Architecting For Detection

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

Disclaimer

The views expressed here
are my own
and in no way
reflects those of my employer

Our objectives

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

About me

- In technology for around …. maybe a little too long
- Last 10 more focused on security
- Sr. Manager, Cyber Security @ Managed Security Services Provider (MSSP)
- Teach SANS 503 – Intrusion Detection in Depth &
  SANS SEC504 – Hacker Tools, Techniques, Exploits and Incident Handling
- Masters in Cyber Security Forensics
- A few industry certifications including:

  CISSP | GCIH | GCIA | CCNP R&S and Security | Splunk Admin | ISO9001 etc
- Blog at www.securitynik.com

What is meant by architecting for detection

- Architecting a network in a way that allows an 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

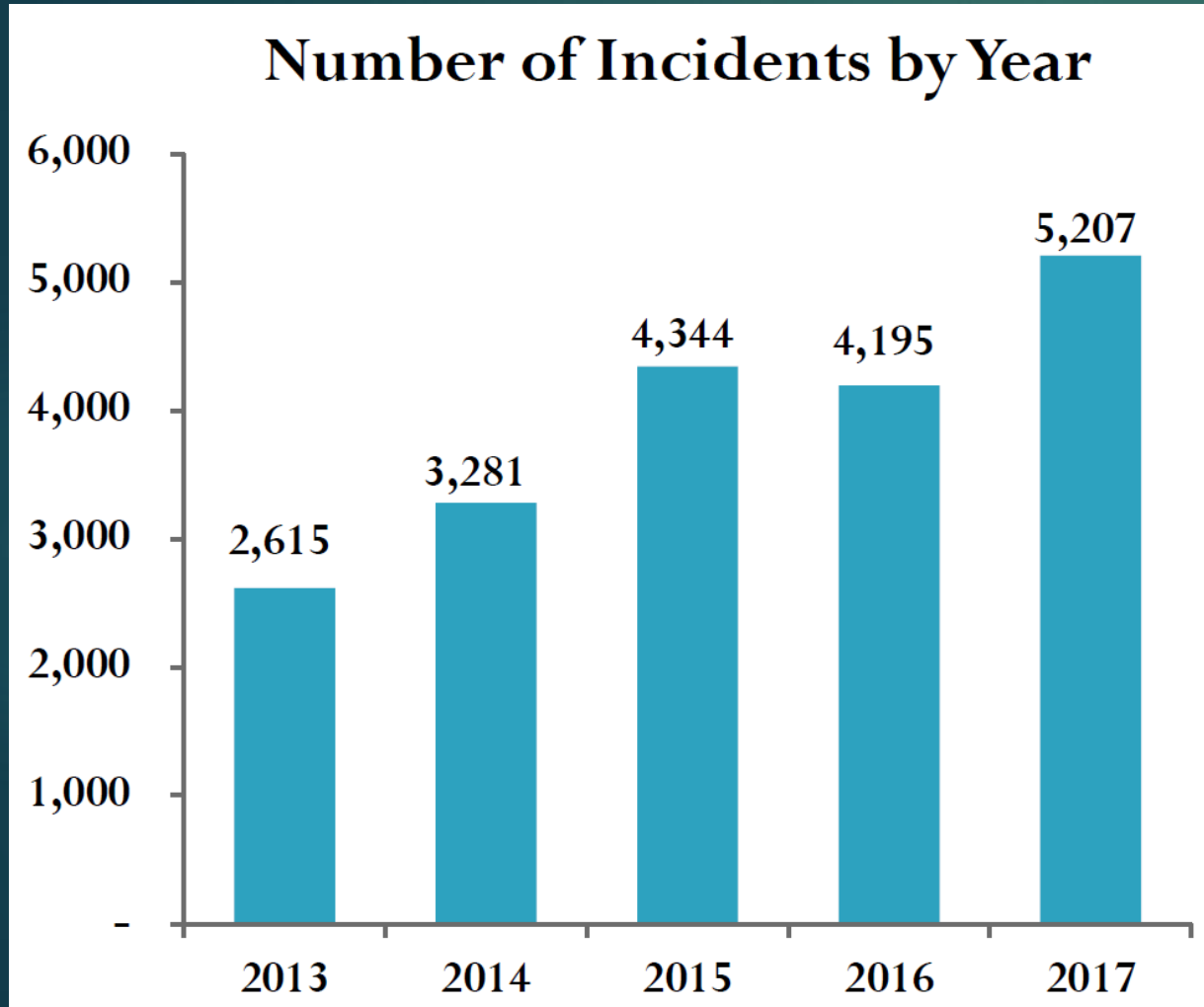
- While this can also be done for operational purposes such as establishing baseline, identifying operational (d)efficiencies, the objective of this presentation is strictly from bullet 2's perspective

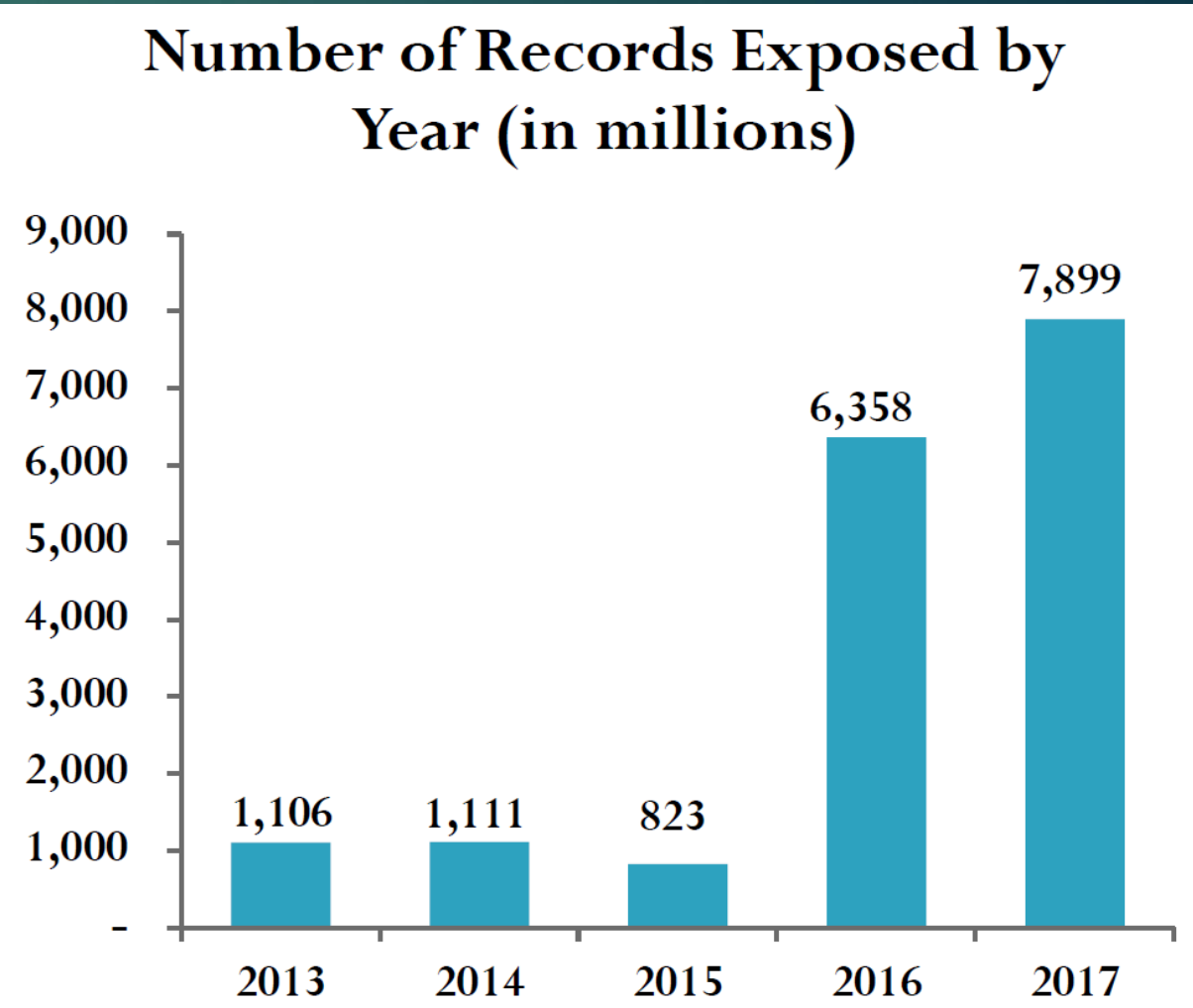
Considerations for being architecting for detection

- 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

2017 Year End Compared To Previous Years





* Risk Based Security – Data Breach Quick View Report, Data Breach Trends – Year End 2017

Facing the facts

- Cyber crime in 2016 was US$600B
  2014 it was US$500B
- 2017 Considered the worse year on record
- 5,200 Breaches Reported
  Up 24.1% from 2016
- 7.89 Billion Records exposed
  Up 24.3% from 2016
- Hacking leads the way @ 55.8%
  Hacking considered as unauthorized intrusion

* CSIS - Economic Impact of Cybercrime – No slowing down
* Risk Based Security – Data Breach Quick View Report, Data Breach Trends – Year End 2017

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

Peeking into the future

- does not look like it will be much better
- New devices added everyday
- Internet of Things (IoT)
- Misconfigured cloud environments
- The list goes on

We're heading for an interesting future!

What does 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, analyze, detect
- Assume you have been compromised …
- … or will be soon

Ensure the network is architected for detection

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

So many technologies

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

So many tools

SIEM	Log Aggregators	Flow Collectors
Full Packet Captures	SSL Decryptors	Event Collectors
Event Processors	Endpoint Detection and Response	IDS
Network Analysis Framework	Wireless Security	AntiVirus
Etc	Etc	Etc

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

What do we need?

- To prioritize
- 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)

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

An open source tools perspective

- Full Packet Capture (can be expensive)
  tcpdump, thsark
- 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

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
- Forward non cleaned or non-blocked malware data
- Configure firewall permits and denies
- Capture attempts to elevate privileges
- Capture attempts modify critical accounts and groups
- Forward proxy events

Yes you can capture everything

BUT can you action and or retain everything … Prioritize

Protect the confidentiality, integrity and availability of captured data

- Manage integrity of logs
- Manage 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

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

Reliance on multiple data sources for intelligence purposes

- Know your infrastructure
- 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

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
- Consider using Active Directory Domain Controllers for time management
- Domain joined computers and servers have to be within 5 minutes of each other for Kerberos to work properly
- Configured the devices to use UTC
- Show the users information based on their timezone
- Leverage NIST Special Publication 800-92 (Guide to Computer Security Log Management)

The Person with one 1 watch KNOWS the time,

the person with multiple watches 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

Q&A:

www.securitynik.com

Coming soon: n^{3}security.com