

# How to Implement IT Security after a Cyber Meltdown

---


CHRIS KUBECKA

@SECEVANGELISM



# Introduction


---

- Aramcoed- 2012 attacks and effects on business operations
  - Starting from zero
  - Moving past the security poverty line
  - If I had a hot tub time machine
- 



# Cybergeddon

---

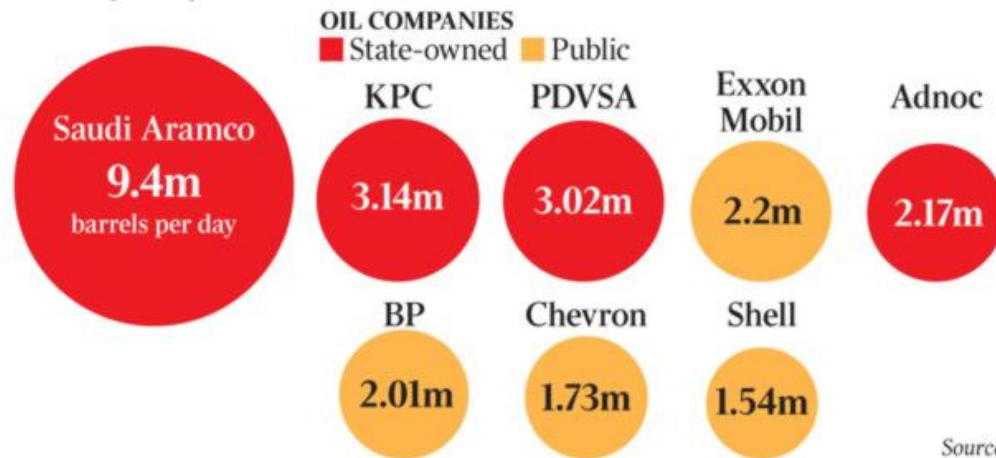
- Why Saudi Aramco and Affiliates?
  - Two prong attack during Ramadan
  - >50% of Windows systems affected
  - Shamoon/W32.Distrack
- 

# Attractive Target

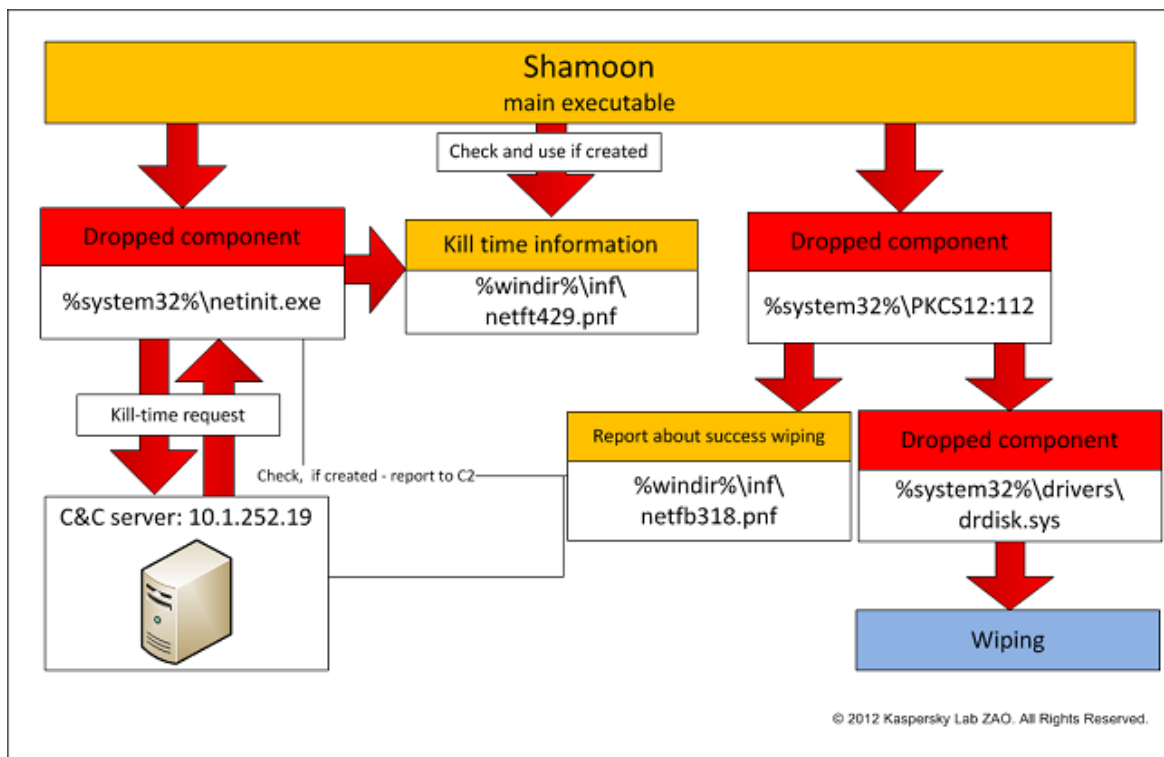
---

## Big oil

Aramco is the world's biggest oil producer. Here's how it stacks up with some other large state-owned and publicly listed companies. Liquids output in millions of barrels per day in 2013



# Shamoon/W32.Distrack



# 2012 Attack Timeline

---

Targeted Phishing attack

- Date Unknown

First indicators of attack

- August 2012

Saudi Aramco  
Disconnects from  
the world

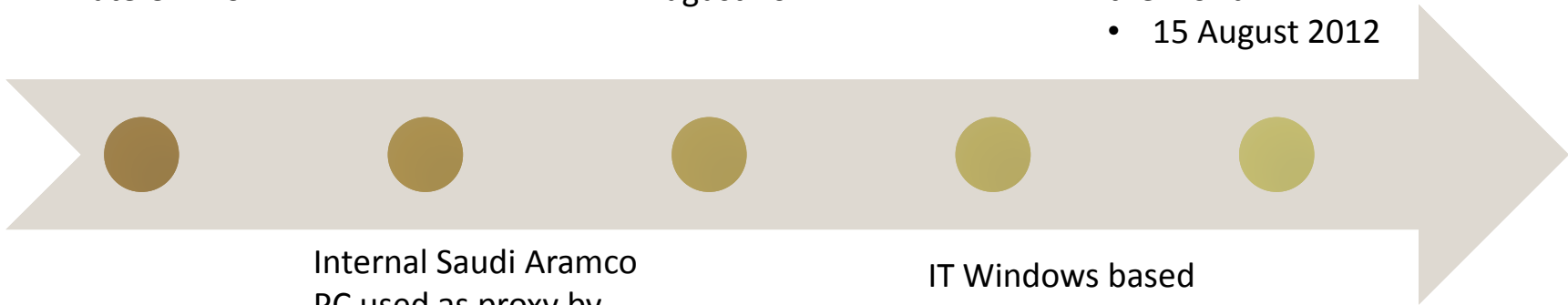
- 15 August 2012

Internal Saudi Aramco  
PC used as proxy by  
attackers

- Date unknown

IT Windows based  
Saudi Aramco PCs  
>35K begin shutting  
down & being wiped

- 15 August 2012





When you realize most of your security budget was spent on ICS & IT gets Pwnd



# Cybergeddon

---

“Never underestimate how dependent you are on your information technology and systems. It’s become like oxygen. You think you can live without it but you can’t.” Khalid A. Al-Falih

# No IT payment systems, no Gas

---



# ICS vs. IT Risk

---

**A**

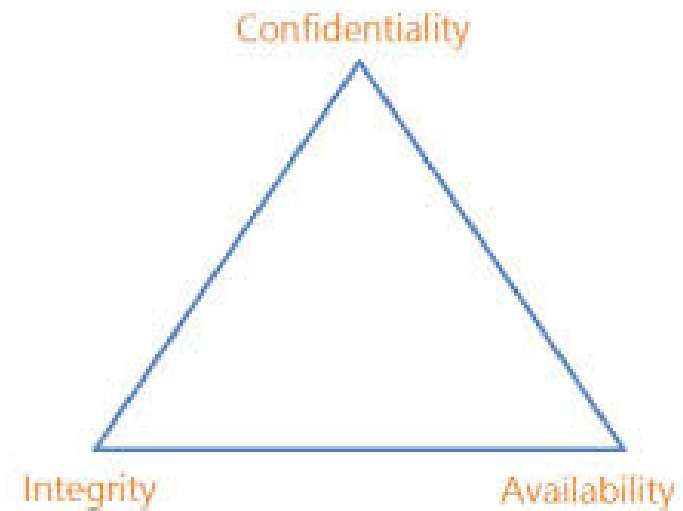
**Availability**

**I**

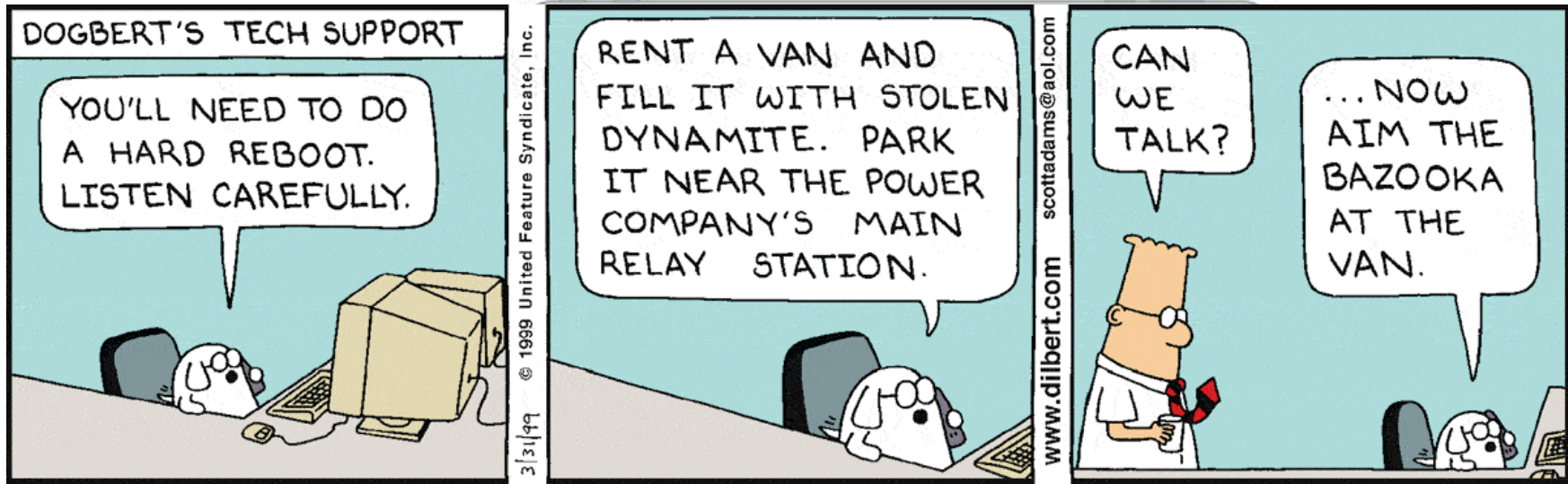
**Integrity**

**C**

**Confidentiality**



# Have you tried turning it off & on again?




# Cybergeddon

---

- Saudi Aramco wasn't the only one
- ICS & IT networks isolated
- Cut off from the outside world

# Starting from Zero to Hero

---

- An offer I couldn't refuse
  - Starting from Zero
  - Recruiting the Security & Network Operations Center (SNOC) team
- 

# The Joker

---




The image shows a screenshot of a Twitter profile page. The profile picture is a Joker character. The name is "saudi Aramco" and the handle is "@Saudi\_Aramco". The website listed is "saudiaramco.com". The statistics show 976 tweets, 18 following, and 46,746 followers. There is a "Follow" button. The "Tweets" section contains three tweets:

- Joseph hacker @ Dr\_gozeef** (10 mins): "Bhamdallah penetrate three Iranian sites Pu.is / Www.youtube.co ...". Retweeted by Saudi Aramco.
- saudi Aramco @ Saudi\_Aramco** (1 hr): "Account has been compromised by Mister Rero for through a loophole of Alheczzr discovery Joseph hacker to connect with Joseph @ hacker dr\_gozeef".
- Mister Rero hacker: \$ @ Saudi\_Aramco** (5 hrs): "Saudi Aramco exhibition and conference sponsors the Middle East for oil and gas next Sunday and participate in its activities - bit.ly / Aramco # MakeAGIF.com".

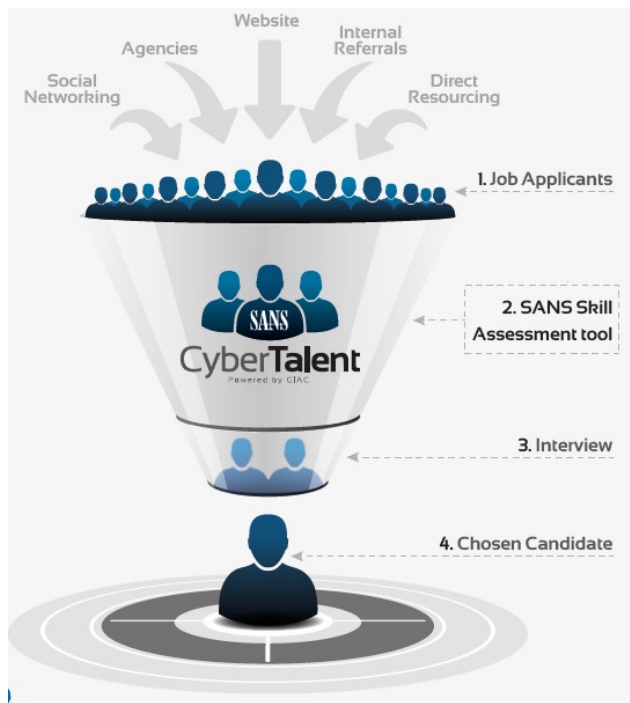
## Recruitment tools & tips

---

- Use your network, including recruitment agencies, poach and Reddit!
  - Don't try and reinvent the wheel if time is limited
  - Don't cheap out, good analysts are difficult to find
  - Hackers, lock pickers, geniuses and Harlem Shakers
- 



# Tools & Tips



meta /r/netsec's Q2 2015 Information Security Hiring Thread (self.netsec)  
submitted 3 months ago \* by sanitybit [M]

## Overview

If you have open positions at your company for information security professionals and would like to hire from the /r/netsec user base, please leave a comment detailing any open job listings at your company.

We would also like to encourage you to post internship positions as well. Many of our readers are currently in school or are just finishing their education.



# Starting from Zero to Hero

---

- Retaining rock star security analysts
- Let them rest
- Feed them

# Security Hero, Forensics and R&D

---



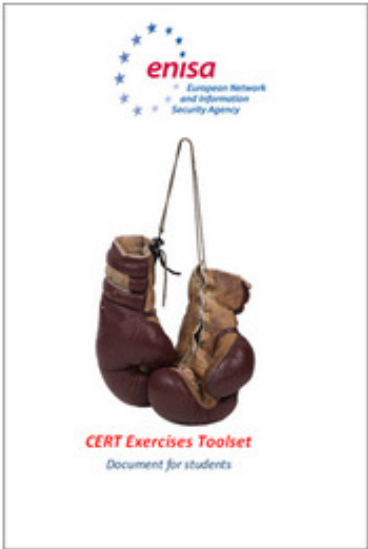
# Beyond the security basics

---

- Dreaded auditors
- When a SNOC turns into a full Security Unit
- Building incident response & CERT


# Exercises

---



# Lessons Learned

---

- Corporate culture affects of the attack
  - Panic and Twitter setbacks
  - Collaboration
- 

# Twitter setbacks

---



**Saudi Aramco** @Saudi\_Aramco

4h

There is no truth to what's been circulating on social media sites about another attack or any damage to company networks.

[Collapse](#) [← Reply](#) [↻ Retweet](#) [★ Favorite](#)

## Cyber attack denied

Posted on » Wednesday, November 27, 2013

KHOBAR: Saudi Aramco said yesterday it had shut some of its computers for an upgrade and denied it had suffered a cyber attack. Earlier, posts on Twitter said some or all of the company's computers were down, possibly because of a cyber attack.

"Saudi Aramco confirms its electronic network is completely safe and speculations of an electronic breach are completely untrue. The temporary shutdown was limited to personal computers and was the result of an update of some applications of the network," the company said.

# The No Team

---



© Scott Adams, Inc./Dist. by UFS, Inc.




# If I had a Hot Tub Time Machine

---

- Project overload
- Cultural awareness
- Collaboration

# Conclusion

---

- Saudi Aramco and affiliated experienced a major cyber attack that greatly affected business operations
  - Recovery was expensive & time consuming
  - Change is possible
  - Learn from past and present experiences
- 

Questions?

---

Chris Kubecka

HypaSec

@secevangelism