Security Incident Discovery and Correlation on .Gov Networks

Cory Mazzola, MSIA, CISSP
US-CERT Surface Analysis Group

Timothy Tragesser
US-CERT Fusion Analysis & Development
Agenda

- Overview
- Data Collection
- Malware Activity Sets:
  - Beaconing
  - Redirection
  - Suspicious Activity
- Findings/Analysis
- Samples/Examples
- Recommendations
- Takeaways
Who we are...

- **US-CERT is the operational arm for cyber security under the Department of Homeland Security**
- **Analysis Branch uses flow data from Einstein sensors deployed across .gov networks**
Information Correlation...

Facilitating collective analysis of cyber threats through partnerships.
Threat Summary

- Security incidents reported to/by US-CERT since 1 January
  - ~108,000 total incidents reported YTD
  - 13,000 Malicious Code Incidents YTD
- Malicious Logic Incidents comprise primary focus area
Context

- **What we have:**
  - Repository of federal/state/local govt, private/foreign sector security incidents
    - ~108K so far this year

- **What we needed:**
  - Automated method to detect and identify security incidents/events using netflow

- **What we devised:**
  - Queries to mine database, correlate information and positively identify security incidents
Prep: Data Collection
Initial Data Pull/RW Binary Creator

- Creates bin file to prep and execute queries:

```bash
#!/bin/sh

perl -pi -e "s/\|\//\|/g" hosts.txt
perl -pi -e "s/\|\//\|/g" hosts.txt
perl -pi -e "s//\//g" hosts.txt

BINFILE=`date "+%Y-%m-%d-%T.bin"`

day=`date "+%a"

if [ "$day" = "Mon" ]; then
    STARTDATE=`date -d '-4 days' '+%Y/%m/%d'`
    ENDDATE=`date "+%Y/%m/%d"`
elif [ "$day" = "Sun" ]; then
    STARTDATE=`date -d '-7 days' '+%Y/%m/%d'`
    ENDDATE=`date "+%Y/%m/%d"`
elif [ "$day" = "Sat" ]; then
    STARTDATE=`date -d '-8 days' '+%Y/%m/%d'`
    ENDDATE=`date "+%Y/%m/%d"`
else
    STARTDATE=`date -d '-3 days' '+%Y/%m/%d'`
    ENDDATE=`date "+%Y/%m/%d"`
fi

if [ -f $BINFILE ]; then
    echo "$BINFILE already exists !!!"
    echo "Please insure rwprocessor.sh is not already running and then move or remove $BINFILE"
else
    if [ -f temphosts.txt ]; then
        rm -f temphosts.txt
    fi

    if [ -f temphosts.set ]; then
        rm -f temphosts.set
    fi
```
Initial data pull: RW Binary Creator

- Creates bin file to execute queries against (cont.)

```bash
for i in `cat hosts.txt | cut -d "|" -f1 | sort | uniq`
  do
    echo $i >> temphosts.txt
  done

rwsetbuild temphosts.txt temphosts.set
echo "Einstein query from $STARTDATE to $ENDDATE"
echo "Created $BINFILE"

rwfilter --anyset=temphosts.set --type=all --start-date=$STARTDATE --end-date=$ENDDATE --pass=$BINFILE &
  if [-f temphosts.txt ];
  then
    rm -f temphosts.txt
  fi

  if [-f temphosts.set ];
  then
    rm -f temphosts.set
  fi
Fi
```
Malware Activity Patterns

- **Main Focus Areas:**
  - Beaconing
  - Redirect
  - Suspicious
Beaconing

- Goal is to detect and identify beaconing activity to/from constituent systems
  - Regular and irregular patterns
  - High and low volume connections
  - Known malicious IPs/domains
  - Investigate to identify data exfiltration / low-and-slow actions

- Triggers when victim IP address sends requests on the same dest port with a consistent packet size and at a specific time interval or pattern (i.e., 60 secs., 60 mins., etc.)

- Beaconing is a symptom
Beaconing

- **Personal favorite**
- ‘Quick and easy’ to vet true positives
- Good indicator of compromise/infection

Sample Output (beaconing occurring at 1 hour / 10 minute intervals):

<table>
<thead>
<tr>
<th>sTime</th>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>bytes</th>
<th>sensor</th>
<th>InitFlag</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010/10/04T13:06:38</td>
<td>199.9.9.9</td>
<td>195.161.112.6</td>
<td>1315</td>
<td>80</td>
<td>1623</td>
<td>USGA</td>
<td>S</td>
</tr>
<tr>
<td>2010/10/04T14:16:40</td>
<td>199.9.9.9</td>
<td>195.161.112.6</td>
<td>1366</td>
<td>80</td>
<td>1623</td>
<td>USGA</td>
<td>S</td>
</tr>
<tr>
<td>2010/10/04T15:26:42</td>
<td>199.9.9.9</td>
<td>195.161.112.6</td>
<td>1418</td>
<td>80</td>
<td>1623</td>
<td>USGA</td>
<td>S</td>
</tr>
<tr>
<td>2010/10/04T16:36:44</td>
<td>199.9.9.9</td>
<td>195.161.112.6</td>
<td>1515</td>
<td>80</td>
<td>1623</td>
<td>USGA</td>
<td>S</td>
</tr>
<tr>
<td>2010/10/04T17:46:45</td>
<td>199.9.9.9</td>
<td>195.161.112.6</td>
<td>1600</td>
<td>80</td>
<td>1623</td>
<td>USGA</td>
<td>S</td>
</tr>
<tr>
<td>2010/10/04T18:56:48</td>
<td>199.9.9.9</td>
<td>195.161.112.6</td>
<td>1721</td>
<td>80</td>
<td>1623</td>
<td>USGA</td>
<td>S</td>
</tr>
</tbody>
</table>
Beaconing Script

- The beaconing script uses several commands, as sampled below, to filter by flows for indications of hourly/daily/weekly beaconing activity:

```bash
for bytes in `rwfilter --saddress=$victimip --daddress=$badip --type=all bin/$i.bin --pass=stdout | rwuniq --fi=bytes --flows=5 --no-titles --no-final-delimiter --no-columns | cut -d "|" -f1`
do
daycount=`rwfilter bin/$i.bin --type=all --saddress=$victimip --daddress=$badip --bytes=$bytes --pass=stdout | rwcut --fi=9 --no-titles | cut -d "/" -f3 | cut -d "T" -f1 | sort -u | wc -l`
```
Findings Analysis: Beaconing

- Using seconds/milliseconds to build timeline
  - Helps dispel irregularities
  - Common traffic obfuscation technique for FakeAV and Rootkits

Sample Output (note the second count):

<table>
<thead>
<tr>
<th>sTime</th>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>bytes</th>
<th>sensor</th>
<th>initialF</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010/08/17T11:25</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>1529</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/17T14:21</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>1989</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/17T21:26</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>2346</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/17T22:32</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>2602</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/18T02:09</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>3103</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/18T05:43</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>3607</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/18T14:10</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>3996</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/18T16:18</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>4295</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/18T18:51</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>4640</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/19T05:22</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>1229</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/19T09:56</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>1341</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/19T15:42</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>1806</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/20T06:24</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>2186</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/20T09:37</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>2321</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/20T12:04</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>2871</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/21T15:22</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>3439</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
<tr>
<td>2010/08/21T17:34</td>
<td>199.9.9.9</td>
<td>94.228.209.200</td>
<td>3532</td>
<td>80</td>
<td>549</td>
<td>USGA1</td>
<td>S</td>
<td>1</td>
</tr>
</tbody>
</table>
Findings Analysis: Beaconing

- Graphical Representation
  - Easy-to-read synopsis of activity
  - Helpful handout/reference for constituency

- Victim IP observed beaconing every 8 minutes and 55 seconds
Beaconing Script: Excel Charting

Beaconing excel macro is used to give pattern charts:

```
Sub Patterns()
    ' Patterns Macro
    ' Macro recorded 12/3/2010 by ttragess
    ' Keyboard Shortcut: Ctrl+Shift+T
    Columns("B:B").Select
    Selection.Insert Shift:=xlToLeft
    Columns("B:B").Select
    Selection.Insert Shift:=xlToLeft
    Columns("A:A").Select
    'Range("A549").Activate
    Selection.TextToColumns Destination:=Range("A1"), DataType:=xlDelimited, _
        TextQualifier:=xlDoubleQuote, ConsecutiveDelimiter:=False, Tab:=False, _
        Semicolon:=False, Comma:=False, Space:=False, Other:=True, OtherChar _
            :="\", FieldInfo:=Array(1, 1), TrailingMinusNumbers:=True
    Columns("A:A").EntireColumn.AutoFit
    Columns("A:A").Select
    Selection.TextToColumns Destination:=Range("A1"), DataType:=xlFixedWidth, _
        OtherChar:="\", FieldInfo:=Array(Array(0, 1), Array(10, 1), Array(11, 1)), _
        TrailingMinusNumbers:=True

    totalrows = ActiveSheet.UsedRange.Rows.Count
totalrows = Int(totalrows) beginRange = 1 loopcount = 1

    For i = 1 To totalrows
        Range("A" & i).End(xlDown).Select
        ' patterns Macro
        ' Macro recorded 11/26/2010 by ttragess
        ' Test contents of active cell; if active cell is empty, exit loop.
        Do Until IsEmpty(ActiveCell)
```

Homeland Security
Beaconing: Excel Charting (cont.)

```
ActiveCell.Offset(1, 0).Select
endRange = ActiveCell.Address(False, False)
' myCell = ActiveCell.AddressLocal

    endRange = Right(endRange, Len(endRange) - 1)

    If loopcount = 1 Then
        beginRange = 1
    Else
        beginRange = i - 1
    End If
    loopcount = loopcount + 1
End Sub
```

```vbnet
Charts.Add
ActiveChart.ChartType = xlColumnClustered
ActiveChart.SetSourceData Source:=Sheets("Sheet2").Range("G" & beginRange)
ActiveChart.SeriesCollection.NewSeries

ActiveChart.SeriesCollection(1).XValues = ":Sheet2!R & beginRange & "C1:R" & endRange & "C1"
ActiveChart.SeriesCollection(1).Values = ":Sheet2!R & beginRange & "C3:R" & endRange & "C3"

ActiveChart.Location Where:=xlLocationAsObject, Name:="Sheet2"
With ActiveChart
    .HasAxis(xlCategory, xlPrimary) = True
    .HasAxis(xlValue, xlPrimary) = True
    .HasTitle = True
    .ChartTitle.Characters.Text = goodguy & " beaconing to " & badguy & " with a byte count of " & bytecount
End With
```

Next
End Sub
Redirect Activity

- **Victim IP Address communicates with first mal IP/domain and is immediately redirected to a secondary mal IP/domain**

- Identifies malicious and anomalous activity
  - Tracks connections/patterns to IPs/domains of interest
  - Correlates activity with incident database information
  - Can help to:
    - Identify post infection beaconing such as pattern is seen every half hour before victim tries again.
    - Identify new types of malicious activity or malware based off of pattern recognition from the victim IP
      - First and last/size of bytes downloaded from each
    - Provide more than two attacker sessions and identify malicious traffic such as Gumblar
Redirect Campaigns

Gumblar

Compromised Site

Exploit Site

Beladen

Compromised Site

Redirection Host

Exploit Site

Nine-Ball

Compromised Site

If host system has not previously been infected in Nine-Ball attack

Redirection Host

Redirection Hosts

Exploit Site

If host system has previously been infected in Nine-Ball attack

Ask.com
Redirect Criteria

- Victim initiates connection to first malicious IP address and then within milliseconds initiates connection to second malicious IP address. The victim then does the same activity 30 minutes later in a dual initiate connection to the malware IP address set.

  - VICTIM ---------> MAL1
  - MAL1 ---------> VICTIM
  - VICTIM ---------> MAL2
  - MAL2 ----------> VICTIM

  - VICTIM WAITS 30 MINUTES TO INITIATE NEXT SESSION
  - VICTIM ---------> MAL1
  - MAL1 ----------> VICTIM
  - VICTIM ---------> MAL2
  - MAL2 ----------> VICTIM

- Alternate criteria:
  - Victim IP contacts several IP addresses/domains in sequence (and repeats activity). Examples include Gumblar or other fast flux activity.
The snippet below creates the coupling between the victim and attacker IPs. Many more lines are used to accurately focus on back and forth communications, however this is the basis for pairing the attacker/victim:

```bash
# Check to make sure there was a ip.set for the pair of malicious IP addresses if so pull victim IP addresses and add then to one set.
if [-f $i.outweb.set ] || [-f ${ip[$p]}.outweb.set ]; then
  rwsetintersect --add-set=$i.outweb.set --add-set=${ip[$p]}.outweb.set --set=bothout.set if [-f bothout.set ]; then
# Create the the flow data for the pair of malicious IP addresses.
# from from the small binary files and place the results in a base.bin # Using the ip.set query of base.bin and place results in intersected.bin

  rwappend --create base.bin bin/$i.bin bin/${ip[$p]}.bin
  rwfilter --anyset=bothout.set base.bin --pass=Intersected.bin
  count=`rwfilter Intersected.bin --type=outweb --pass=stdout | rwsort --fi=22 | rwcut --fi=1-12,26 | grep -A 1 $i | grep -B 1 ${ip[$p]} | wc -l`
```

```bash
```
Findings Analysis: Redirect

- **Sample Output**
  - Quick second/millisecond session redirects
  - Detected recent gbot activity w/ 2k+ infections

<table>
<thead>
<tr>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>packets</th>
<th>bytes</th>
<th>flags</th>
<th>sTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>attacker IP1</td>
<td>victim</td>
<td>80</td>
<td>1514</td>
<td>5</td>
<td>629</td>
<td>FS PA</td>
<td>2010/10/27 14:58:03.219</td>
</tr>
<tr>
<td>attacker IP1</td>
<td>victim</td>
<td>80</td>
<td>1519</td>
<td>5</td>
<td>629</td>
<td>FS PA</td>
<td>2010/10/27 14:58:05.072</td>
</tr>
<tr>
<td>attacker IP2</td>
<td>victim</td>
<td>80</td>
<td>1515</td>
<td>4</td>
<td>589</td>
<td>FS PA</td>
<td>2010/10/27 14:58:07.243</td>
</tr>
<tr>
<td>attacker IP2</td>
<td>victim</td>
<td>80</td>
<td>1515</td>
<td>1</td>
<td>40</td>
<td>A</td>
<td>2010/10/27 14:58:07.418</td>
</tr>
<tr>
<td>victim</td>
<td>attacker IP</td>
<td>1514</td>
<td>80</td>
<td>5</td>
<td>470</td>
<td>FS PA</td>
<td>2010/10/27 14:58:08.174</td>
</tr>
<tr>
<td>victim</td>
<td>attacker IP</td>
<td>1519</td>
<td>80</td>
<td>6</td>
<td>517</td>
<td>FS PA</td>
<td>2010/10/27 14:58:08.026</td>
</tr>
<tr>
<td>victim</td>
<td>attacker IP</td>
<td>1515</td>
<td>80</td>
<td>8</td>
<td>602</td>
<td>FSRPA</td>
<td>2010/10/27 14:58:11.159</td>
</tr>
<tr>
<td>victim</td>
<td>attacker IP</td>
<td>1515</td>
<td>80</td>
<td>1</td>
<td>40</td>
<td>R A</td>
<td>2010/10/27 14:58:14.418</td>
</tr>
</tbody>
</table>
Suspicious

- Seeking to detect and identify ‘suspicious activity’ and outliers
  - Communicating with known mal IPs
  - Pattern matching/identification
  - Conjecture

- The query covers activity that may not be caught elsewhere
  - Low and Slow beaconing that may not be caught
  - High port to high port activity
  - Rootkit type activity with unique instructional patterns
Data Exfil Criteria

- Beaconing can potentially become data exfiltration when:
  - The victim IP address downloads a percentage of total packets exchanged (at least with web traffic).

Noted false positives when the victim is a web server and normal web traffic exceeds downloaded data of 70-90% and uploads of 10-30%
Suspicious Script/Code

- The suspicious script gets all possible victim IP addresses and then prints out traffic based on time (what the communication looked like back and forth) to help determine suspicious patterns. Simply put it is a straight rwcut filtered on time.

```
for j in `rwfilter bin/$IP.bin --type=all --pass=stdout | rwuniq --fi=1 --no-titles --no-columns | grep -v $IP | cut -d "|" --fi=1 | sort -u`
do
    sensor=`rwfilter bin/$IP.bin --any-address=$j --pass=stdout | rwcut --fi=12 --no-titles --no-columns --no-final-delimiter | head -1`
sensor=`grep -w $sensor ../sensor.txt | head -1 | cut -d "|" -f2`
```
Findings Analysis: Suspicious

- Heuristic detection techniques
- Rarely detects FakeAV

*Example Output:* **Victim IP uploaded 21360 bytes and downloaded 8142 bytes to malicious IP Address:**

<table>
<thead>
<tr>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>protocol</th>
<th>packets</th>
<th>bytes</th>
<th>flags</th>
<th>sTime</th>
<th>dur</th>
<th>eTime</th>
<th>sensor</th>
<th>initialF</th>
</tr>
</thead>
<tbody>
<tr>
<td>victim</td>
<td>attacker</td>
<td>41745</td>
<td>80</td>
<td>6</td>
<td>288</td>
<td>S</td>
<td>2010/12/06T15:58:35.282</td>
<td>92.985</td>
<td>2010/12/06T16:00:08.267</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>victim</td>
<td>attacker</td>
<td>38283</td>
<td>80</td>
<td>6</td>
<td>288</td>
<td>S</td>
<td>2010/12/06T15:58:47.025</td>
<td>92.985</td>
<td>2010/12/06T16:00:20.010</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>victim</td>
<td>attacker</td>
<td>23620</td>
<td>80</td>
<td>6</td>
<td>288</td>
<td>S</td>
<td>2010/12/06T15:59:02.375</td>
<td>92.982</td>
<td>2010/12/06T16:00:35.357</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>victim</td>
<td>attacker</td>
<td>22906</td>
<td>80</td>
<td>6</td>
<td>288</td>
<td>S</td>
<td>2010/12/06T15:59:26.089</td>
<td>92.984</td>
<td>2010/12/06T16:00:59.073</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>victim</td>
<td>attacker</td>
<td>48356</td>
<td>80</td>
<td>6</td>
<td>288</td>
<td>S</td>
<td>2010/12/06T16:00:05.258</td>
<td>92.984</td>
<td>2010/12/06T16:01:38.242</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>victim</td>
<td>attacker</td>
<td>24169</td>
<td>80</td>
<td>6</td>
<td>288</td>
<td>S</td>
<td>2010/12/06T16:24:20.051</td>
<td>92.984</td>
<td>2010/12/06T16:25:53.035</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Requirements

- Commodity hardware and available storage capacity
- In-house development capability to create/tune/maintain scripts
  - Update scripts based on new patterns and emerging threats
- Process to coordinate actions/activities
  - Standardization/certification of analytical process and background
- Manpower to verify and/or vet findings for accuracy and action
Recommendations

- **Provide user-friendly portal/system to process findings**
  - Hierarchical view for different users
    - Incident summary or overview for management
      - Paraphrase activity and provide easy-to-understand format
      - HTML and Executive Summary reports
      - The report script is approximately 2500 lines of shell script and analyzes different parts of the above logs to give initial findings.
    - Detailed view explaining specific query findings (e.g., beaconing, suspicious, etc.)
  - Detailed technical specifics for findings and incidents
    - Incident findings
    - Department impacted
    - Associated activity

- **Provide automated methods and templates for processing**
  - Vehicle and report template to disseminate validated findings
    - i.e.- “Notify Accounting of virus identified on IP 1.1.1.1”
Recommendations (cont.)

- Standardize incident criteria, taxonomy, templates
- Normalize incident handling/analysis processes
- Standardize product and include incident information
  - Network Flow data
    - Usual Stuff: Src/Dest IPs/Ports/Proto/Bytes/Time/etc.
  - IP correlation / analyst notes / database entries
  - Include references (proprietary, open source, etc.)
- Trust but Verify
  - Ensure automated findings are checked for accuracy and properly vetted prior to dissemination, formal reporting and/or follow-up action
Considerations

- **Integrate into operations**
  - Ensure capability is properly integrated into operations commensurate with organizations priority and operational necessity

- **Maintenance and Functionality**
  - Be able to allocate support levels to add/modify as necessary

- **Eyes-on analysis/vetting**
  - What person/department and what level of granularity
Benefits

• Discover and detect security events and malicious activity
  • Predicated on flow data
  • Expand incident discovery/detection capabilities
  • Timely and effective reporting of security incidents
  • Enables mitigation and remediation of findings
  • Scalable and especially useful for large/compartmented enterprises

• Automated query process
  • 2-click vetting and approval process optimal (depending)
Takeaways

• Harness flow data to identify security events and incidents of interest across the enterprise

• Develop automated queries to do work for you and vet results for accuracy
  • Tune appropriately

• Layered view to provide a user friendly view of information and data pertinent to different levels of org.
  • Customize different views across organization:
    • Leadership / Security Operations
    • Technicians / Responders
    • Constituents (if desired)
Contact

- **US-CERT**
  - US-CERT Security Operations Center
    Email: soc@us-cert.gov
    Phone: +1 888-282-0870
  - US-CERT Information Request
    Email: info@us-cert.gov
    Phone: +1 888-282-0870
  - GFIRST: gfirst@us-cert.gov

- Information available at http://www.us-cert.gov
Questions?