The road to nIRvana

Rob Lowe
acknowledgements

- Jakub Bittner
- Matthew Braid
- Doug Brown
- Alistair Chapman
- Franta Kolacek
- Jay Madison

- Fran Marquez
- Richard Monk
- Alison Perkins
- Ilin Petkovski
- Nick Pratley
- Ivan Stojmirov
me

• 20 years in IT and 15 in information security
• Incident Coordination and Response and Security Operations
• AusCERT, CERT Australia, Red Hat
Red Hat

• The world's leading provider of open source, enterprise IT solutions
• US$2.92B revenue in FY18
• 90+ offices in 35 countries
• Approximately 4,500 employees in 2012, now almost 14,000

• Culture of openness and freedom
• Values: Freedom, Courage, Commitment and Accountability
infosec@redhat

• Overview of the last 7-9 years of Red Hat’s Information Risk and Security Team
• Corporate Information security - founded in 2008
  o (Product Security founded in 2001)
• Red Hat systems and data
  o Also some community work
this presentation

- Warts and all
- Detection focus
- Our (continuing) road to nirvana
- Middle of the road in maturity
2008, 2009, 2010

- Team establishment
- Significant incident (RHSA-2008:0855)
- Regional hubs with MPLS
- Strong North American focus
- Infosec team expands to Czech Republic in 2010
2011 (i)

• Expansion into APAC time zone (Australia)
  ○ Tooling to enable handoffs and dispersed Team coms
• Moving to a Managed Security Service Provider
  ○ Decision to provide immediate capability
  ○ IPS - concern about the risk of false positives
  ○ Signatures were carefully tuned
  ○ Mixed signatures, skewed towards server, rather than client
2011 (ii)

• MSP pain
  ○ Technical staff frustrated with a blackbox
  ○ Don’t know us (business, risk, assets)
  ○ MSP not having a clear threshold

Me: “Why did you escalate alert X, but not alert Y.”
Operator: “Because we thought you’d like to know.”
MSC aren’t inherently a bad idea, but will be more productive with

- Clear scope
- Well defined tasks and context
- “Commodity” functions

MSCs are often used for services for which you don’t have a capability (often experience). Without that experience, it is hard to define what you need.
2012 (i)

- Netflow
  - Commercial tool
  - Slow
- IPS failure
  - Layer2 failure of the bypass switch
  - Taking out the network in a major datacenter
“Additionally, because your sensor is inline with production traffic, expect repeated scapegoating of the device when something goes wrong with the network.”

Chapter 7: Tools of the trade
Intrusion detection isn’t dead
Stand up of PoC IDS

- Snort IDS & BASE GUI
- Built on repurposed hardware
- Immediate value - insight and control
- Still lacking context
- Emerging Threats
  - Community and paid subscriptions
2013 (i)

• Centralised logging

• \o/ no more:
  for h in hosts
    ssh root@$h grep ...

TLP: AMBER (FIRST TEAMS ONLY)
NO PHOTOGRAPHY

14
2013 (ii)

- Because Cloud
- Hybrid cloud DC
- SaaS footprint increasing
  - SAML on most services (now)
  - API/logging access wasn’t often considered
2014 (i)

- Began to move away from MPLS to hubs
- Direct internet connections at site + VPNs
- Planning for 80 locations in 30 countries
- Opportunity to roll out new network monitoring infrastructure
  - In warranty hardware
  - 50+ sensors
Open source NSM stack

- alerts
- indefinite
- connection logging
- 6 months
- full packet capture
- up to 7 days
2014 (ii) Implementation

• Logistics/ordering/cost in 30 different countries
• Maintenance effort
  ○ Not the usual footprint for local offices
  ○ bcfg (retired), Ansible, puppet, satellite, clevis, Zabbix
  ○ Wiring, local hands issues
  ○ Failures/warranty
2015 (i)

- GUI migration to Snorby
- Truffle
  - Historical activity on signature and/or IPs
  - Enrichment
  - Started out as an add-on
2015 (ii)

• Charlotte
  ○ Python replacement for barnyard - now open source
  ○ Multiple snort instances per sensor
  ○ Graceful handling of map changes
  ○ Improved database connection handling
  ○ Lower resource footprint
  ○ https://github.com/redhat-infosec/charlotte
2015 (iii) - Inspiration

“How We Saved the Death Star and Impressed Darth Vader”

Matthew Valites and Jeff Bollinger
FIRST 2015 (Berlin)
2015 (iv) - Inspiration

“Automated Detection Strategies”

John Davison
BsidesCincy 2015

Hunting and Tuning

- The detection team can handle $X$ alerts in a day.
- If $n \geq X$ then tune.
- If $n < X$ then hunt.
- Hunt + Tune $\Rightarrow$ Coverage++
2015 (v) - Inspiration

“Keynote: What Got Us Here Won’t Get Us There”

Haroon Meer
Blackhat Europe 2015
2016 (i)

- Restructure of the team
  - Structured GRC function
  - consideration: move to a tiered triage model?
  - Hired dedicated operations staff
- Alert fatigue
- Started crafting the infosec playbook
“A SOC typically will designate a set of individuals devoted to real-time triage of alerts, as well as fielding phone calls from users and other routine tasks. This group is often referred to as Tier 1.”

Fundamentals (page 11)
2016 (ii)

• Tiered SOC: your least skilled analysts are making the most important decision.
  ○ Continue with skilled analysts handling alerts
  ○ Local liaisons?

• Ideally detecting on correlation of activity over isolated alerts
  ○ Snort becomes just another log file
  ○ Focus detection on high value assets, rather than attempting to detect across our entire client population
2016 (iii)

• Switch to a commercial SIEM
  ○ Excellent alerting
  ○ Risk scoring (based on asset value)
  ○ Enrichment just OK (still a bit of “tab hell”)
  ○ Poor incident management

• Expertise still a critical factor
“The SOC must weigh trade-offs between custom tools that provide more flexibility and commercial tools that have vendor support, all while factoring in the total cost of ownership (TCO)”

Fundamentals (page 39)
2017 (i)

- Incident Response Plan review
- Communications tracking
  - Separation from our IR tooling
  - Integration via a communications framework
  - Inspiration from Dropbox’s securitybot
“Building a Threat Hunting Framework for the Enterprise”

Joseph Ten Eyck
FIRST 2017
2017 (iii)

• Lessons Learned in Detection Engineering
  Ryan McGeehan
  ○ Rules are codified and subject to peer review.
  ○ Rules trigger automation before alerting.
  ○ Hunting makes a great sandbox for new rules and new alerts.
  ○ Employees are a part of the alert escalation path.
  ○ Information is captured on closed alerts.
  ○ Frequently used investigative tools are integrated.
2018 (i)

- The next organisational iteration
  - Dedicated Threat Intelligence team
- Incident management process refinement
- Communication tracking tool
- MISP
  - Consuming intel feeds to enhance alerting
2018 (ii) - Challenges

- Couldn’t quite let go of some legacy alerting
- Incident management
  - text files to track alerts
  - IoC management
  - Metrics
- Play development slow
  - Time and prioritization
  - Inspiration
  - Understanding of the objective
  - Search-fu
The road ahead

● Incident management processes improvement
● Integration of tools
● Continued development of playbooks
● Automation - both comms and response
● Planning for “Local liaisons”
References and further reading

- **The Art of Detection Using Splunk Enterprise Security**
  Doug Brown (SplunkConf 2017)

- **Crafting the InfoSec Playbook**
  Jeff Bollinger, Brandon Enright, Matthew Valites

- **Ten Strategies of a World-Class Cybersecurity Operations Center**
  Carson Zimmerman

- **What Got Us Here Wont Get Us There**
  Haroon Meer (Blackhat Europe 2015)
References and further reading

• **Enterprise Security: The wood for the trees?**
  Haroon Meer (Blackhat Europe 2015)

• **Lessons Learned in Detection Engineering**
  Ryan McGeehan

• **Automated Detection Strategies John Davison**
  John Davison (BsidesCincy 2015)

• **Building a Threat Hunting Framework for the Enterprise**
  Joseph Ten Eyck (SANS Threat Hunting Summit 2017)
Questions & Discussion

• rlowe@redhat.com
• infosec@redhat.com