RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-W02

The Rise of the Purple Team

Robert Wood

Head of Security
Nuna
@robertwood50

William Bengtson

Senior Security Program Manager
Nuna
@waggie2009

#RSAC

Typical Team Responsibilities

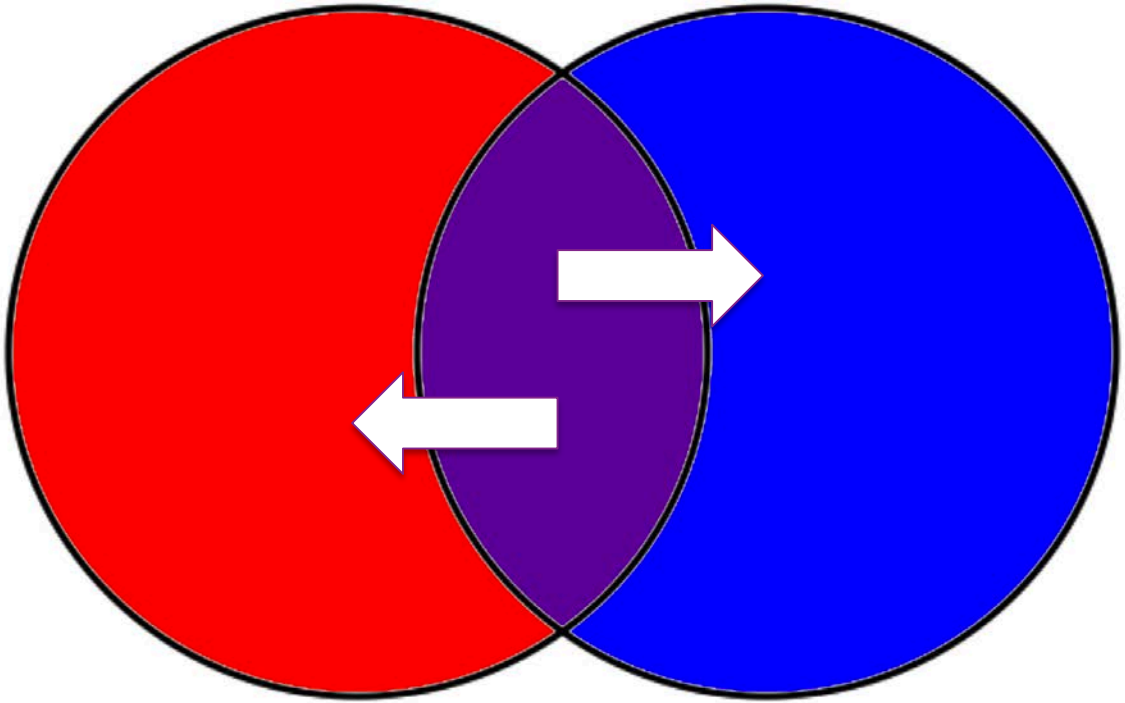
Red

- Vulnerability scanning
- Social engineering
- Physical and digital pentesting (typically done in a vacuum)
- Open source intelligence gathering

Blue

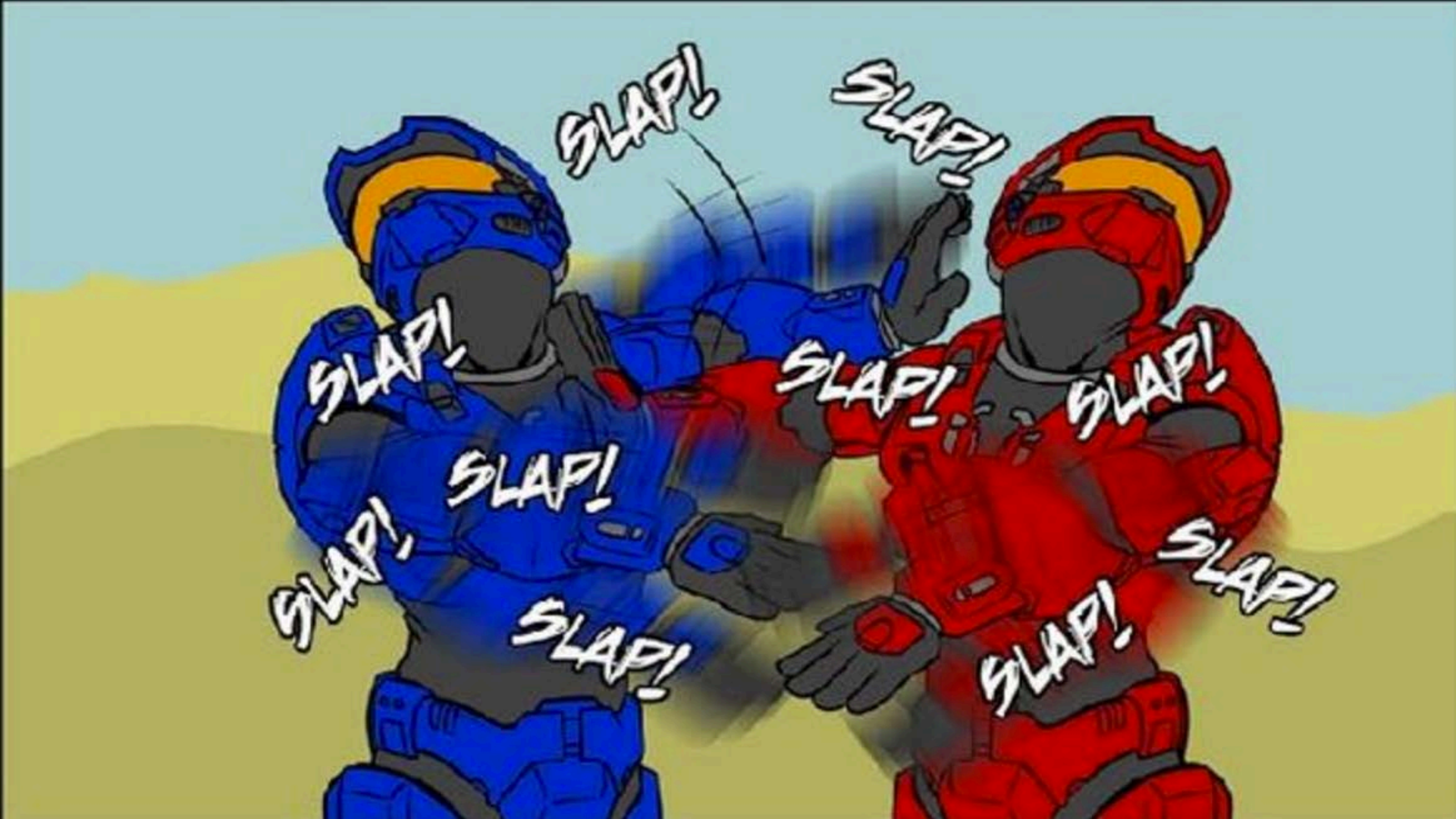
- Threat intelligence
- Malware and exploit reverse engineering
- Digital forensics
- Active monitoring

Overlap



Current State

-  and  often operate in a vacuum on a day-to-day basis, sometimes even within their own teams
- Feedback loops consist of reports being tossed over the wall if shared at all
- Emphasis is given on remediation of vulnerabilities rather than prevention and detection growth
- Teams are incentivized by their ability to outwit the other side
-  are often composed at least partially of outsourced groups


SLAP!
SLAP!
SLAP!
SLAP!
SLAP!
SLAP!
SLAP!
SLAP!
SLAP!
SLAP!

Team Structure and Incentives


I DONT ALWAYS
PENTEST
BUT WHEN I DO I
DONT SHARE RESULTS
imgflip.com

Org Chart Issues

- Teams typically report to different leads with different agenda, objectives, etc.

Misaligned Incentives

Red Team

- Big scary report = job well done
- Success is dependent on how many controls the team can bypass (Blue team failure points)

Blue Team

- No alerts = preventative controls all worked!
- A lot of alerts means that detection capabilities are firing on all cylinders

Aligned Incentives

Purple Team

- Big scary report = improvements
- No alerts = badly tuned SIEM
- No attack success = New TTPs for
- Success is improvement in both attack and defense

Red Teaming

What does  look like at your company?

Approach

- Passive reconnaissance
  - OSINT
- Active reconnaissance
  - Port scans
  - Service discovery
- Vulnerability referencing
  - CVE?
- Social engineering
  - Emails
  - Physical

What should it look like?

Approach

- Passive reconnaissance
  - OSINT
- Active reconnaissance
  - Port scans
  - Service discovery
- Vulnerability referencing
  - CVE?
- Social engineering
  - Emails
  - Physical

Feedback Loops

How'd you do that?

- Team paring:
  - Allow the  to see how things work:
    - Exploits
    - Pivoting
    - Credential harvesting
  - Allow the  to see how things work:
    - Active monitoring and alerts
    - Response playbook
    - Policies
- What are the specific forensic artifacts from all of the above?
- Do we understand why these attacks are succeeding?

Can you see me now?

- During vulnerability scans and more in depth exploit attempts:
  - Does the  have logs of all attack activity?
  - Are alerts set up for successful or continued attempts?
  - Does the  know how to query logs for attack activity?
  - What is the response procedure for the various scans and attacks that are attempted?
- Each of the above represent a potential gap that can be improved upon
- This can occur for all parts of an organization (corporate network, product, badging systems, employee workstations, etc.)

Who told you that?

- Manage social engineering campaigns together
- Use experience with real campaigns to drive more realistic campaigns
- Use alerting to modify your TTPs for
- Use to monitor results and cross-reference with reporting from employees

Outsourced Help

- Engage  during scoping efforts and regular touch points where possible for interactive discussions
- Push  to deliver bug reports (i.e. JIRA tickets) instead of 100 page PDFs for tighter integration into remediation workflows
  - Removes a translation step for 
- Have  keep a journal of where, how, and what attacks are conducted for future cross-reference with  hunt teams

Metrics for Success

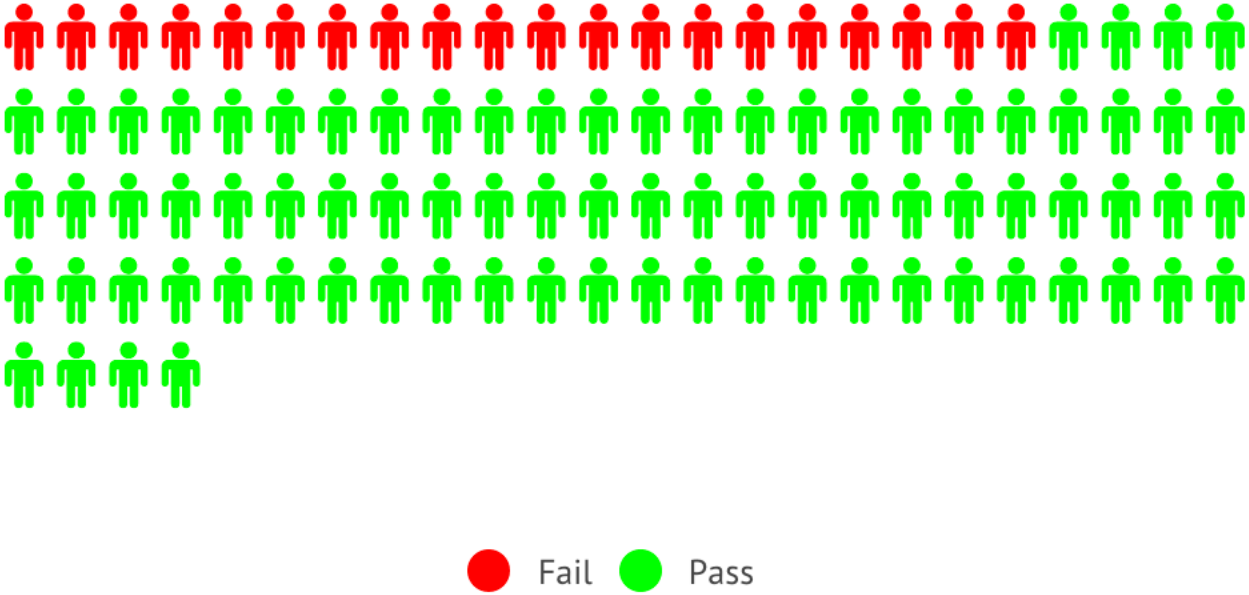
What do I measure?

- Do I measure  or  ?
  - BOTH!

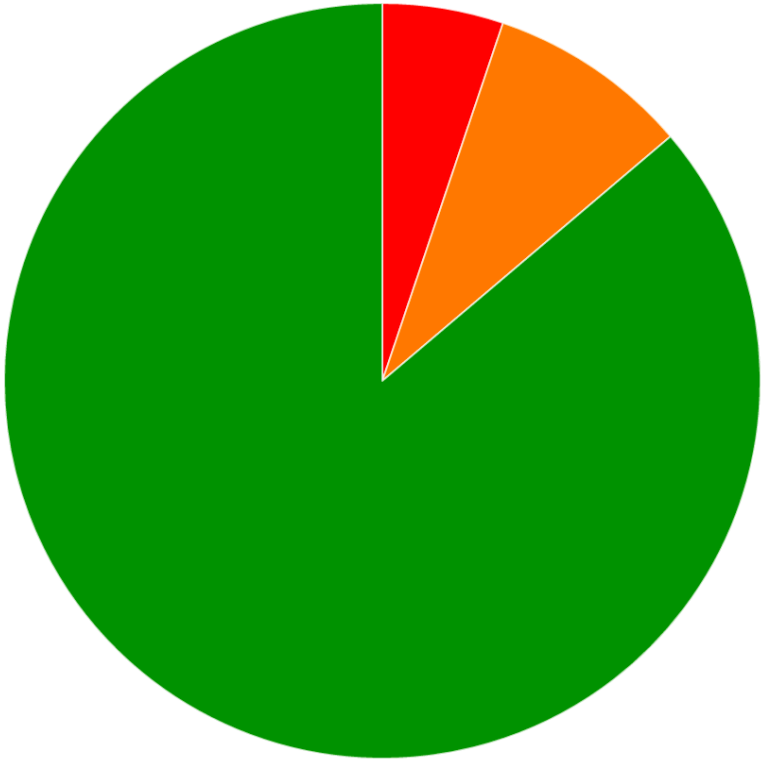
Metrics

- Attack complexity
- Number of targets
- Duration of exercises
- Boxes compromised
- Users compromised
- Historical data

Email Campaign



Vulnerabilities Across Enterprise

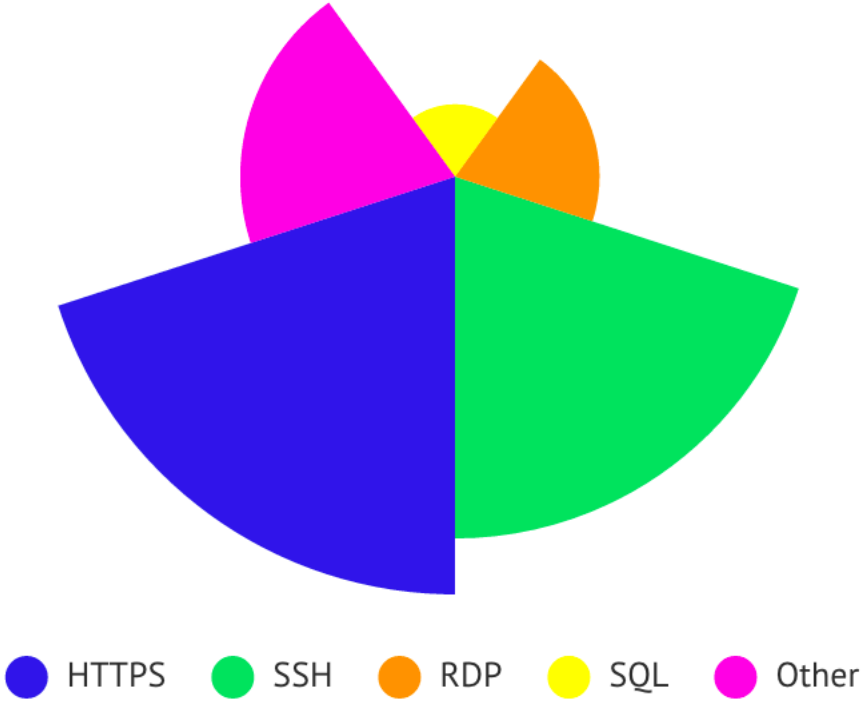


High Medium Low

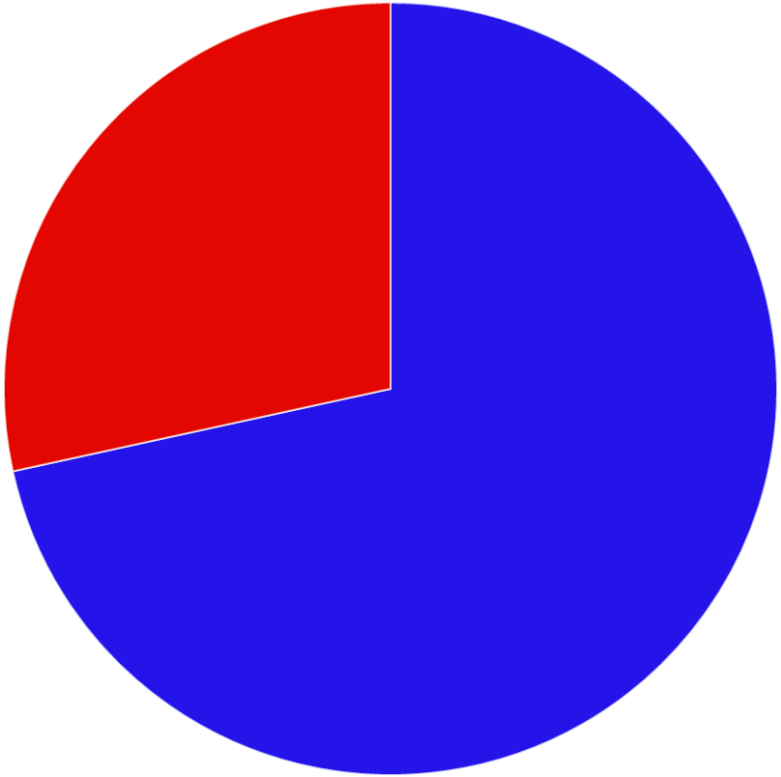
Metrics

- Attacks Detected
- Detection Time
- Response Time
- Forensic Information
- Improvement from Previous Tests

Attacks By Protocol

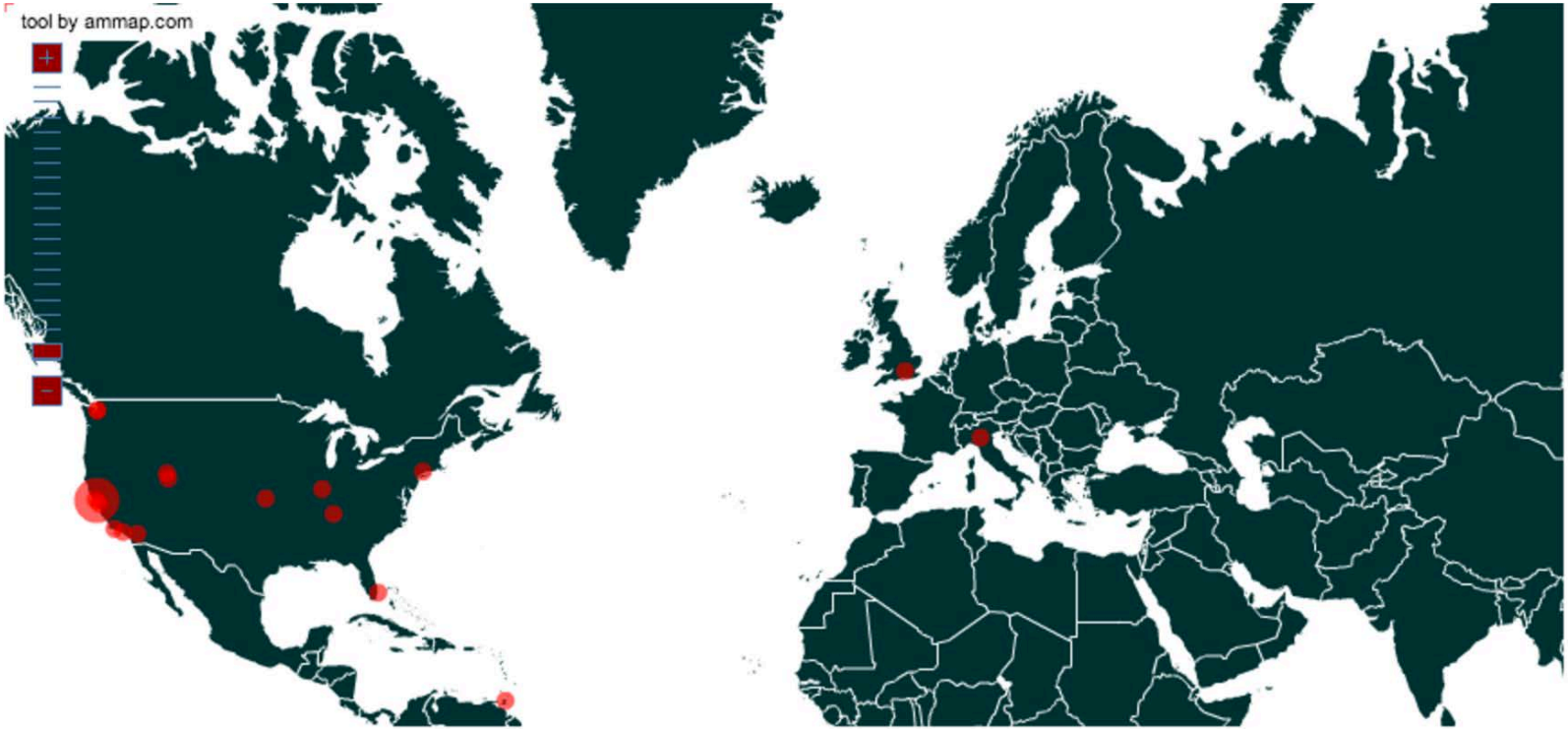


True vs. False Positives



True FP

Login Attempts



https://labs.opendns.com/2013/05/24/big-data-driven-security-with-splunk/

Purple Team Metrics

- Measure improvement scan over scan
- Measure growth in team knowledge
  - learning playbook
  - learning TTPs

Apply It

What should you apply?

- Proactive protection
  - Tabletop exercises
  - Threat modeling
  - Security assessments

Next Week

- Pairing (tester + responder)
- Walk through common techniques
- Walk through protection mechanisms in place
- Identify gaps
  - Improve on these gaps

3 Months Out

- Pairing (tester + responder)
-  exercises with  pairing
  - Execute discovery or payload, determine if it is detectable
  - See what is currently being monitored to determine what tactic to use
- Communication between teams to allow growth

6 Months Out

- Pairing (tester + responder)
-  understands what is being monitored and alerted on. Starts to think what would happen if another vector was used instead
-  starts to predict  attacks and provides preventative measures instead of responsive

6+ Months

- Pairing (tester + responder)
- Continued security exercises
- Each iteration continues to advance in techniques used
- Each cycle improves overall security stature

Questions?

Robert Wood | batman@nuna.com | @robertwood50

Will Bengtson | punisher@nuna.com | @waggie2009