BUILDING A FORENSICALLY CAPABLE NETWORK INFRASTRUCTURE

Nik Alleyne, MSc | CISSP | GCIA|H
securitynik.blogspot.com

ABOUT ME

- In technology for around 17 years
- Last 8 more focused on security
- Currently employed as a Manager, at a MSSP
- Teach SANS 503 – Intrusion Detection in Depth &
- Masters in Cyber Security Forensics
- A few industry certifications including:
  CISSP | GCIH | GCIA | CCNP R&S and Security | Splunk Admin | ISO9001, etc
- Blog at http://securitynik.blogspot.com

OUR OBJECTIVES

- Discuss what is meant by forensically capable
- Look at the facts as it relates to security incidents
- Understand the available challenges in becoming forensically capable
- Choosing between open source and commercial
- Understand the importance of time

WHAT IS MEANT BY FORENSICALLY CAPABLE?

- A network which allows a forensic investigator, network security analyst, intrusion analyst, etc., to be able to retrace the steps of any (potential) security issue which may be identified, thus allowing them to not only fix the current issue but prevent and or mitigate it in the future.

- These issues may include but not limited to identification of fraud, policy violations, security incidents, auditing, forensic investigations, inappropriate usage, etc

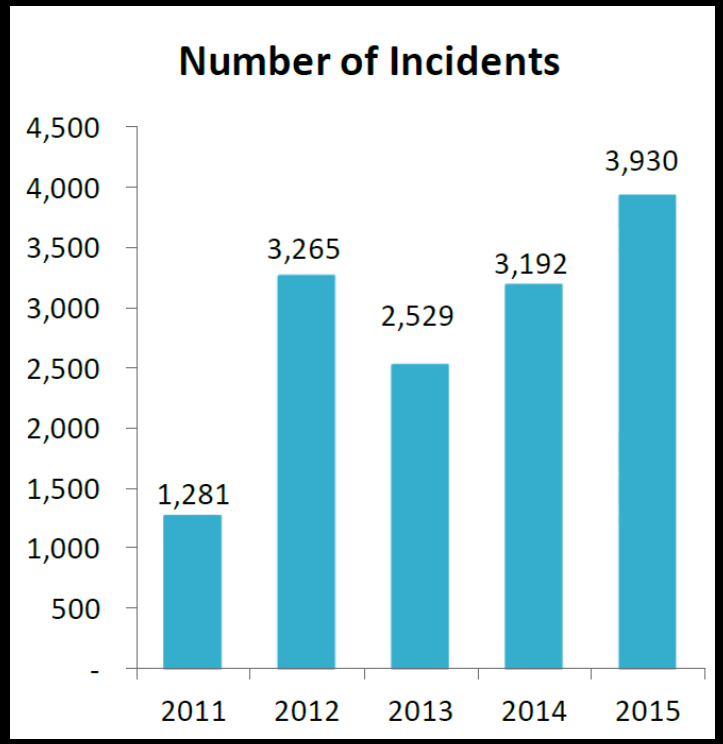
- While this can also be done for operational purposes such as establishing baseline, identifying operational (d)efficiencies, the objective of this presentation is strictly from bullet 2's perspective

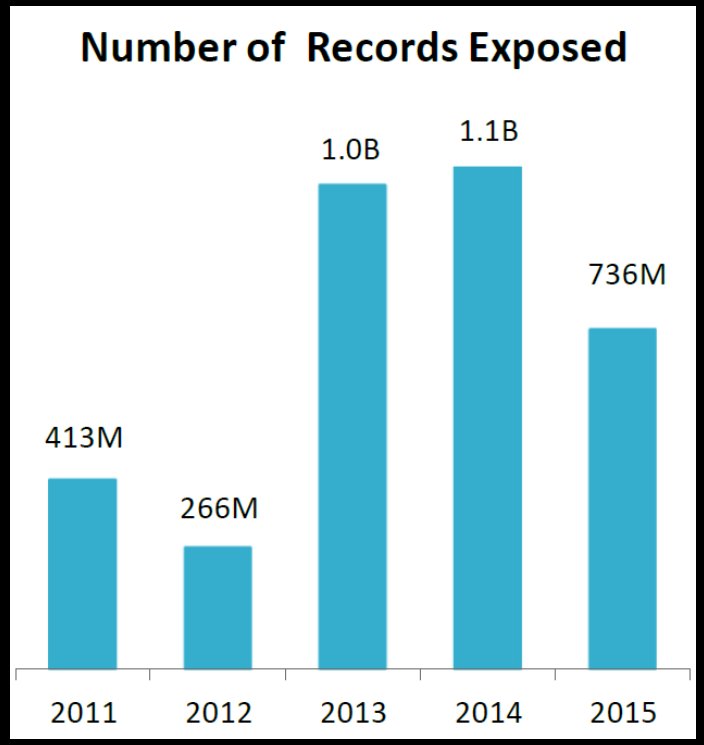
CONSIDERATIONS FOR BEING FORENSICALLY CAPABLE

- Design to allow for easier investigation
- Configure to ensure appropriate data is captured
- Protection against data tampering and or replay
- Log to one or more centralized destinations
- Control access to the logged data
- Rely on multiple data sources for intelligence purposes
- Time is properly configured by leveraging NTP
- Agent vs Agentless

FACING THE FACTS

- Looking back at the past 4 years





Security Incidents are on the rise

Source: Risk Based Security - 2015 Data Breach Trends

FACING THE FACTS

- During 2013-2014: > 2 billion records exposed
- 2015 had the highest amount of data breaches ever reported - 3,930
- Over 736 million records exposed
- 77.7% of incidents had an external source
- 64.6% of incidents were caused by hacking
- 58.7% of exposed records were caused by hacking
- Hacking and web based activities results resulted in 89.3% of all exposed records

  Source: Risk Based Security - 2015 Data Breach Trends

We rely on the Internet and web for everything …
that should be EVERYTHING

FACING THE FACTS

Other Considerations

- 4 hacking incidents exposed 237.8 million records
- 1 Database misconfiguration exposed 191 million records
- At least 46 incidents had more than 1 million records exposed

Looking specifically at Canada

- Not Immune to this type of activity
- #3 at 114 incidents reported by country behind US (1,593), UK (246)
- #4 with 45,131,583 records exposed
- Average 395,891 exposed records per incident

Source: Risk Based Security - 2015 Data Breach Trends

No one is immune to a potential compromise

FACING THE FACTS

Even a closer look at Canada

- 1 organization – CRA
- 1 vulnerability - Heartbleed
- 900 Social Insurance Numbers (SIN) exposed

Source: http://www.cbc.ca/news/politics/stephen-solis-reyes-accused-in-cra-heartbleed-hack-has-case-put-over-1.2709556

Peeking into the Future

- does not look like it will be much better
- 2,955 reported breaches so far for 2016
- 2,212,823,840 Compromised records

Source: https://www.cyberriskanalytics.com/

We're heading for an interesting future!

WHAT DO THE FACTS SAY?

- We have to do a better job at securing our infrastructure
- Securing is a cat and mouse game of defenders vs attackers
- Make it easier to investigate
- Assume you have been compromised …
- … or will be soon

Ensure the network is forensically capable!

WHERE TO START

- Number 1 Priority? Figure out what the business needs
- It's about the business NOT the technology
- and definitely NOT about the tool
- Let the tool support the business NOT the business support the tool

- Identify people to support the effort
- Develop processes to support the effort
- Then identify the technology to support the effort

Business needs take precedence

SO MANY TECHNOLOGIES

IIS web server	Linux Web Servers	Routers
Switches	Proxies	Firewalls
IPS/IDS	SIEMs	Web application Firewalls
Unified Communication Systems	Mail Servers	AntiMalware
Databases	BYOD	Directory Services
Vulnerability Scanners	Threat Monitoring Systems	Load Balancers
VPNs	Authentication Servers	Custom Applications

Multiple Sources of Forensic Data

SO MANY TOOLS

QRadar	tcpdump	ArcSight
McAfee	Wireshark	SolarWinds
Splunk	Gigamon	Cisco
Niksun	Fortinet	Baracuda
SyslogNG	Netscout	DLP

Choosing the right ones is important

SUCH A SMALL BUDGET

- Budget is always a primary concern
- Not enough to spend
- Which business needs (NOT technologies) to give priority
- How much of that budget to use per business need

You cannot spend what you don't have

WHAT DO WE NEED?

- To know what we are trying to protect
- Full packet capture preferred
- Network Flow data acceptable
- Collection of relevant events
- Collection from relevant devices
- Collection of bandwidth utilization data for both egress and ingress points
- Appropriate positioning of collection devices
- Reliable Time Sources (NTP)

To prioritize

COMMERCIAL OR OPEN SOURCE

- Does the company have any concerns with open source tools
- Does the open source tools meet the business needs
- Do you have people to support open source on an ongoing basis
- Do you provide training to maintain open source
- Are you ensuring continuity in the presence of staff turnover

- Maybe you need commercial

Only two choices does not necessarily mean easy choice

AN OPEN SOURCE TOOLS PERSPECTIVE

- Full Packet Capture (can be expensive)
  tcpdump, thsark, snort
- Flow Analysis
  Silk, Bro, NFDump/NFSen, nTop, flow-tools, Argus
- Event Collection (and or correlation)
  Alient Vault's OSSIM, Enterprise Log Search and Archive (ELSA), GrayLog, SyslogNG, OpenSOC, Elastic+Logstash+Kibana, OSSEC, Prelude-LML, Splunk (500MB per day limit)
- Bandwidth
  nTop, vmstat, cacti, Nagios, Centreon, IP Audit, BandwithD

DESIGNED TO ALLOW FOR EASIER INVESTIGATION

- Data should always be readily available
- Should be in a manner which is easily understandable
- Have people who can make sense of and add context to the data

Without a proper design no implementation will be successful

CONFIGURED TO ENSURE APPROPRIATE DATA IS CAPTURED

- Capture authentication events – both success and failure
- Capture access to critical data or resources – both success and failure
- Capture non cleaned or non-blocked malware activity
- Capture firewall permits and denies
- Capture attempts to elevate privileges
- Capture attempts modify critical accounts and groups
- Capture proxy events

Yes you can capture everything

BUT can you action and or retain everything

PROTECT THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF CAPTURED DATA

- Manage integrity & confidentiality of logs
- Leverage TLS (SSL) where possible for confidentiality
- SSH Tunnels can also be used for confidentiality
- SNMP v3 is another excellent alternative where possible
- How much data will you log
- How long will you log for
- Monitor forwarding devices to ensure they are forwarding their logs
- Consider leveraging a separate network for management functions

Ensuring you can trust your logs is extremely important

CONTROLLING ACCESS TO THE LOGGED DATA

- Configure sources to forward to specific destinations
- Allow only authorize personnel to access the logged data
- Manage the access granted to users who can access the data
- Consider log retention periods
- Implement access control policies to limit specific subnets and or IPs

Only on a need to know and need for access basis

RELIANCE ON MULTIPLE DATA SOURCES FOR INTELLIGENCE PURPOSES

- Bandwidth data can help
- What does that spike in the bandwidth graph for traffic leaving the infrastructure suggest?
- What roles should specific devices be playing
- At what time should specific activity occur
- Is cleartext allowed
- Is encrypted traffic allowed

Know your infrastructure

TIME IS PROPERLY CONFIGURED BY LEVERAGING NTP

- Devices MUST be configured to use at least 2 NTP servers for time syncing
- Avoid relying on the local clocks for time management
- Leverage Active Directory Domain Controllers for time management
- Kerberos require skew of not more than 5 minutes
- Configured the devices to use UTC
- Show the users information based on their timezone
- Leverage NIST Special Publication 800-92

The Person with one clock KNOWS the time,
the person with multiple clocks is NOT SURE about the time

AGENT vs AGENTLESS

- Agentless reduce the attack surface
- Agentless requires less software to manage
- Agentless in general brings easier management
- Agentless may require additional credentials with admin privileges

- Agents do provide added benefits
- Maybe able to leverage encryption features not natively available
- Maybe able to leverage integrity features not natively available

Where possible go AGENTLESS

FORENSICALLY CAPABLE IS WHERE WE NEED TO BE

- Starting Point: Business Needs before Technology Solutions
- The Facts: Incidents and Exposures will continue to rise
- Assume you will be compromised next
- Being forensically capable is not that difficult
- Can be expensive based on business needs
- But can also require little resources

- Don't wait until you are compromised to verify you are forensically capable

It can be done!

REFERENCES:

- NIST 800-92 - http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
- http://www.cbc.ca/news/politics/stephen-solis-reyes-accused-in-cra-heartbleed-hack-has-case-put-over-1.2709556
- Risk Based Security - 2015 Data Breach Trends
- http://www.rsyslog.com/doc/v8-stable/tutorials/tls_cert_summary.html
- https://drive.google.com/file/d/0B0qDfJ30s2I9QzlGT2dqRVQxY28/view

Q&A:

securitynik.blogspot.com