# BEACON Security

Craig Sheridan

BEACON

27/06/2016, Crete

Horizon 2020
European Union Funding
for Research & Innovation

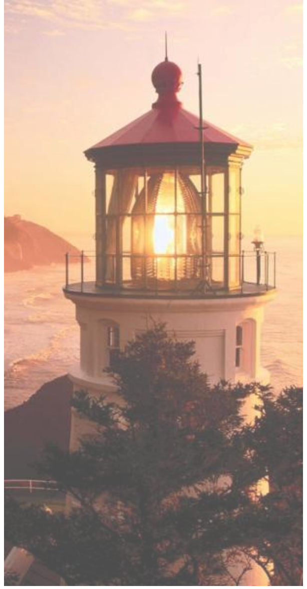
# *Deployment-time multi-cloud application security*

Craig Sheridan, SOC, Crete

BEACON

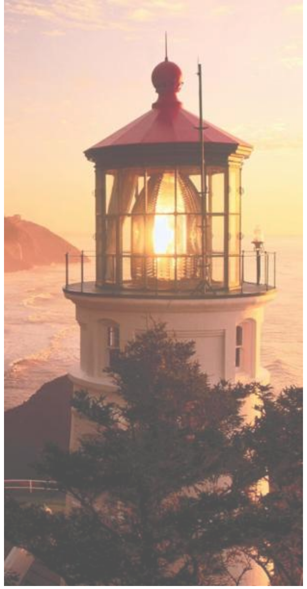
27/06/2016, Crete

Horizon 2020
European Union Funding
for Research & Innovation



# Content

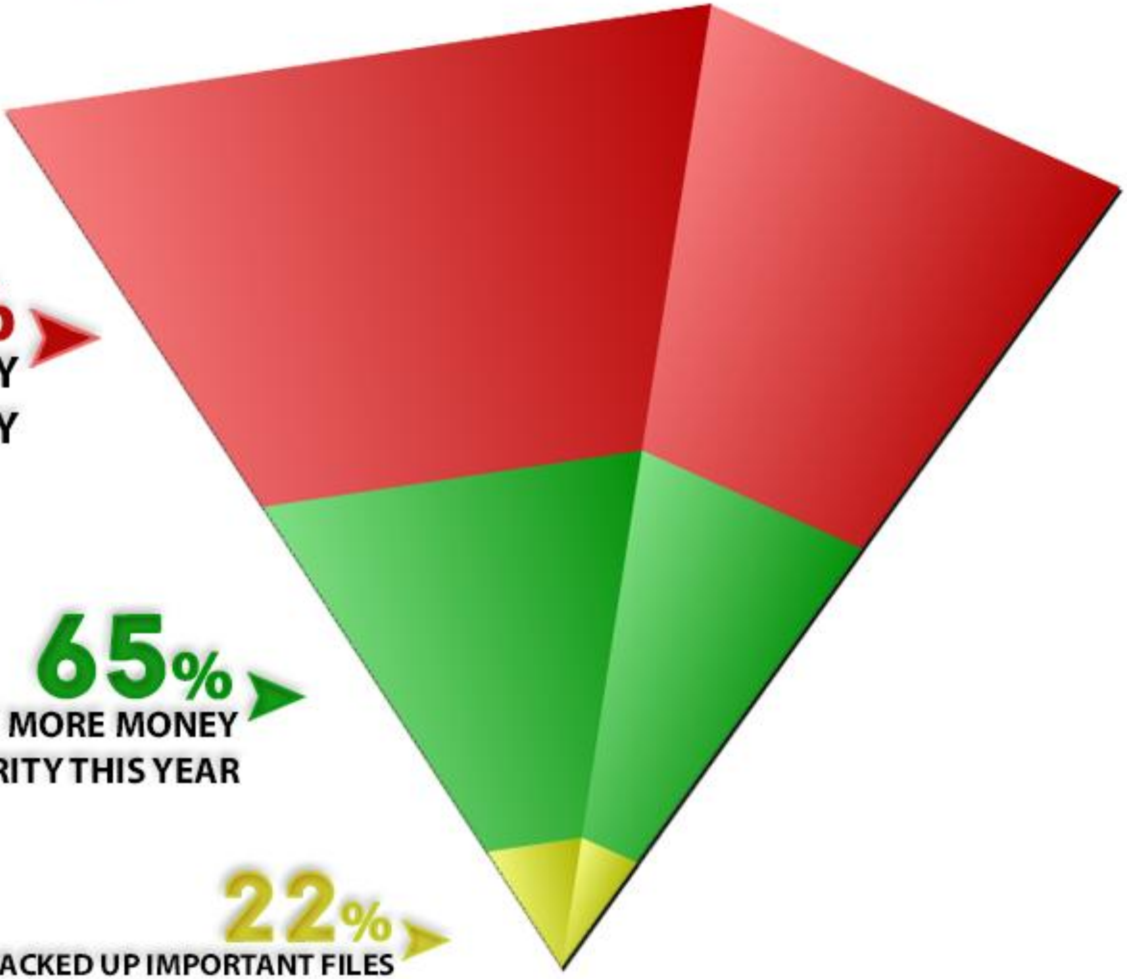
- Overview
- Problem
- Impact
- Solution
- OpenVAS Vulnerability Scanner
- Firewall deployment
- Chef integration
- Other Approaches



BOOM!

# Small Business Budgets Little for Cyber Security

## As Attacks Rise, Preparedness Not a Priority Just Yet, Either



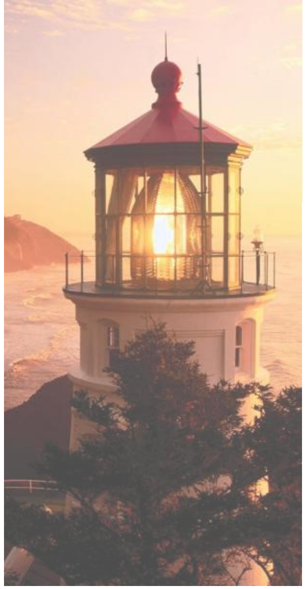
**75%** HAVE NO CYBER SECURITY INSURANCE POLICY

**65%** WON'T BUDGET MORE MONEY FOR CYBER SECURITY THIS YEAR

**22%** HAVEN'T BACKED UP IMPORTANT FILES

Small Business TRENDS

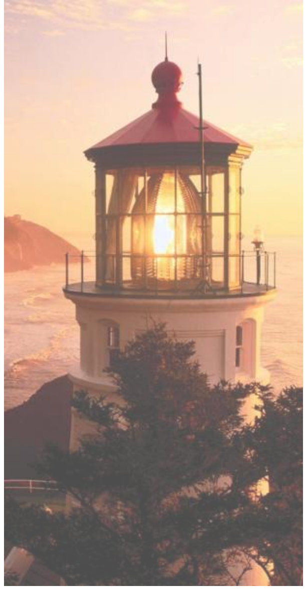
*Source: IDT911*
*More Charts: http://sbt.me/charts*



- Vulnerabilities
- Automation
- Current Practice
- Goal

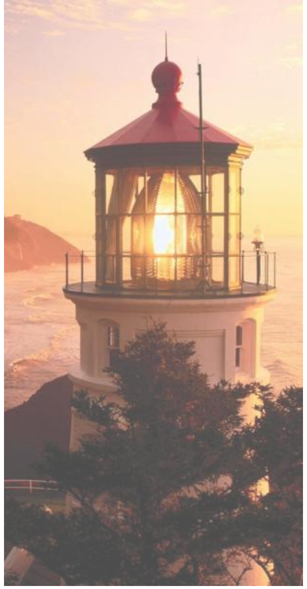
- Attacker tools
- Design errors
- Timeliness

Horizon 2020
European Union Funding
for Research & Innovation



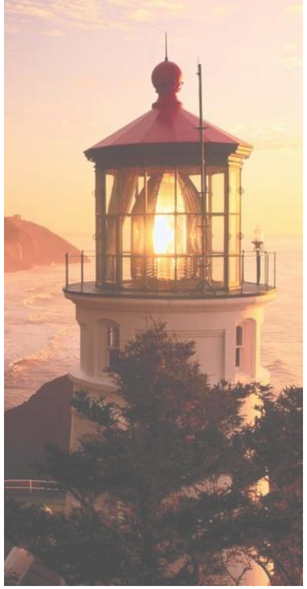
# Problem - Who?

- App owners, Service Providers, End User
  - Malware
  - Deface
  - Ransomware
  - Botnet
  - Data theft

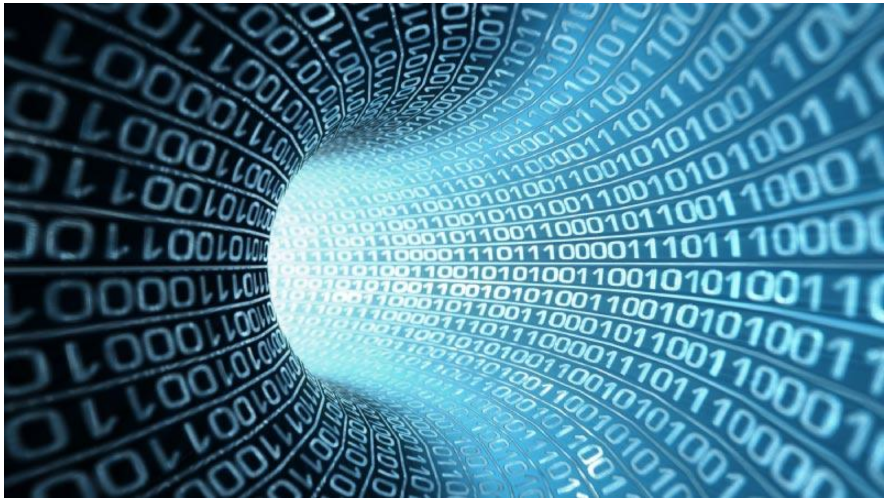


# Problem – When?

- As VM goes live
- Secure at the point of creation
- All platform types



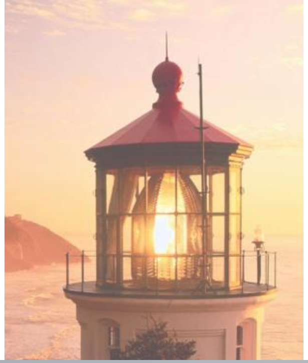
# Problem - Scale



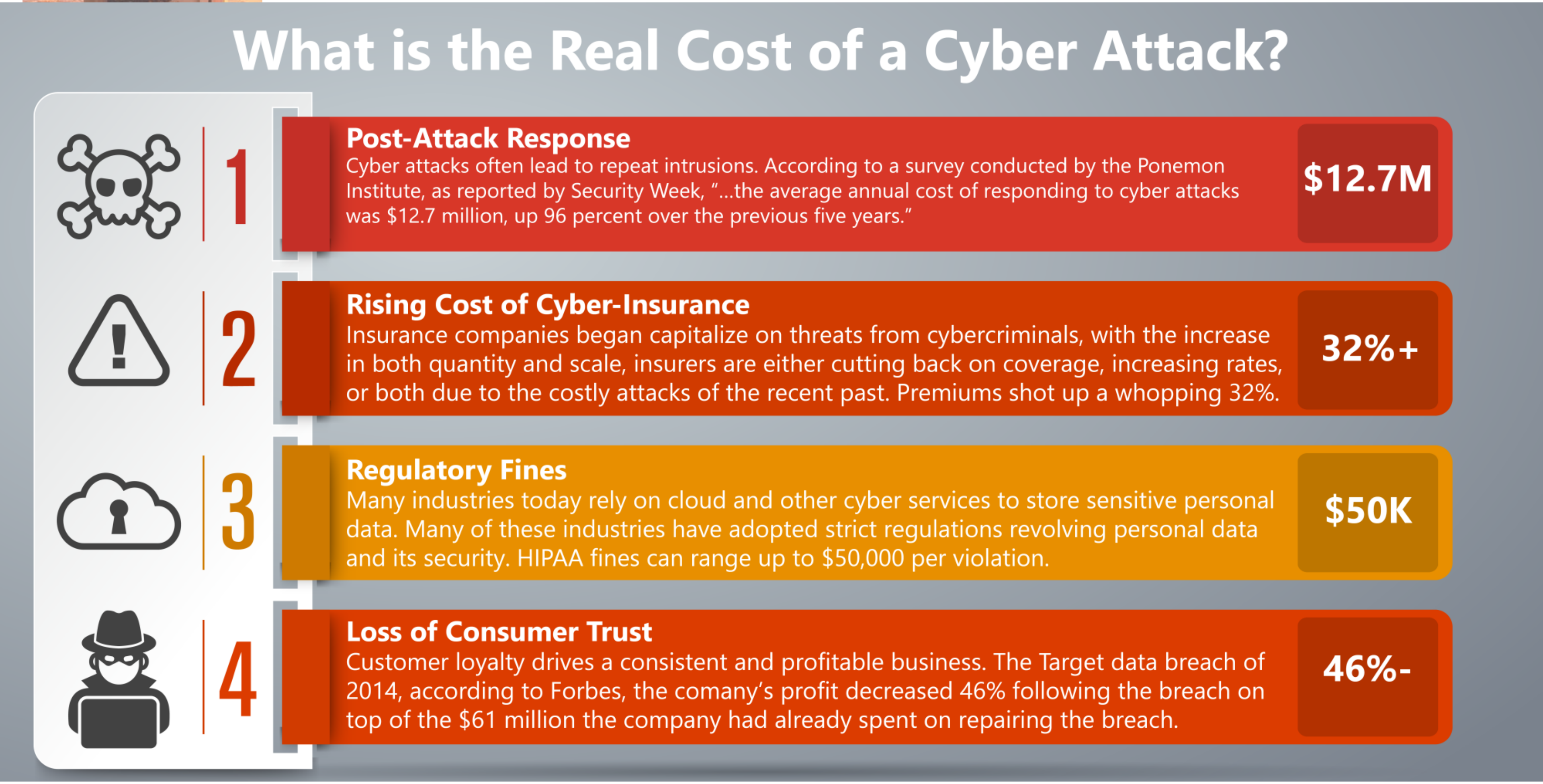
- Increasing
- WannaCry
- Deloitte -14 business impacts
- $110Bn per year $197 per victim (consumers)
- 1 Million+ victims per day (14 every second)
- 431 Million victims in last 12 months
- 69% of Adults have experienced cybercrime

# Impact - Customers

Globally, one in six consumers lost money, with
20% of victims losing more than $1,289



# Impact – business costs



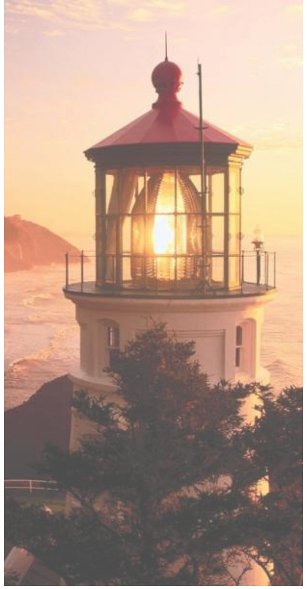
## What is the Real Cost of a Cyber Attack?

1 **Post-Attack Response**
Cyber attacks often lead to repeat intrusions. According to a survey conducted by the Ponemon Institute, as reported by Security Week, "...the average annual cost of responding to cyber attacks was $12.7 million, up 96 percent over the previous five years."
**$12.7M**

2 **Rising Cost of Cyber-Insurance**
Insurance companies began capitalize on threats from cybercriminals, with the increase in both quantity and scale, insurers are either cutting back on coverage, increasing rates, or both due to the costly attacks of the recent past. Premiums shot up a whopping 32%.
**32%+**

3 **Regulatory Fines**
Many industries today rely on cloud and other cyber services to store sensitive personal data. Many of these industries have adopted strict regulations revolving personal data and its security. HIPAA fines can range up to $50,000 per violation.
**$50K**

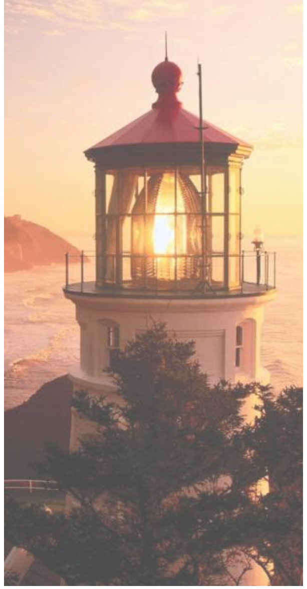
4 **Loss of Consumer Trust**
Customer loyalty drives a consistent and profitable business. The Target data breach of 2014, according to Forbes, the comany's profit decreased 46% following the breach on top of the $61 million the company had already spent on repairing the breach.
**46%-**



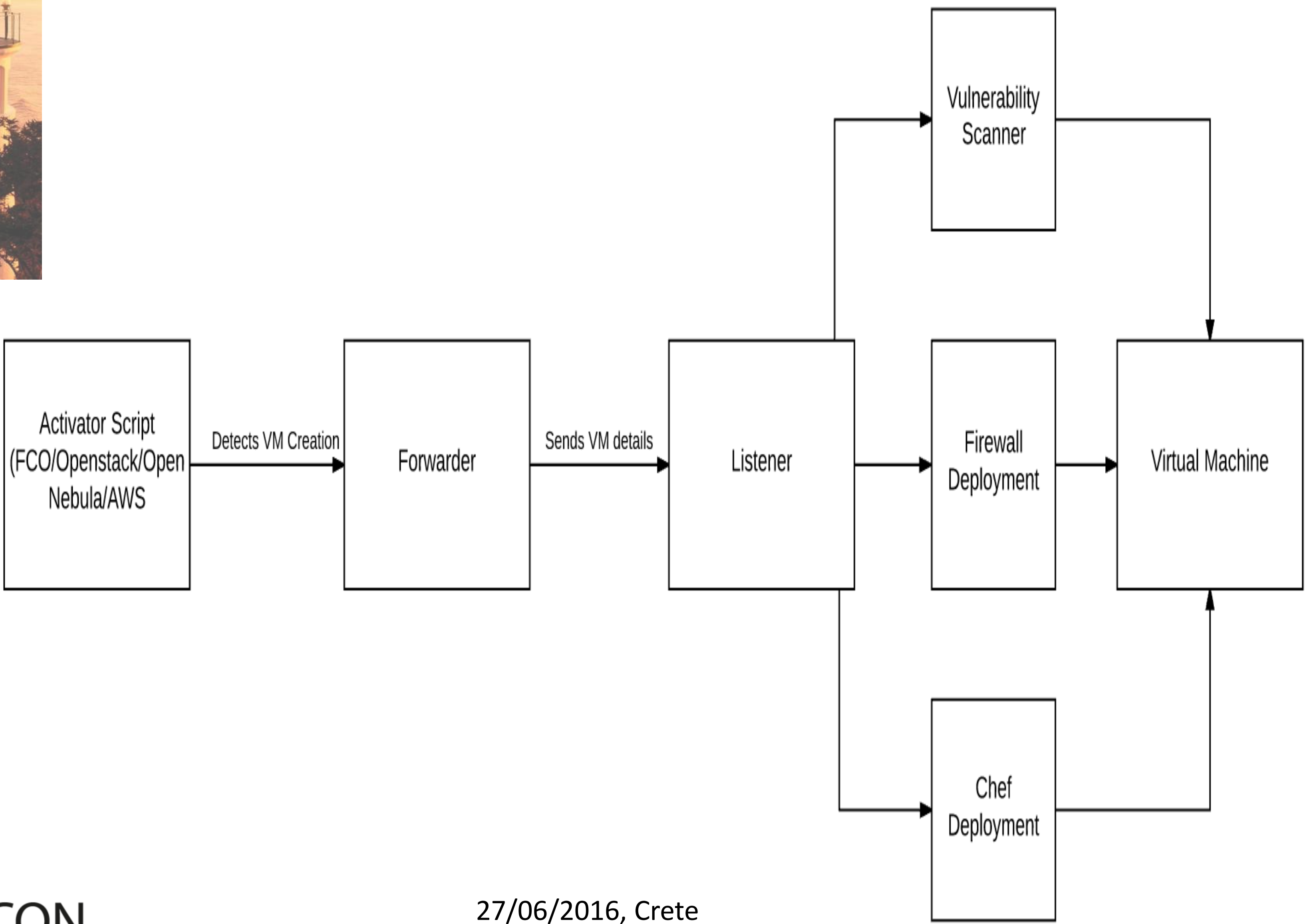
# Solution

**‘Implement all required security measures to an application and its container in an automated way from the point of deployment’**

- Implemented easily from the user perspective
- Effective at solving the exposed vulnerability
- Cost effective to operate



# Workflow



Activator Script (FCO/Openstack/Open Nebula/AWS)

Detects VM Creation

Forwarder

Sends VM details

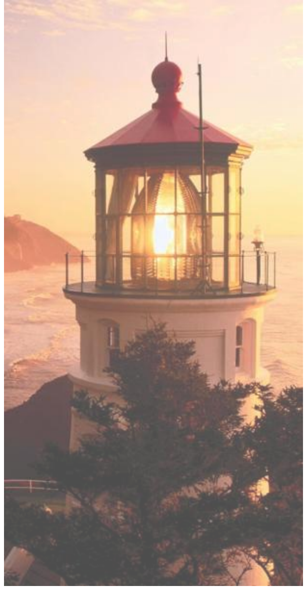
Listener

Vulnerability Scanner

Firewall Deployment

Chef Deployment

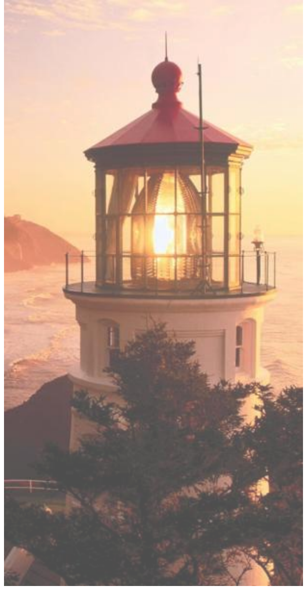
Virtual Machine



# Vulnerability Scanner Automation

- Open Vulnerability Assessment System (OpenVAS) a collection of tools & services providing a vulnerability-scanning framework to automatically scan new VMs

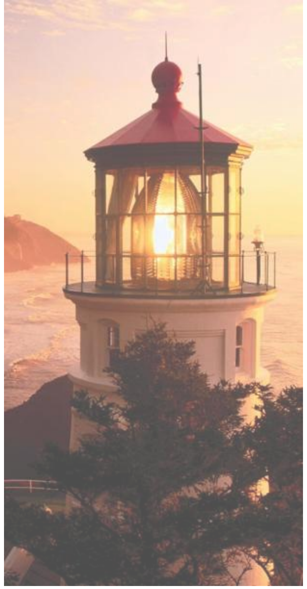
“End result is an assessment of the system containing the application, which reports known weaknesses both before and after the security automation is implemented.”



# Firewall Automation

- Automatic and customisable deployment of a firewall on a cloud platform level to create and apply a new security group to the VM.

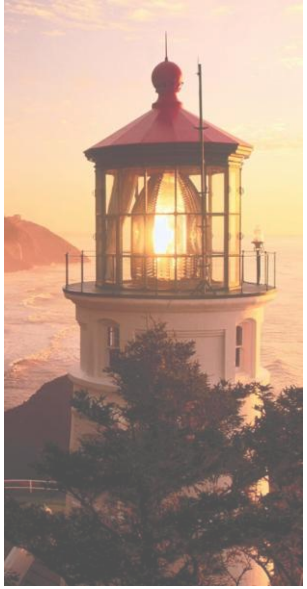
"The end result is the creation of a firewall perimeter around a VM to block attacks and limit communication to only the necessary ports and protocols."



# Chef Automation

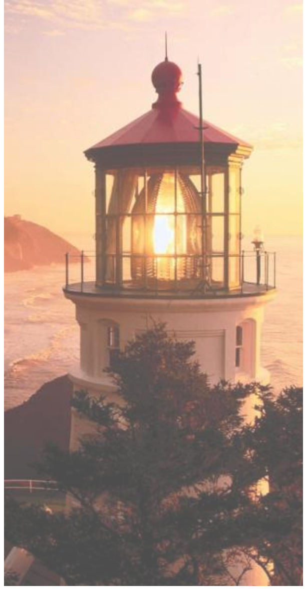
automatic deployment of Chef infrastructure on the VM to facilitates the automatic deployment of security packages known as “cookbooks” to servers.

“The end result is to automatically patch applications against known vulnerabilities to shield them from attack with a set of security policies that are easily updated.”



# Other Approaches

| Solution | Type | Detail |
|---|---|---|
| Automated security suite at deployment time | Proactive/ Automated | Best solution, automated, wide-scoped, cheap |
| Manual setup at runtime | Proactive/ Manual | Good but error prone, time consuming, costly, early exposure |
| Partly Implemented Security Measures | Proactive/ Reactive Automation/Manual | Poor as leaves some level of exposure. Only some security aspects are automated. |
| Post cyber attack clean up | Reactive | Worst solution as no apt security measures in place causing exposure to many vulnerabilities. |



# Summary

- In conclusion, the three main components of the solution described provide a concrete security baseline for newly created VMs and deployed applications.
- The autonomous nature of the vulnerability scanner, firewall creation and chef integration process provide an easy and powerful method of identifying and securing new VMs against malicious security threats on all common platforms.
- We have documented various aspects of a common problem and provided a viable and credible solution together with the benefits of this novel solution in comparison to alternative approaches.
- Plan to tailor firewall template to attempt to better  neutralize the vulnerabilities detected by the vulnerability scanner & chef cookbooks  can be tailored to compliment the firewall deployed to the VM on the cloud platform level.
- Implementing the BEACON security suite to an application and its container in an automated way at the point of deployment solves the identified vulnerability.

# Questions ?