Bringing Cyber Security into Operational Perspective: Visualizing and Securing Key Cyber Terrain

J. Wayne Lloyd | RedSeal Federal CTO & Technical Director
“We continue to put our faith and finances in networks that are increasingly difficult to protect.”

Nilofar Howe, Chief Strategy Officer and Vice President Of RSA

“You know the technologies you intended to use in that network. We know the technologies that are actually in use in that network.”

Rob Joyce, Chief of TAO, National Security Agency
The Shifting Terrain

- Software defined everything
- Digital transformation
- Hybrid datacenters
- Internet of things
- Shadow IT

Skills Shortage

82%

Of global IT leaders report significant labor shortages in cybersecurity today

Source:
April 2016
TechCrunch CIO Report.
Lack of Facts was a 90’s Problem

- We’ve got tons of security tech
- And huge data mountains
- But not enough data mountaineers

Options:
1. Hire people (but they aren’t there)
2. Use fewer products
3. Innovate to get more out of existing tech
Protection and detection are necessary, but not sufficient

Digital Resilience

Comprehensive strategy across all IT functions and business processes to minimize the impact of cyber attacks and network interruptions
A Model For Resilience | The War Room

- Incoming data feeds
- Dashboards
- A map
Be hard to hit
Detect immediately
Respond rapidly
Enemies of Resilience

- **Incomplete Information**: Can I see everything, have I found everything, am I aware of all possibilities?
- **Lack of Actionable Intelligence**: Is the information correlated in a way that allows me to make the best decisions possible?
- **Ability to Act**: Do I have the resources (time, people and skills) to actually act on the information?
What Should Be One Integrated World …
Is Really a Complex Ecosystem

Your Fabric

Cloud & SDN

Security Tech

Network Engineers
Access & Policy

Security Auditor
Audit & Compliance

Security Engineers
Prioritization & Speed
With Serious Gaps

Your Fabric

Incomplete Information

Security Tech

Separate Worlds

Too Many Interfaces

Cloud & SDN

Network Engineers Access & Policy

Security Auditor Audit & Compliance

Security Engineers Prioritization & Speed

Security Auditor

Network Engineers

Security Engineers
Across the technology stack

Across physical, virtual and cloud networks

Across data sources
Gap #1 | Incomplete Information

76% Of CEOs believe they have an accurate blueprint of their network infrastructure

100% Of our deployments find network devices, subnets, and paths that weren’t on the blueprint

Source | RedSeal
2016 CEO Survey
Why is a Complete Picture Hard to Get?

- Gathering half of your network isn’t too hard
- Getting half of the rest costs about the same
- Difficulty goes up fast as you keep going
- Don’t forget, we pay network operations for uptime -- not completeness
- But for security and audit, any gap is crucial
- Bad guys hide in the dark space
Integration #1 | Across Data Sources

- Your network is the chess board
- Your endpoints are the chess pieces
- You have separate teams for each
- Bring the datasets together

We always find:
- Endpoints with no (known) network
- Networks with nothing (known) in them
- Integrating datasets uncovers gaps
Gap #2 | Relating Physical and Virtual Networks

- Cloud isn’t like legacy infrastructure
- Every network is hybrid now
- Fast infrastructure
  - Shifting requirements & providers
  - DevOps: great for speed, less so for control
- Even faster workloads
  - Think Heisenberg – hard to pin down!
- Cloud mgmt. is too much, and not enough
  - Too many details
  - Only single vendor view
• Don’t think beads – think rails
• All virtual machinery is built on rails
  • “Security Groups,” or pick your vendor’s term
• Rails change comparatively slowly
  • Workloads come and go while you watch
• You need to understand how the virtual rails connect to the wider network
Visualizing Pure Cloud Infrastructure

Two Amazon Virtual Private Clouds ("VPC’s")
Threat Access from AWS to On-Premise
Security teams have large security stacks
  • 15 to 50 distinct technologies is typical

Nobody can hire that many experts

The technologies must work together

Vendors listen to your demands
Integration in Action: Tenable or Rapid7 + RedSeal

- Scanners look for things
- Can’t see their own blind spots
- Scanner admins aren’t network access experts
- Integrate scanners with network access mapping
- Automate figuring out what’s blocked, where, why
• Endpoint mgmt. finds your stuff
• Expert on “one-ness” questions
  • What kind of asset?
  • How is it set up?
• Needs integration for “two-ness”
  • Does it have access to Crown Jewels?
  • Is it exposed to outside attack?
• Prioritization needs context
• Results from one vendor directly in the GUI of another
SIEM Alone

Indicator of compromise (early warning sign) based on behavior anomaly and rich data context.

SEIM With Network Context

What is the blast radius?
Which high-value assets can be compromised?
What are my specific containment options?

# Integration in Action | RedSeal and Splunk ES SIEM

## Incident Review

### Urgency
- **CRITICAL**: 0
- **HIGH**: 27044127
- **MEDIUM**: 5216
- **LOW**: 0
- **INFO**: 0

### Security Domain
- All

### Owner
- All

### Security Domain
- Access

### Time
- Last 90 days

### Tag

### Format
- Daily
- By Severity
- By Date

### 0 events during Sunday, July 17, 2016

## Event Details

<table>
<thead>
<tr>
<th>Time</th>
<th>Security Domain</th>
<th>Title</th>
<th>Urgency</th>
<th>Status</th>
<th>Owner</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/31/16 10:51:43.000 PM</td>
<td>Access</td>
<td>host metrics event</td>
<td>Medium</td>
<td>new</td>
<td>unassigned</td>
<td></td>
</tr>
<tr>
<td>5/31/16 10:51:43.000 PM</td>
<td>Access</td>
<td>host metrics event</td>
<td>Medium</td>
<td>new</td>
<td>unassigned</td>
<td></td>
</tr>
</tbody>
</table>

### Description
- This is to host metrics event correlation search

### Additional Fields
- Host Name: 172.16.2.208
- IP Address: 172.16.2.208
- RedSeal Server IP: 172.16.6.231
- RedSeal Server Name: redseal
- Host: splunk
- Host Expected: false
- Host PCI Domain: unlist

### Correlation Search
- Access / host with ID / Rule

### History
- View all review activity for this Notable Event

---

*Image and text content have been extracted and formatted into a readable and natural representation.*
Network Context for an Event
Integration in Action | Looking at Blast Radius
RedSeal Incident Investigation and Containment
Cyber Protection Team (CPT) THAAD Scenario
Cyber Protection Teams are “New Infantry”

- John Hickey, the Defense Information Systems Agency’s cyber development executive
Assess, correct, and maintain overall cybersecurity of a critical Terminal High Altitude Area Defense (THAAD) system.
CPT Scenario Overview

- THAAD is an anti-ballistic missile defense system designed to intercept short-, medium-, and intermediate-range ballistic missiles, and has been produced by Lockheed Martin since 2008.

- Due to the nature of connected systems and software reliance today, most all weapon systems are vulnerable to cyber intrusions and attacks.

- The CPTs assigned to THAAD have a "full time mission ... to protect that THAAD and things like that." (Lt. Gen. Joseph Anderson, deputy chief of staff for the Army's G-3/5/7, 6/1/2017)
Network Topology Overview

- Internet
- IBCS
- THAAD System
- THAAD BNO1
- THAAD HQ
- GIG
- IFCN
- THAAD BL01 & 02
- THAAD Maintenance
Segmentation Validation

Network Policies are compliant.
Threat Query from GIG

Threat queries show that there are no exposed vulnerabilities at this time.

There is no threat from source to destination query.
Outdated Analysis and Threat Reference Library

Model of terrain is out of date

TRL v. 8.5.53, May 1, 2018

Last Analysis Sep 24, 2018 5:32:47 PM
### Status of the Cyber Terrain Model

Model checks identify what data is old and requires updating.

#### Outdated network device configuration data

<table>
<thead>
<tr>
<th>Check ID</th>
<th>Title</th>
<th>Severity</th>
<th>Violation Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>MI-5</td>
<td>Dangling Links</td>
<td>HIGH</td>
<td>1</td>
</tr>
<tr>
<td>MI-8</td>
<td>Stale Devices</td>
<td>HIGH</td>
<td>1</td>
</tr>
<tr>
<td>MI-9</td>
<td>Stale Hosts</td>
<td>HIGH</td>
<td>3</td>
</tr>
<tr>
<td>MI-11</td>
<td>Route to Unknown N...</td>
<td>HIGH</td>
<td>1</td>
</tr>
<tr>
<td>MI-12</td>
<td>Unplaced Objects</td>
<td>LOW</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Import Task

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Import Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>THAAD-BN01-Maint-L3Switch</td>
<td>Router</td>
<td>File Upload</td>
</tr>
</tbody>
</table>
Model checks identify what data is old and requires updating.

### Status of the Cyber Terrain Model

<table>
<thead>
<tr>
<th>Check ID</th>
<th>Title</th>
<th>Severity</th>
<th>Violation Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>MI-5</td>
<td>Dangling Links</td>
<td>HIGH</td>
<td>1</td>
</tr>
<tr>
<td>MI-8</td>
<td>Stale Devices</td>
<td>HIGH</td>
<td>1</td>
</tr>
<tr>
<td>MI-9</td>
<td>Stale Hosts</td>
<td>HIGH</td>
<td>3</td>
</tr>
<tr>
<td>MI-11</td>
<td>Route to Unknown N...</td>
<td>HIGH</td>
<td>1</td>
</tr>
<tr>
<td>MI-12</td>
<td>Unplaced Objects</td>
<td>LOW</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinSrv-Radar-BL02-60</td>
<td>Active Host</td>
<td>10.150.141.60</td>
</tr>
<tr>
<td>WinSrv-TFCC-BL02-60</td>
<td>Active Host</td>
<td>10.150.142.60</td>
</tr>
<tr>
<td>WinSrv-Launch-BL02-60</td>
<td>Active Host</td>
<td>10.150.143.60</td>
</tr>
</tbody>
</table>
Updating Data

Importing data to update the model with current
New Analysis Findings

New data shows exposed hosts in terrain and network segmentation failures

Risk Analysis
- 6% at risk
- 1 Directly Attackable Hosts
- 1 Indirectly Attackable Hosts
- 31 Protected Hosts

Network Access Compliance

<table>
<thead>
<tr>
<th>Host</th>
<th>THAAD-BN01</th>
<th>THAAD-BN01</th>
<th>THAAD-BN01</th>
<th>THAAD-BN01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly</td>
<td>12</td>
<td>2</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>Indirectly</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Protected</td>
<td>31</td>
<td>1</td>
<td>31</td>
<td>1</td>
</tr>
</tbody>
</table>
Network segmentation failures now present after updating cyber terrain model information
Threat from Untrusted

Run query to identify any exposed hosts to untrusted network space due to network segmentation failures
Exposed vulnerable hosts in HQ Ops Subnet
## Attack Vector Details

### Ports, Protocol, IPs and Vulnerability Data

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Target Host</th>
<th>Target IP</th>
<th>Protocols</th>
<th>Ports</th>
<th>Exposure</th>
<th>Vulnerability</th>
<th>Severity</th>
<th>Impact</th>
<th>Patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.156.0</td>
<td>WinSrv-HQ-Ops-50</td>
<td>10.150.113.50</td>
<td>TCP</td>
<td>445</td>
<td>0.99</td>
<td>42106 Ness...</td>
<td>HIGH</td>
<td>ACIS</td>
<td>Yes</td>
</tr>
<tr>
<td>172.16.156.0</td>
<td>WinSrv-HQ-Ops-50</td>
<td>10.150.113.50</td>
<td>TCP</td>
<td>445</td>
<td>0.99</td>
<td>34477 Ness...</td>
<td>HIGH</td>
<td>ACIS</td>
<td>Yes</td>
</tr>
<tr>
<td>172.16.156.0</td>
<td>WinSrv-HQ-Ops-50</td>
<td>10.150.113.50</td>
<td>TCP</td>
<td>135</td>
<td>0.99</td>
<td>34477 Ness...</td>
<td>HIGH</td>
<td>ACIS</td>
<td>Yes</td>
</tr>
<tr>
<td>172.16.156.0</td>
<td>WinSrv-HQ-Ops-50</td>
<td>10.150.113.50</td>
<td>TCP</td>
<td>139</td>
<td>0.99</td>
<td>42106 Ness...</td>
<td>HIGH</td>
<td>ACIS</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Notes:**
- **Source:** GIG
- **Destination:** All Subnets
- **Via:** TCP, UDP
- **Vector:** Direct Attack
## Detailed Path to Vulnerable Host

<table>
<thead>
<tr>
<th>Hop</th>
<th>Flow</th>
<th>Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>IBCS-FW2</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>IBCS-dist-2</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>IFCN-CORE-2</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>THAAD-SYSTEM-dist-2</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>THAAD-BN-01-FW</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>THAAD-BN01-HQ-RTR</td>
</tr>
</tbody>
</table>

### Paths Found
Path Discovered: 6 hops

<table>
<thead>
<tr>
<th>Hop</th>
<th>Flow</th>
<th>Element</th>
<th>Device</th>
<th>Type</th>
<th>First Line/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>IBCS-FW2</td>
<td>Inbound Filter</td>
<td>(config:58) access-list Outside-IN</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>IBCS-FW2</td>
<td>Inbound Filter</td>
<td>(config:59) access-list Outside-IN</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>IBCS-FW2</td>
<td>Inbound Filter</td>
<td>(config:60) access-list Outside-IN</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>IBCS-FW2</td>
<td>Inbound Filter</td>
<td>(config:61) access-list Outside-IN</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>IBCS-FW2</td>
<td>Inbound Filter</td>
<td>(config:65) access-list Outside-IN</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>IBCS-FW2</td>
<td>Inbound Filter</td>
<td>(implicit) deny all</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>THAAD-BN-01-FW</td>
<td>Inbound Filter</td>
<td>(config:80) access-list 12 deny ip 10.150.114.0 0.0.0.255 any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>THAAD-BN-01-FW</td>
<td>Inbound Filter</td>
<td>(config:81) access-list 12 permit ip any any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>THAAD-BN01-HQ-RTR</td>
<td>Outbound Filter</td>
<td>(implicit) deny all</td>
</tr>
</tbody>
</table>

### Access Through Path

<table>
<thead>
<tr>
<th>Access</th>
<th>Device</th>
<th>Interface</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port/Type</th>
<th>Destination IP</th>
<th>Destination Port/Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permitted Input</td>
<td>IBCS-FW2</td>
<td>172.16.156.1 (Ethernet0/0)</td>
<td>TCP, UDP</td>
<td>172.16.156.0</td>
<td>any</td>
<td>10.150.113.0 - 10.150.113.255</td>
<td>any</td>
</tr>
<tr>
<td>Permitted Output</td>
<td>THAAD-BN01-HQ-RTR</td>
<td>10.150.113.1 (Ethernet3)</td>
<td>TCP</td>
<td>172.16.156.0</td>
<td>any</td>
<td>10.150.113.50 - 10.150.113.55</td>
<td>135, 139, 445</td>
</tr>
</tbody>
</table>
Notify the Network Team

Network team dispatched to look for anomalous activity and to determine the cause of network segmentation failure
### Exposed Host Details

#### WinSrv-HQ-OPS-50

<table>
<thead>
<tr>
<th>Details</th>
<th>Interfaces</th>
<th>Applications</th>
<th>Vulnerabilities</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Interfaces</td>
<td>Applications</td>
<td>Vulnerabilities</td>
<td>History</td>
</tr>
</tbody>
</table>

#### Analysis Results
- **Exposure:** 0.99
- **Value:** 75
- **Number Of Services:** 5
- **Vulnerability Count:** 6
- **Risk:** 74
- **Downstream Risk:** 37
- **Combined Risk:** 111
- **Confidence:** 1

#### Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE References</th>
<th>OS/Appl...</th>
<th>Ports</th>
<th>Risk</th>
<th>Downstream Risk</th>
<th>Attack Depth</th>
<th>Severity</th>
<th>Impact</th>
<th>Exposed</th>
<th>Leapfrog</th>
</tr>
</thead>
<tbody>
<tr>
<td>94637 Nessus</td>
<td>CVE-2016-7249</td>
<td>SQL</td>
<td>1433</td>
<td>74</td>
<td>37</td>
<td>1</td>
<td>MEDIUM</td>
<td>ACI-</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>34477 Nessus</td>
<td>CVE-2008-4250</td>
<td>RPC</td>
<td>135</td>
<td>74</td>
<td>37</td>
<td>1</td>
<td>HIGH</td>
<td>ACIS</td>
<td>Network Leapfrog</td>
<td>Yes</td>
</tr>
<tr>
<td>102271 Nessus</td>
<td>CVE-2017-8516</td>
<td>SQL</td>
<td>1433</td>
<td>74</td>
<td>37</td>
<td>1</td>
<td>MEDIUM</td>
<td>-C--</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>42106 Nessus</td>
<td>CVE-2009-2526</td>
<td>SMB</td>
<td>139</td>
<td>74</td>
<td>37</td>
<td>1</td>
<td>HIGH</td>
<td>ACIS</td>
<td>Network Leapfrog</td>
<td>Yes</td>
</tr>
<tr>
<td>97737 Nessus</td>
<td>CVE-2017-0143</td>
<td>SMB</td>
<td>445</td>
<td>74</td>
<td>37</td>
<td>1</td>
<td>HIGH</td>
<td>ACI-</td>
<td>Network Leapfrog</td>
<td>Yes</td>
</tr>
<tr>
<td>42106 Nessus</td>
<td>CVE-2009-2526</td>
<td>SMB</td>
<td>445</td>
<td>74</td>
<td>37</td>
<td>1</td>
<td>HIGH</td>
<td>ACIS</td>
<td>Network Leapfrog</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Vulnerability data on exposed hosts

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE References</th>
<th>Description</th>
<th>Host Count</th>
<th>Total Vulnerabilities</th>
<th>Leapfrog</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>42106 Nessus</td>
<td>CVE-2009-2526</td>
<td>The remote Windows host c...</td>
<td>1</td>
<td>185</td>
<td>True</td>
<td>HIGH</td>
</tr>
<tr>
<td>34477 Nessus</td>
<td>CVE-2008-4250</td>
<td>The remote Windows host i...</td>
<td>1</td>
<td>111</td>
<td>True</td>
<td>HIGH</td>
</tr>
<tr>
<td>97737 Nessus</td>
<td>CVE-2017-0143</td>
<td>The remote Windows host i...</td>
<td>1</td>
<td>104</td>
<td>True</td>
<td>HIGH</td>
</tr>
<tr>
<td>58332 Nessus</td>
<td>CVE-2012-0002</td>
<td>An arbitrary remote code v...</td>
<td>6</td>
<td>54</td>
<td>True</td>
<td>HIGH</td>
</tr>
<tr>
<td>102271 Nessus</td>
<td>CVE-2017-8516</td>
<td>The remote Microsoft SQL S...</td>
<td>2</td>
<td>41</td>
<td>False</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>
Other hosts in exposed subnet

<table>
<thead>
<tr>
<th>Switch</th>
<th>Port</th>
<th>Mode</th>
<th>Peer</th>
<th>Peer IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>THAAD-BN01-HQ-113-sw1</td>
<td>GigabitEthernet0/1</td>
<td>Access</td>
<td>WinSrv-HQ-OPS-50</td>
<td>10.150.113.50</td>
</tr>
<tr>
<td>THAAD-BN01-HQ-113-sw1</td>
<td>GigabitEthernet0/2</td>
<td>Access</td>
<td>Win</td>
<td></td>
</tr>
<tr>
<td>THAAD-BN01-HQ-113-sw1</td>
<td>GigabitEthernet0/3</td>
<td>Access</td>
<td>Win</td>
<td></td>
</tr>
<tr>
<td>THAAD-BN01-HQ-113-sw1</td>
<td>GigabitEthernet0/4</td>
<td>Access</td>
<td>Win</td>
<td></td>
</tr>
<tr>
<td>THAAD-BN01-HQ-113-sw1</td>
<td>GigabitEthernet0/5</td>
<td>Access</td>
<td>Win</td>
<td></td>
</tr>
<tr>
<td>THAAD-BN01-HQ-113-sw1</td>
<td>GigabitEthernet0/6</td>
<td>Access</td>
<td>Win</td>
<td></td>
</tr>
</tbody>
</table>

Switch, port, and MAC address details
Deploy the Windows Forensics team

Windows forensics team sent to assess the exposed endpoints
Network Analysis Team Reports

The Network Analysis team confirmed that there has been network traffic to the identified system and that it is also sending large amounts of data externally.
Network Access from Host

Where can this host go if compromised?
What are the exfiltration paths?

External?

Internal?
The Windows Forensics team analyzed the system and confirmed that it was compromised. It has been confirmed that data was being sent externally, but internal communications with a system in MAINT OPS on port 1433 was also discovered.
Battery line operators are reporting their systems are suddenly rebooting continuously.
Threats from host

What vulnerabilities can be reached by this compromised host?
### Threats from Host Reveals Vulnerable SQL Application

#### WinSrv-Maint-OPS-70

<table>
<thead>
<tr>
<th>Details</th>
<th>Interfaces</th>
<th>Applications</th>
<th><strong>Vulnerabilities</strong></th>
<th>History</th>
</tr>
</thead>
</table>

#### 1 row

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE Reference</th>
<th>Host Name</th>
<th>IP</th>
<th>OS/Application</th>
<th>Ports</th>
<th>Risk</th>
<th>DoS</th>
<th>Att</th>
<th>T</th>
<th>...</th>
<th>...</th>
<th>...</th>
<th>...</th>
<th>...</th>
<th>...</th>
<th>2C</th>
<th>...</th>
<th>...</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>102271 N...</td>
<td>CVE-2017-8...</td>
<td>WinSrv-Maint-OPS-70</td>
<td>10.150.131.70</td>
<td>SQL</td>
<td>1433</td>
<td>37</td>
<td>0</td>
<td>2</td>
<td>C</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Access to Maint Ops

What can access Maintenance ops subnet?
Access from Maint

What can Maintenance ops Subnet access

THAAD-BN01-HQ

THAAD-BN01-MAINT

MAINT BLO2

10.150.133.0/24 (1 host)

MAINT OPS

10.150.131.0/24 (1 host)

10.150.132.0/24 (1 host)

WinSrv-HQ-OPS-50

WinSrv-Maint-OPS-70

0.150.113.0/24 (6 hosts)

80.1.1.0/24

70.1.1.0/24

172.16.10.0/24 172.16.11.0/24

GIG

GIG-BORDER-1 GIG-BORDER-2

HQ OPS

GIG-BORDER-3

172.16.12.0/24

THAAD-BN01-Maint-L3Switch

10.150.133.0/24 (1 host)
Problems Identified and correction put in place

- You’ve identified where to place TAP’s for hunting

- You’ve patched the HQ OPS and MAINT OPS hosts

- You’ve applied the ACL to the interfaces and stopped the RDP access from the GIG.
RADAR, TFCC, and LAUNCH are still rebooting for both battery lines.
Access & Threats To

Why da reboot sky?

What can access the Battery Lines subnets?

Are there any threat vectors?
Deploy the Windows Forensics team

Windows forensics team sent to assess the endpoints in Maintenance OPS subnet
RDP Session reported

Windows Forensics team reports on MAINT OPS. There was a desktop session and cached RDP sessions over to MAINT BL01 and MAINT BL02.
The attacker setup an MSF maxchannelids DoS script from MAINT BL01 and BL02 to attack all the Battery Line servers via an RDP related vulnerability.
Threats from host

What vulnerabilities can be reached by this compromised host?
Further investigation into MAINT OPS host turns out MSF was installed here under a hidden folder. An MSF session was identified minimized running the EsteemAudit exploit gaining shell prompt to both the MAINT BL01 & BL02 hosts.
Build Your Own War Room

- Integrate data silos
- Map hybrid networks
- Push vendor integration
- Become Digitally Resilient
Summary

- Target resilience, not flawless protection
- Network context is the foundation for resilience
- Improve productivity and resilience with strong integration:
  - Existing data sources
  - Virtual with physical
  - Vendors in your technology stack

RedSeal's network modeling and risk scoring platform enables enterprise networks to be resilient to cyber events and network interruptions in an increasingly digital and virtualized world.
Thank you.