dotSec
dot com security

What the hell was that??!?

dotSec
dot com security

splunk>

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

aws partner network
Standard Consulting Partner

irap

dotSec
dot com security

Overview

- DotSec has been using Splunk for over 10 years!
- Review four past DotSec Splunk projects:
  - Splunk for compliance (PCI DSS, IRAP, etc.)
  - Splunk for due diligence (insurance, negligence, etc.)
  - Splunk for incident prevention
  - Splunk for incident response
- Conclusions

dotSec
dot com security

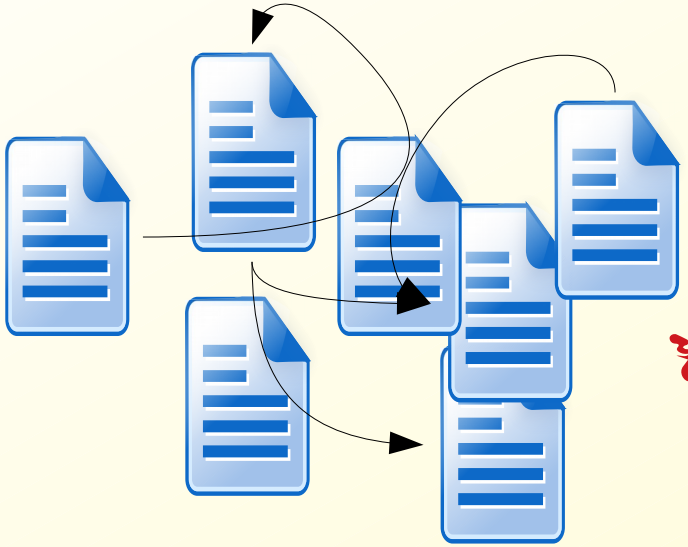
Splunk for compliance

- DotSec provides review, audit and assessment services
  - Our online-retail customers require PCI DSS compliance
    - See Requirement 10.6
  - Federal service-provider requires IRAP compliance
    - See ISM Control: 0120, 1405 and 1344
  - General audits done in line with ISO 27001
    - See Control 12.4.1

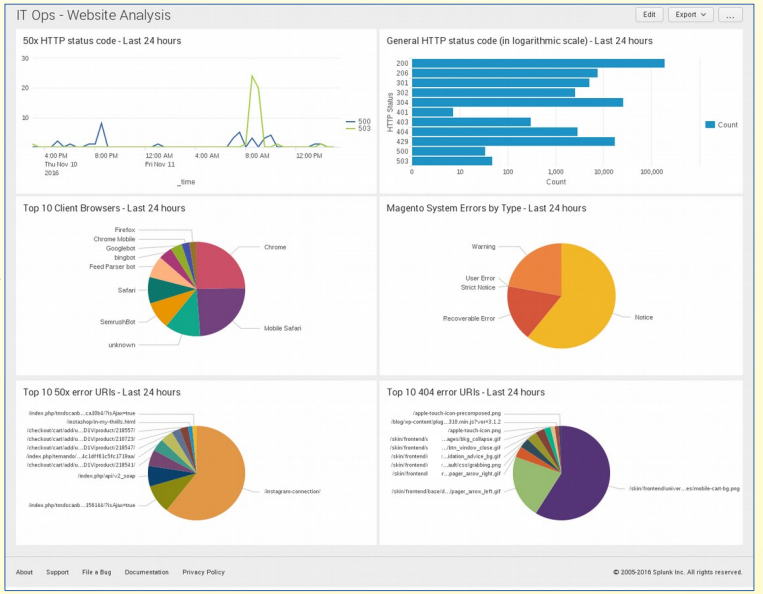
dotSec
dot com security

Review time!

- Assessor needs evidence. Business has two* choices:



or



Hours out of each day, every day.

Minutes out of each day, every day.

* Three, really!

dotSec
dot com security

Cyber security insurance

- The not-so-fine print from actual policy applications:
  - *Describe how your security personnel analyse audit reports...*
  - *Confirm that your business continuously refines and tunes your SIEM...*
  - *Confirm that your incident response plan is formally documented….*
  - *Confirm that your SOC obtains relevant (IOCs)...*
- Of course we can demonstrate that we do all that!
  - Good, because the payout will depend upon it.

dotSec
dot com security

Splunk for incident prevention

- Ring a bell?
  - We wouldn’t know if an online service was failing.
  - We’re not sure if we’re compliant.
  - I don’t know; we might be under attack.
  - We thought that invoice was paid.

dotSec
dot com security

So a funny thing happened

- Assessments and double checks

```
index=_internal sourcetype=splunkd_access "/servicesNS/*/saved/searches/*" AND NOT user=splunk-system-user
| eval file=urldecode(file)
| table _time, user, file
```

Last 30 days

✓ 5 events (13/02/2017 00:00:00.000 to 15/03/2017 13:17:20.000) No Event Sampling

Job Smart Mode

Events Patterns Statistics (5) Visualization

20 Per Page Format Preview

_time	user	file
2017-03-15 13:16:21.040	cmckenzie	REPORT - Privileged vs Unprivileged Server Access
2017-03-15 12:58:13.885	cmckenzie	ALERT - Excessive number of password failures detected
2017-03-15 12:56:38.418	cmckenzie	ALERT - Changes detected to privleged AD group
2017-03-15 12:56:08.536	cmckenzie	REPORT - Notible Active Directory Events
2017-03-15 12:05:53.314	cmckenzie	DMC Alert - Missing forwarders

Illustration 1: Table showing accesses to Splunk reports

dotSec
dot com security

Splunk for post-incident

- O365… the boil or the pot?… One thing's for sure!
- Short version (without Splunk):
  - We paid money; our customer didn't get the coins; we don't know what happened.
- Long version (with Splunk):
  - June 1*: The first overseas login was recorded in the O365 logs.
  - June 5: A new Inbox rule was created, which diverted all mail containing the words "bsb" or "invoice" to a folder used by the attacker.
  - June 10: An email was sent by the attacker (apparently from person@supplier.com) to person@purchaser.com.au requesting that purchaser update the supplier's bank account details for the receipt of payments.
  - June 20: Funds go to attacker's account (instead of supplier's) and are lost.

* Dates changed to protect the innocent

dotSec
dot com security

Splunk for post-incident

- Good side
  - Splunk lets us know what happened
  - Expedites insurance claims and helps to contain the attack
- Bad side
  - Splunk can’t get the money back
- Good side
  - We can learn: Set up Splunk with pro-active O365 log monitoring and alerting for when this all happens again… and you know...

dotSec
dot com security

From the press:
Just how bad can “I dunno” get?

Business ▸ Policy

Australian Senate vote-counting-ware contract a complete shambles

Auditor says the right people were elected, probably, despite security and other messes

By Richard Chirgwin 22 Jan 2018 at 23:23 5 SHARE

Copyright (c) The Register
https://www.theregister.co.uk/2018/01/22/senate_software_shambles/

dotSec
dot com security

“I dunno” quote of the year*

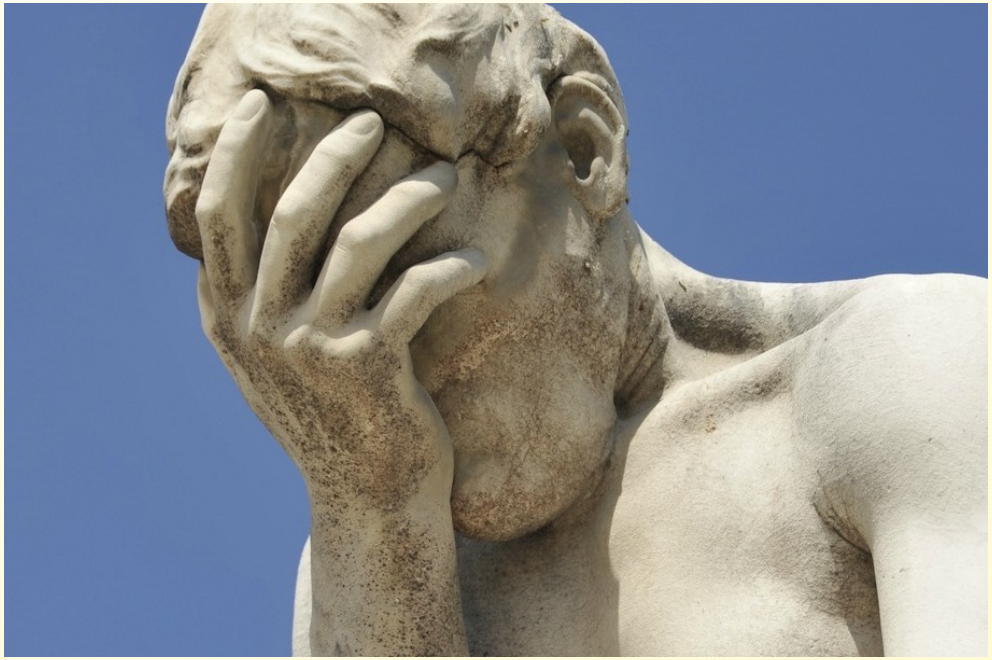
“It cannot be concluded from the above figures, or from other AEC records examined by the ANAO, that any ballot papers were lost. Rather, the above figures and other records support the audit finding that the AEC is not currently in a position to report that it has achieved its performance target of 100 per cent of ballot papers being accounted for.”

* Yes, minister :-)

dotSec
dot com security

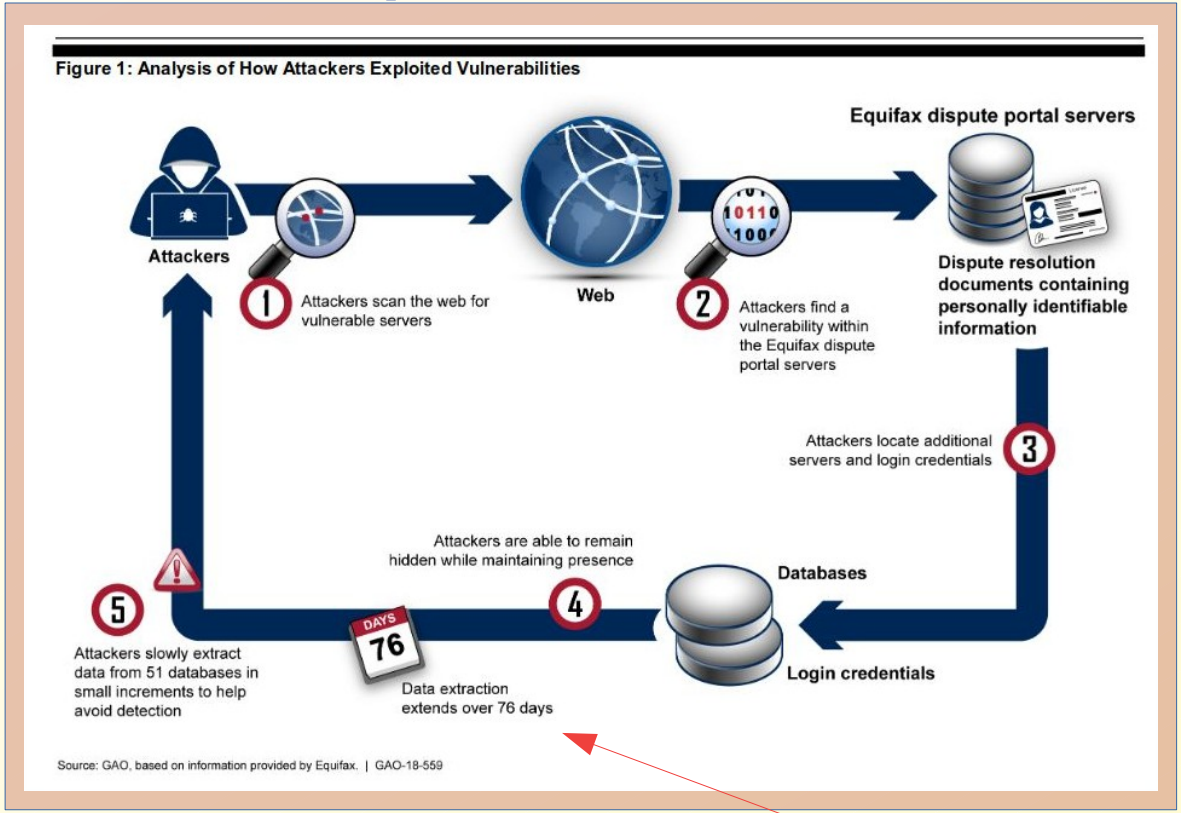
Target 2013

- Oh the sadness… I can’t even write about this one…



dotSec
dot com security

Equifax 2017



Yes, that's 76... days! 76 days!

dotSec
dot com security

Conclusions

- Four DotSec Splunk project examples from the past 10 years:
  - Splunk for compliance (PCI DSS, IRAP, etc.)
  - Splunk for due diligence (insurance, negligence, etc.)
  - Splunk for incident prevention
  - Splunk for incident response
- 10 years of Splunk experience; 20 years of infosec experience!
- There are no conclusions; this is an ongoing improvement.
- For a good time, just call!
- Thanks!