management (SIEM) – will provide event correlation and trigger proactive alerts, as well as provide remediation guidance

Utilizing this tool, we will be able to monitor the activity of intruders in our network. Which tools do they use? How do they behave? Which data are they trying to access? We will just sit and observe, we don't want to scare them off at this stage.

4.2 RSA Web Threat Detection

RSA Web Threat Detection is a fraud detection platform which utilizes behavioral analytics to provide real-time visibility into Web transactions. This will help us to identify who is accessing our HumanityLink sites are what are they doing there.

Are they accessing our website? What are they doing there? Are they probing for vulnerabilities? Abusing business logic? We'll see.

4.3 CyberArk Privileged Threat Analytics

"The solution is designed to identify an attack in real-time and automatically respond to stop an attacker from continuing to advance the attack. At the core of the solution, the analytics engine runs a sophisticated combination of proprietary algorithms – including both deterministic and behavior-based – on users, entities, and network traffic to detect indications of compromise early in the attack lifecycle. By identifying attackers early, security teams have more of the critical time they need to be able to stop an attack before it stops business" (CyberArk, 2016).

Some of the features:

- Built-in proprietary algorithms conduct Privileged User, Entity and Network Behavior Analytics to detect previously unidentifiable indications of an attack such as suspected credential theft, lateral movement, and privilege escalation.
- Self-learning analytics engine adjusts over time to account for authorized behavioral pattern changes.
- Kerberos attack detection enables organizations to detect and respond to potentially catastrophic attacks that exploit vulnerabilities in the Windows authentication protocol.
- Threat scores are assigned to each individual incident to help prioritize incidents that pose the greatest risk.
- Targeted, actionable alerts include detailed incident information to enable incident response teams to respond immediately to detected suspicious activity.
- Automatic response to detected threats streamlines incident response by enabling security teams to immediately invalidate a suspected stolen privileged credential without requiring human intervention.
- Adapt threat detection to a changing risk environment with machine learning algorithms that continuously adjust the baseline behavior profiles as the authorized behavior changes over time.

- Automatically respond to a suspected stolen privileged credential to stop an attacker from continuing to use a compromised credential.
- Accelerate remediation with immediate access to detailed information about detected incidents.

Exploitation of privileged accounts is one of the largest vulnerabilities today. One the intruders gain access to privileged accounts they can do anything in our infrastructure. Even worse, they will look like us, we may not even notice them. With this solution we will be able to monitor and record privileged activities and get real-time notification on malicious activities. They may look like us but they don't behave like us, we'll find them.

4.4 Bastille Airborne Threat Detection

Bastille Airborne Threat Detection is a solution combining sensors and software to provide full situational awareness about activities ongoing in facilities, with regards to IoT and air space.

This solution will help us to safely and privately scan our airspace, to provide an overview of all IoT devices to identify potential risks of Radio Frequency Hacking.

Sensors will be set up in all of our facilities and will provide ability to track the movement of devices.

Who's in our datacenter, it's not us. Where are they going, what are they doing? We will be able to see exactly where they are without them knowing. It's almost like Marauder's Map!

4.5 Decoy Shipments

We will send a decoy shipment of spare parts to the earth datacenter. We will be vocal about it, assuming at least one of the intruders is an insider, he will try to modify the shipment again. Otherwise the shipment would never reach the location and he would know that we would notice that something went wrong. Tracking will be enabled for the shipment to allow us to monitor its path.

4.6 Cutting Intruders off

Once we will identify the intruders, the scope of the changes they have done, which approaches and tools they use and what activity are they performing, we will be able to evaluate the option of cutting them off. All configuration changes will be easily reverted by applying configuration policies.

5 Polices and Processes

5.1.1 Access policies

Role based access to components will be used in order to limit privileges.

Trusted Administrators, a small closed group of trustworthy engineers, will have full access to all infrastructure components and tools.

OS Administrators will be limited to access to their respective Operating Systems

5.1.2 Password policies

All AD passwords must meet highest security standards and complexity which will be enforced by security policy.

All Infrastructure components passwords have to be generated as a random hash, following the security policy. Passwords will be stored in a Password Management system.

Password retrieval will be monitored and notifications will be send to Trusted Administrators upon each retrieval.

5.1.3 Change Management

All changes have to be documented and approved. Change has to be requested by opening a ticket in Ticketing tool, describing the action, impact and fall back plan, and sending it to Trusted Administrators groups for approval. Once approved, changed has to be scheduled and executed. Ticket can be closed after successful implementation.

5.1.4 Incident Management

All raised incidents will be handled in the Ticketing tool. Tickets will be acted on based on their criticality.

5.1.5 Patching policy

All infrastructure components must be regularly patched and kept at the highest security patch level. Critical patches have to be installed within a week of the release. Zero day exploits have to be installed immediately.

6 Lessons Learned

6.1 Knowledge sharing

We have falsely assumed that everybody wants humanity to succeed in recolonizing the Earth. We have been very local about our plans and shared the information with everyone. Now that we know that the intruders had to had somebody on the inside, we need to more careful when talking about future plans.

Anything related to the infrastructure setup, changes and future plans will be shared only within a small closed group of trusted people.

6.2 Train people on security

We need to train people to remind them of standard security principles, such as:

- Do not provide account details to anyone
- Do not open untrusted emails and if you do, do not click on the link
- You do not have (and you have never had) a distant relatives living in Nigeria who wants to transfer money/diamonds/gold to you. Even if you had, they would have been eaten by Zombies by now
- DO NOT PLUG IN A USB STICK YOU HAVE FOUND LAYING AROUND

7 References

AlientVault. (2016). *AlienVault Unified Security Management*. Retrieved from www.alienvault.com: https://www.alienvault.com/products

Bastille. (2016). *Airborne Threat Detection* . Retrieved from www.bastille.net: https://www.bastille.net/about

CyberArk. (2016). *Privileged Threat Analytics*. Retrieved from www.cyberark.com: http://www.cyberark.com/products/privileged-account-security-solution/privileged-threat-analytics/

Haletky, E. (2016). *IT SLICES, IT DICES: IT IS ANALYTICS*. Retrieved from www.virtualizationpractice.com: https://www.virtualizationpractice.com/slices-dices-analytics-37243/

Kiffney, K. (2016). *Observations from the 2016 RSA Conference*. Retrieved from www.cyberark.com: http://www.cyberark.com/blog/observations-2016-rsa-conference/

RSA. (2015). *NOW YOU SEE THEM, NOW YOU DON'T: Hacker Tactics, Techniques and Procedures*. Retrieved from www.emc.com: http://www.emc.com/collateral/white-papers/h14669-hacker-tactics-techniques-and-procedures-wp.pdf

RSA. (2016). *RSA SECURITY ANALYTICS*. Retrieved from www.rsa.com: https://www.rsa.com/en-us/products-services/security-operations/security-analytics

RSA. (2016). *RSA Web Threat Detection*. Retrieved from www.rsa.com: https://www.rsa.com/en-us/products-services/fraud-prevention/rsa-web-threat-detection

VMware. (2015). *https://pubs.vmware.com*. Retrieved from vSphere Security - ESXi 6.0: https://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf

VMware. (2015). *VSphere 6 Hardening Guide*. Retrieved from https://blogs.vmware.com: https://blogs.vmware.com/vsphere/2015/06/vsphere-6-hardening-guide-ga-now-available.html

VMware. (2016). *https://pubs.vmware.com*. Retrieved from vRealize Log Insight 3.0 Documentation Center: https://pubs.vmware.com/log-insight-30/index.jsp

VMware. (2016). *www.vmware.com*. Retrieved from vRealize Configuration Manager Help: https://www.vmware.com/support/vcm/doc/help/vcm-582/CM_Help.htm