Logs and Tactical Defence

Allan Stojanovic
David Auclair
University of Toronto
#include <disclaimer.h>

Our Environment

- Six /16 IPv4 networks one /32 IPv6 network

  (393,204 Ipv4s and 4,294,967,296 /64s)
- > 600 Departments / Faculties / Affiliates
- > 450,000 users in our IdM

We are a city unto ourselves

Our Drivers / Motivators

- A (mostly) open network
- Departments are largely autonomous
- Research means a lot of intellectual property
- Not a big budget (but who does?)
- Academic Freedom

Every Make, Model, Vintage and Skill level

(https://youtu.be/f48lOuHmVxI)

The Original Six

- **Trial By Firewall**: Expanding denied access
- **Dr. Bad Touch**: Network wide honeyports
- **Blatant 404**: Known bad requests
- **Impossible Multi-Auth**: Untravellable access
- **Questionable Single Source**: Many logins from a single place
- **Phake-Phishing**: Feeding fake creds.

The Original Actions

- Bad intentions deserve to be denied all access
- Attempt to block the attacker, not just the attack
- Whitelist where appropriate
- Worry less about false positives but minimize them
- Investigate and test your recipes

The Original Actions (2)

- Aggregate attacking IP addresses
- Investigate repeated compromises, user or machine
- Check for “hotspots” of compromises
- Research and share (threat intelligence)

The Original Reactions

- Quarantine or block permanently from critical systems or the entire Org.
- Redirect to “safer” places. Like honeypots.
- Whitelist
- All-404 (make the website disappear)
- Be prepared to release quickly
- Log everything you do


PLEASE STAND
BY
WE ARE
EXPERIENCING
TECHNICAL
DIFFICULTIES

Location Detection Failure

- Introduced GEOIP errors in feeds
- IPv4 churn
- Proxies, TOR, and others

- De-anonymize (web) logins
  - Too much surveillance?

Device Limits

- Maximum number of firewall rules
- Maximum number of firewall object definitions
- Maximum number of IPS quarantines
- Maximum number of IPTABLES deny rules

There is a practical limit and theoretical limit to consider as well.

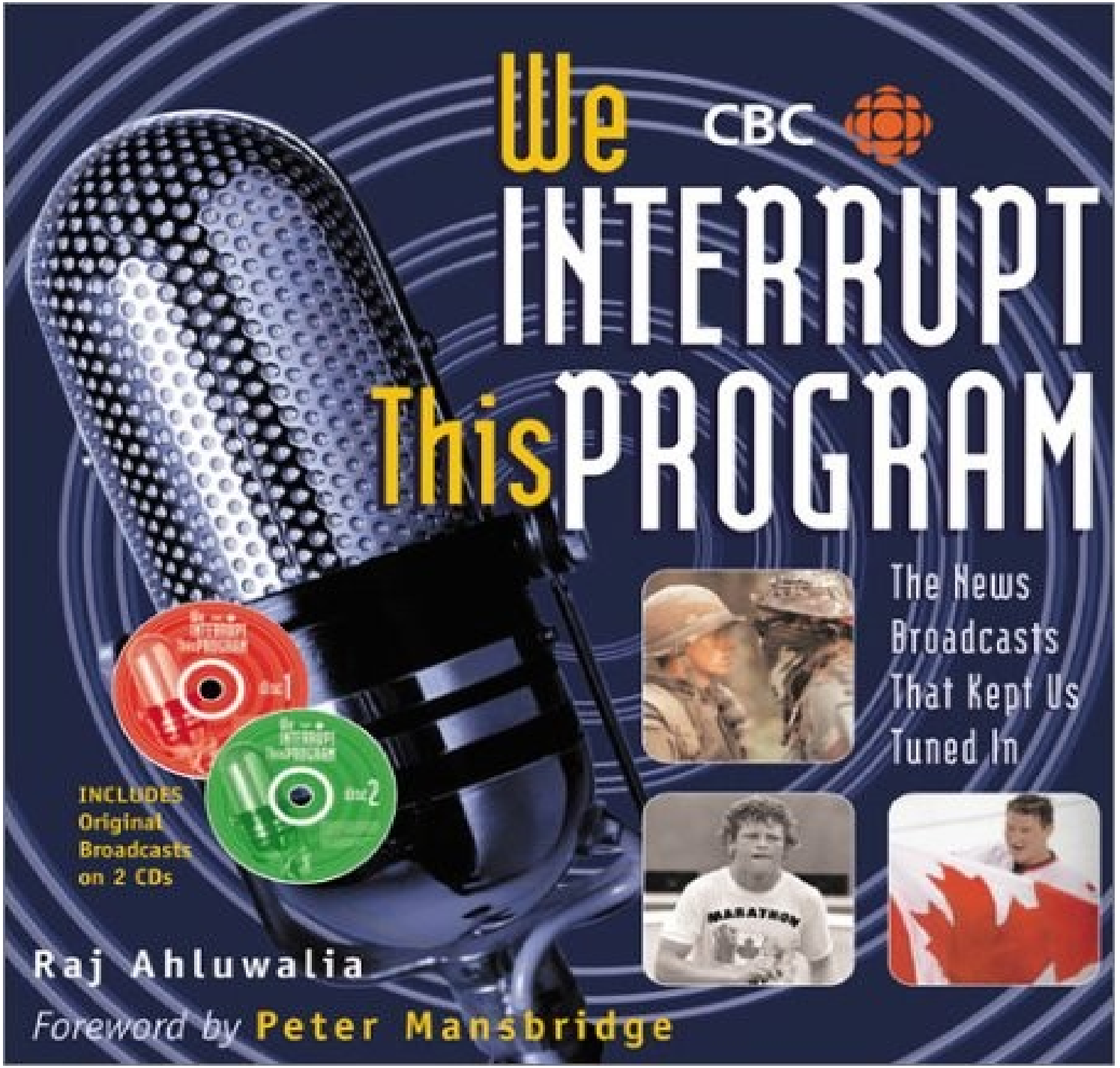
Device Capability Failures

- Fail open vs. Fail closed
- “Leaky” ruleset
- Operational limitations (IPS firewall rule reload)
- And all the usual memory, storage, and bandwidth problems

“False Positives”

- False positives
  - User remotes to workstation then to a server
  - A technical problem
- “False positives”
  - Assistant with the user's password
  - An organization problem

An Opportunity for (Re)Education


We CBC
INTERRUPT
This PROGRAM
The News Broadcasts That Kept Us Tuned In
INCLUDES Original Broadcasts on 2 CDs
MARATHON
Raj Ahluwalia
Foreword by Peter Mansbridge

The 5 stages of Infosec ...

- DENIAL
  - We have never been hacked
  - We have nothing they want
- ANGER
  - How dare they hack us!
  - I told you so.
- BARGANING
  - Please don't hack us again
  - Don't leave, we're secure now!
  - Free credit monitoring!
- DEPRESSION
  - HOW many attacks per hour?!
  - We are so f**ked.
  - Murphy was an optimist.
- ACCEPTANCE
  - We can learn from this
  - We can do better
  - There is no silver bullet

... versus the Pentest Army

- You are under constant attack
- They have all levels of skill, and are relentless
- They are actively trying to subvert / deceive you

BUT

- *They cleverly hide their reports in your logs*
- Why wait? Hack yourself first! (And watch your logs)

SO

- Can we skip the painful steps and go directly to acceptance?

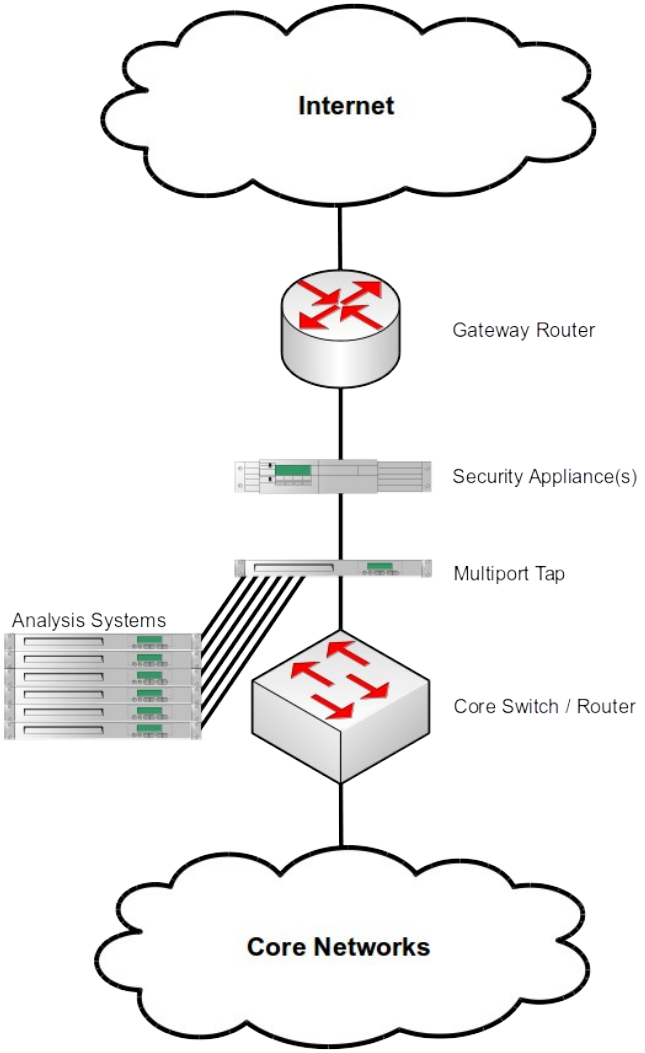

WE
NOW
RETURN
TO
MOAR Logs and
Tactical Defence

Our Visibility Project

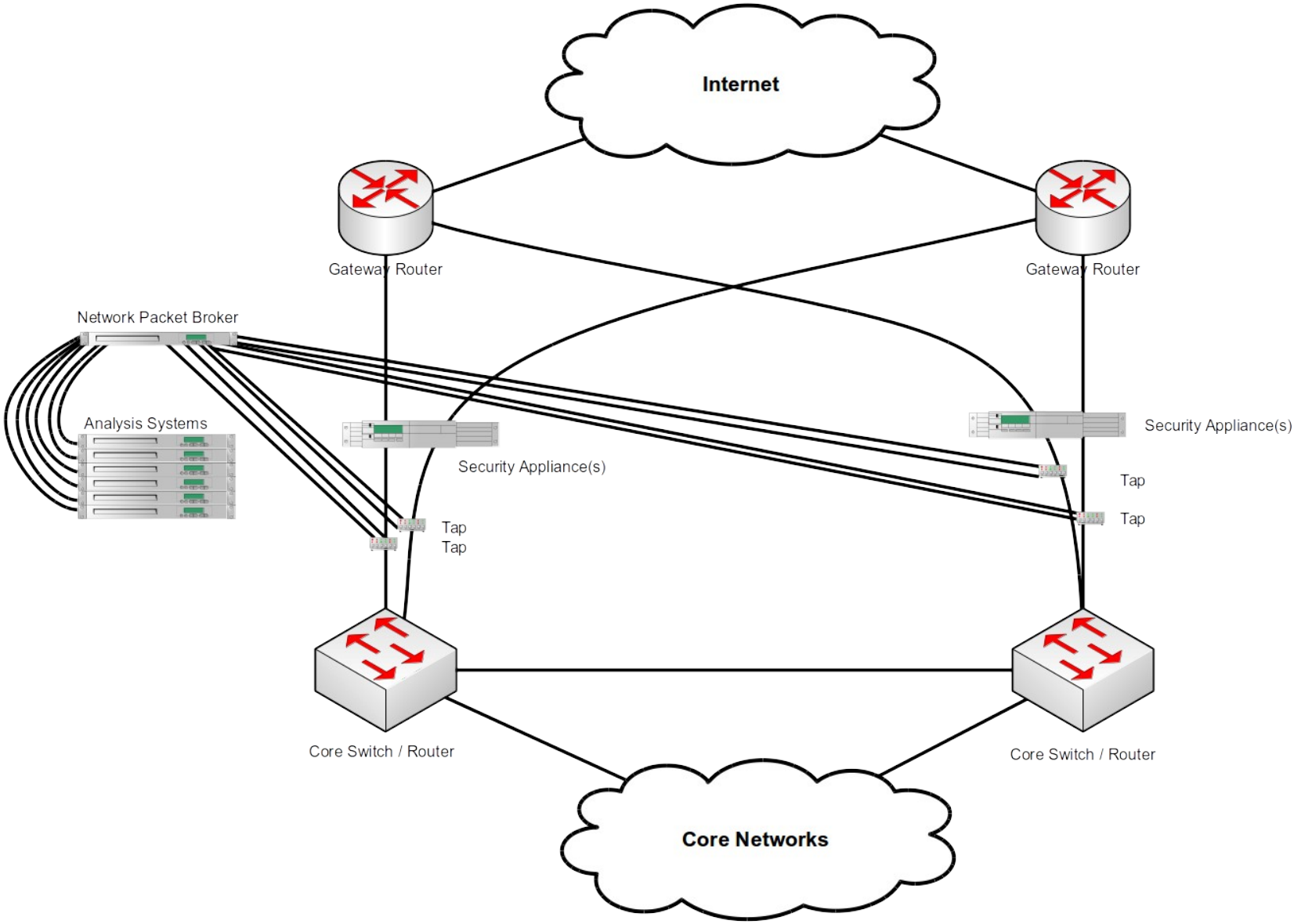
Monitor All The Things

- Monitor systems & network traffic
  - Netflow
  - Metadata
  - PCAP
  - System Logs (syslog, event logs, etc)
- Get logs from non-cooperative systems

Visibility Project (2)



Visibility Project (3)



Anomaly Detection

Pick out the interesting bits from the logs

- Too many logs, need to automate
- Protocol Anomalies (SSH, RDP, etc)
- Timing Irregularities
- Case Irregularities (Username != username)

Anomaly Detection Actions

- Block the remote host
- Redirect to honeypot
- Careful not to block Google/Bing/etc

- Automation isn't “Fire & Forget”
- Attackers are intelligent and work around obstacles

Attack Tool Signatures

Classify and/or fingerprint known and unknown attack tools

- Some tools announce their use (ncrack, THC-IPv6)
- Other tools have characteristic patterns (NMAP)
  - Pattern may shift by attack stage (AppScan)
- Common attack pattern (SQLi, etc)
  - Develop custom signatures (“SeLeCt”)

Run the tools.

Attack Tool Response

- Block them, as usual.
- Review actions and responses
- (Re) Test the attacked target

- If you know the attack tool, you can validate their findings.

Retrospective Review

Keep an appropriate event history

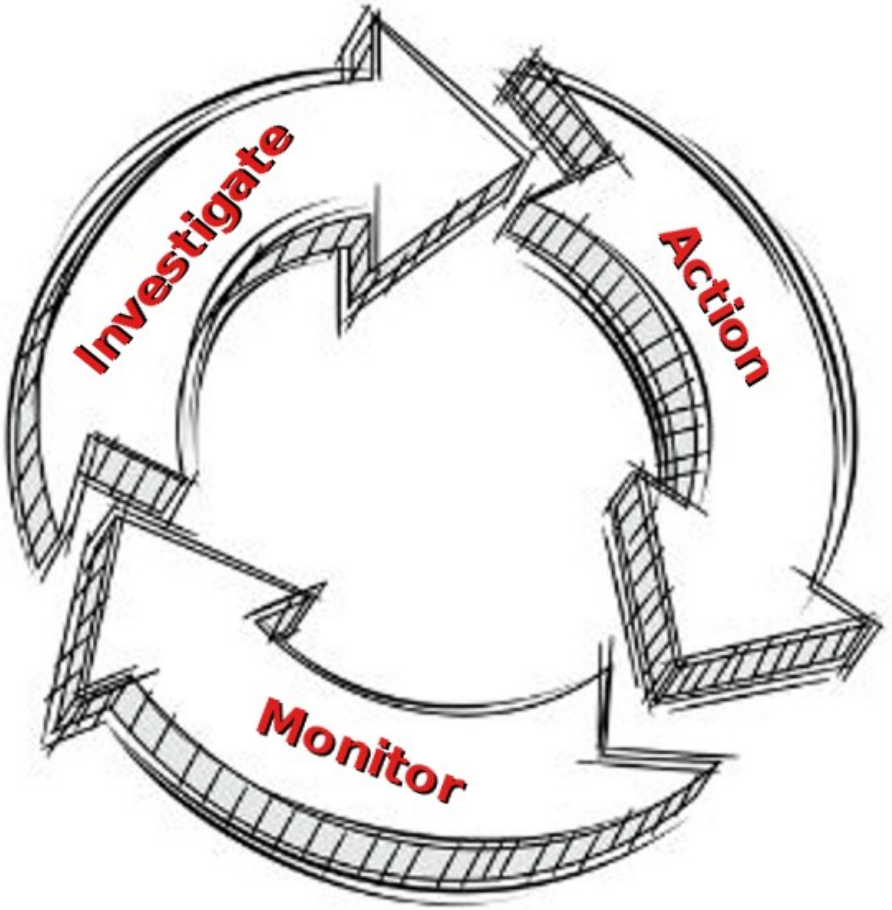
- Review new IOCs against old data
- For example new Angler C2 recently discovered
- Hits against C2 IPs is good
- Hits against C2 domains is better
- Full PCAPs is *badass*

Automated Analysis

- Monitor metadata flow in real time
- Anomaly detection “on the fly”
- “Leaky Bucket” scoring system
- Automated blocking
- IP blocking history contributes to the score
- Avoid false positive loops

- Attack traffic tends to increase every Friday night

Simplified Care and Feeding



404.TransitionSlideNF

Asset Management

- Automatically check addresses against known assets, especially for Ipv6 + privacy extentions
- Do you track vhosts as assets?
- Alert on new assets?
- Find “unregistered / unmanaged” assets?
- Report on dormant assets?
- Cross-reference with ...

Vulnerability Management

- Scan new assets automatically
- Check against passive vulnerability DB
- Report what is found often (daily? Weekly?)
- Fill in missing data (ownership, etc)
- Report assets unreachable by the scanner?
- Especially good for IPv6

Threat Intelligence

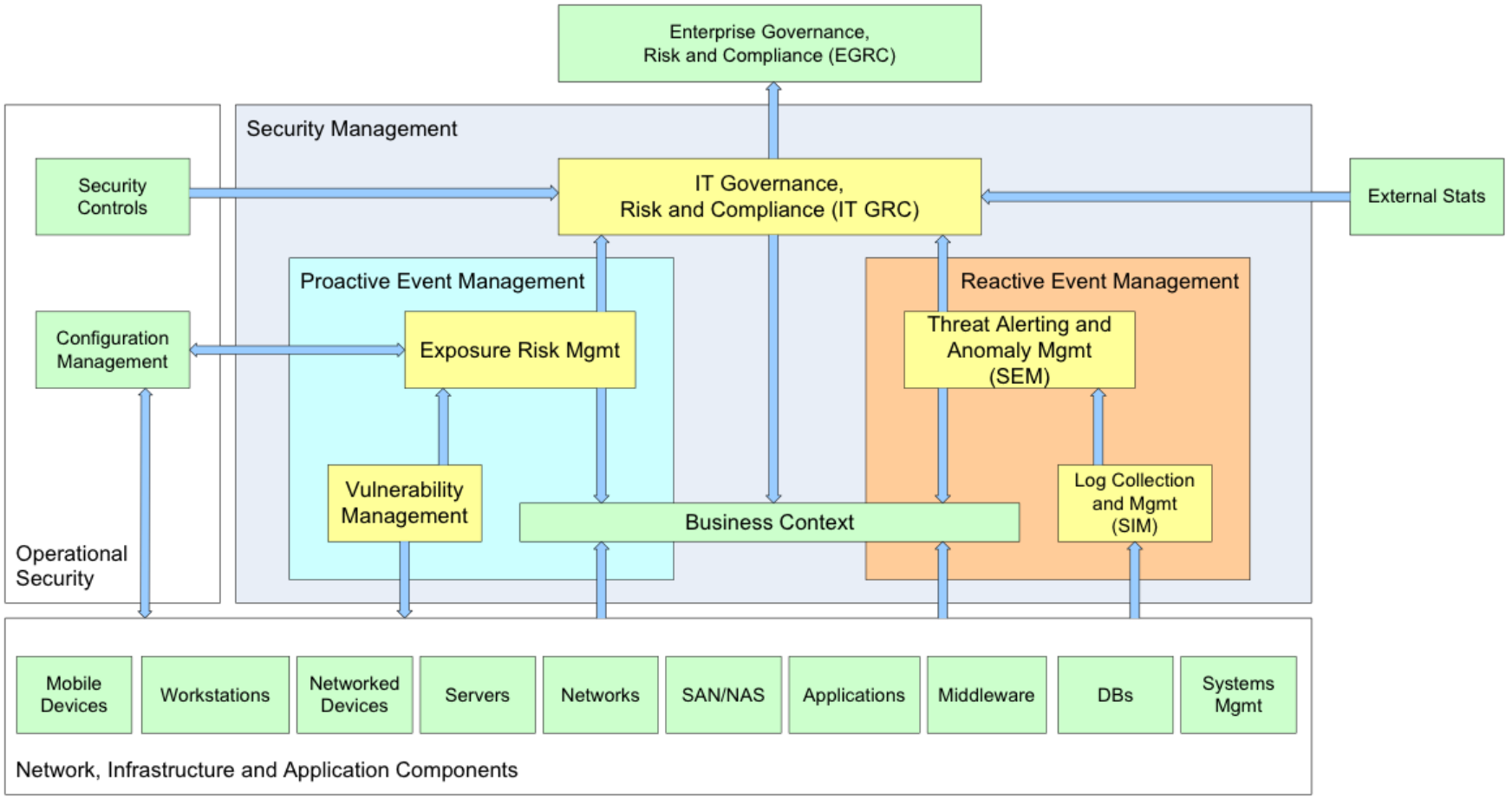
- Check against an external feed or three
- Create an internal one as well
- Use the recipes to discover incidents against you
- Use the TI feeds to enrich the incidents / give them some context (hopefully)

Incident Response

- **ALL** of the previous information can be used to enrich almost every aspect of the incident report
- **INCLUDING** the question of intent
- **AND** maybe even the effort expended by the attackers to do so.

(Now if only we can get that attribution problem solved too)

Fitting to a GRC model




Next Time On
THE WALKING DEAD
Logs and Tactical Defence

IPv6

- Random / sequential scanning? Not likely.
- Quarantine / block single IP addresses? Even less likely.
- Block entire /64s? Maybe.
- A slanted version of Dr. BadTouch with DNS records is possible
- Latest thc-ipv6 tools has built in sigs, We must check for them...

IPv6 (2)

2^96 hosts

=

79 octillion 228 septillion 162 sextillion 514 quintillion 264 quadrillion 337 trillion 593 billion 543 million 950 thousand 336 *

*** wolframalpha.com**

Software Defined Networking

- Total on-the-fly control of the network flow
- Redirect questionable network activity with ease
- Choose network paths with different toolsets
- In combo with “private cloud”, redirect traffic to a “safe” image (Dev, QA, Prod, Honey?)

Outgrowing Your Solution

- When your firewall can't handle more deny rules or object definitions
- When your IPS can't handle more quarantine rules
- Can you upgrade?
- Can you scale?
- Can you safely ignore some subset of traffic?

I don't know what this looks like yet, but I'm about to find out.

Questions?

John and Ash:
Patron Saints of Tactical Defence