Fight the Network

Presented By Kevin Jacobs
On Behalf of WIN-T TMD and
CERDEC S&TCD CyberOps Branches
kevinj@netwerxinc.com

ARMY TEAM C4ISR

from concept to combat

Problem

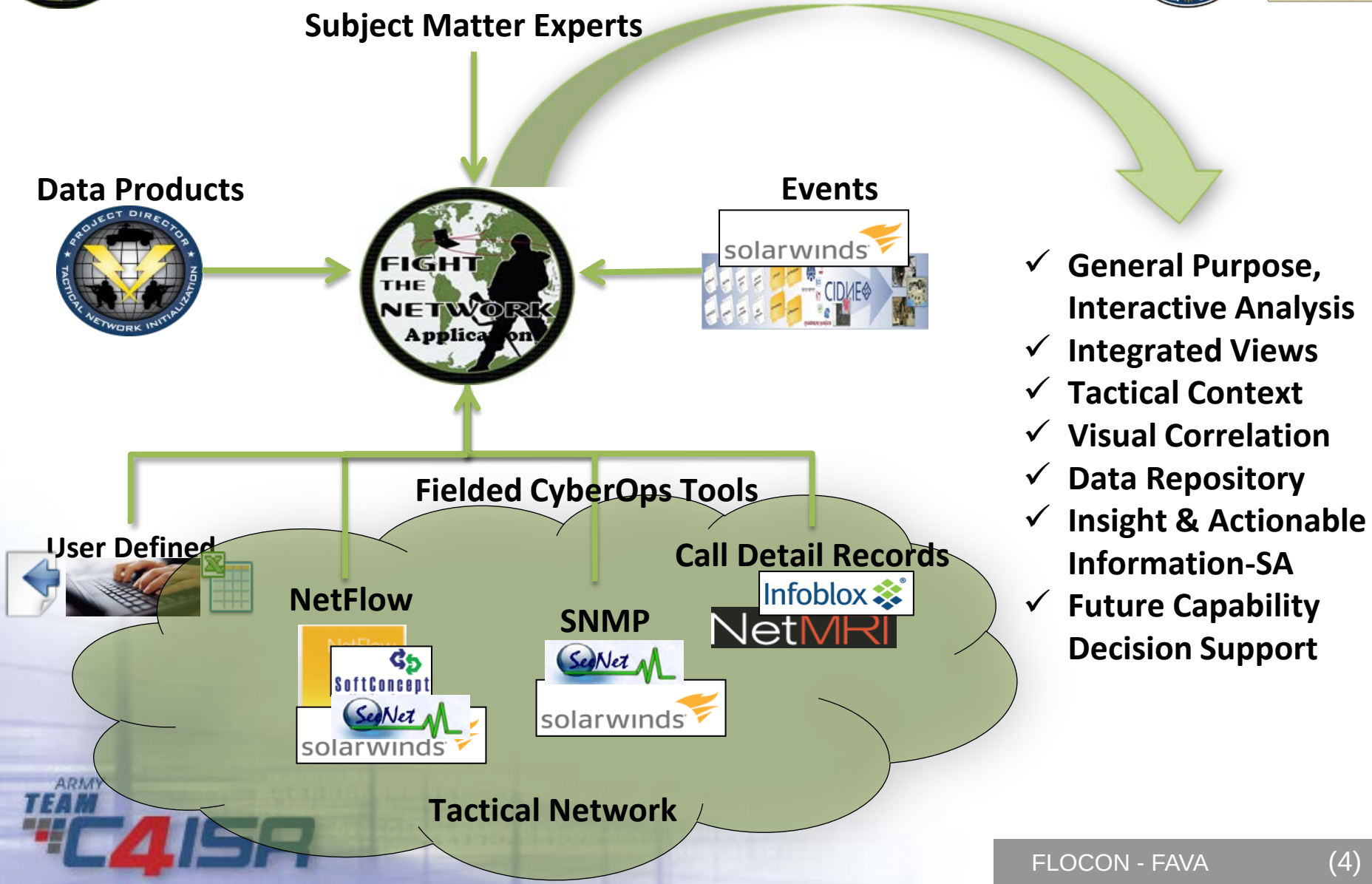
- Army Strategy for Net-Centric Fighting Force - Leverage & Integrate COTS technology innovations
- Currently Deployed Commercial CyberOps Capabilities:
  - Lack Tactical Network Design Context
  - Require Large Investment to Customize
  - Treat Data as Perishable
  - Stove Pipe Design - Lack the Big Picture Perspective
  - Will have an enduring presence in the Army inventory

FTN Goals

Maximize Utility of the Current Force CyberOps Solutions

- Configure to fully leverage individual CyberOps system capabilities
- Harvest and utilize data to
  - Enhance warfighter's Cyber Operations Situational Awareness
  - Provide decision support analysis to the C4ISR community
- Integrate data from across stove-pipe CyberOps systems to provide information and knowledge not provided by individual CyberOps systems/data
- Add Army Echelon, Tactical Network, and Mission Command Context
- The FTN Analysis And Visualization Application (FAVA) is the fusion point.

FTN Operational View

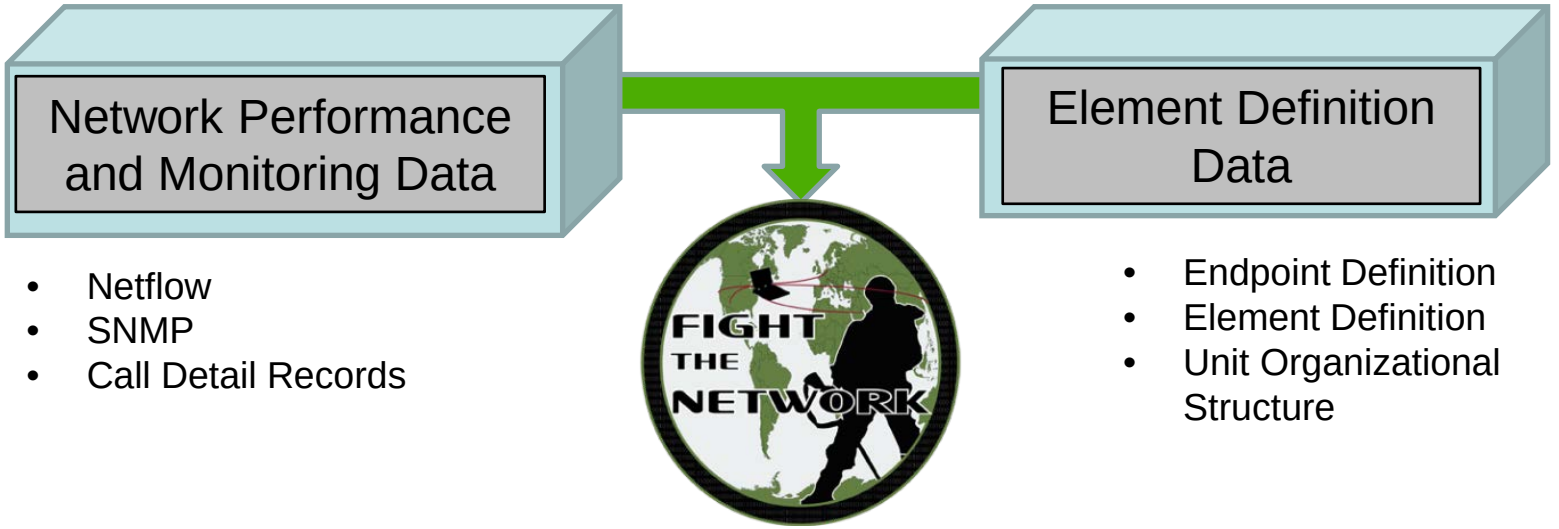


- ✓ General Purpose, Interactive Analysis
- ✓ Integrated Views
- ✓ Tactical Context
- ✓ Visual Correlation
- ✓ Data Repository
- ✓ Insight & Actionable Information-SA
- ✓ Future Capability Decision Support

Task Details

- **Combat Training Center (CTC) Support**
  - National Training Center (NTC)
    - Design and implement custom network instrumentation and configure CyberOps suite
    - Collect and analyze data during unit (BCT) training exercises
    - Provide training center and unit leadership insight into network performance and configuration issues
    - Assisting in troubleshooting
    - Harvest and store data for future analysis
  - Joint Readiness Training Center (JRTC) coming soon
- **Overseas Contingency Operations (OCO)**
  - Collect and analyze data for units in theater
  - Help units establish network operations center (NOC)
  - Help units streamline network operations and maximize efficiency
  - On as-needed/requested basis

FTN Data Fusion

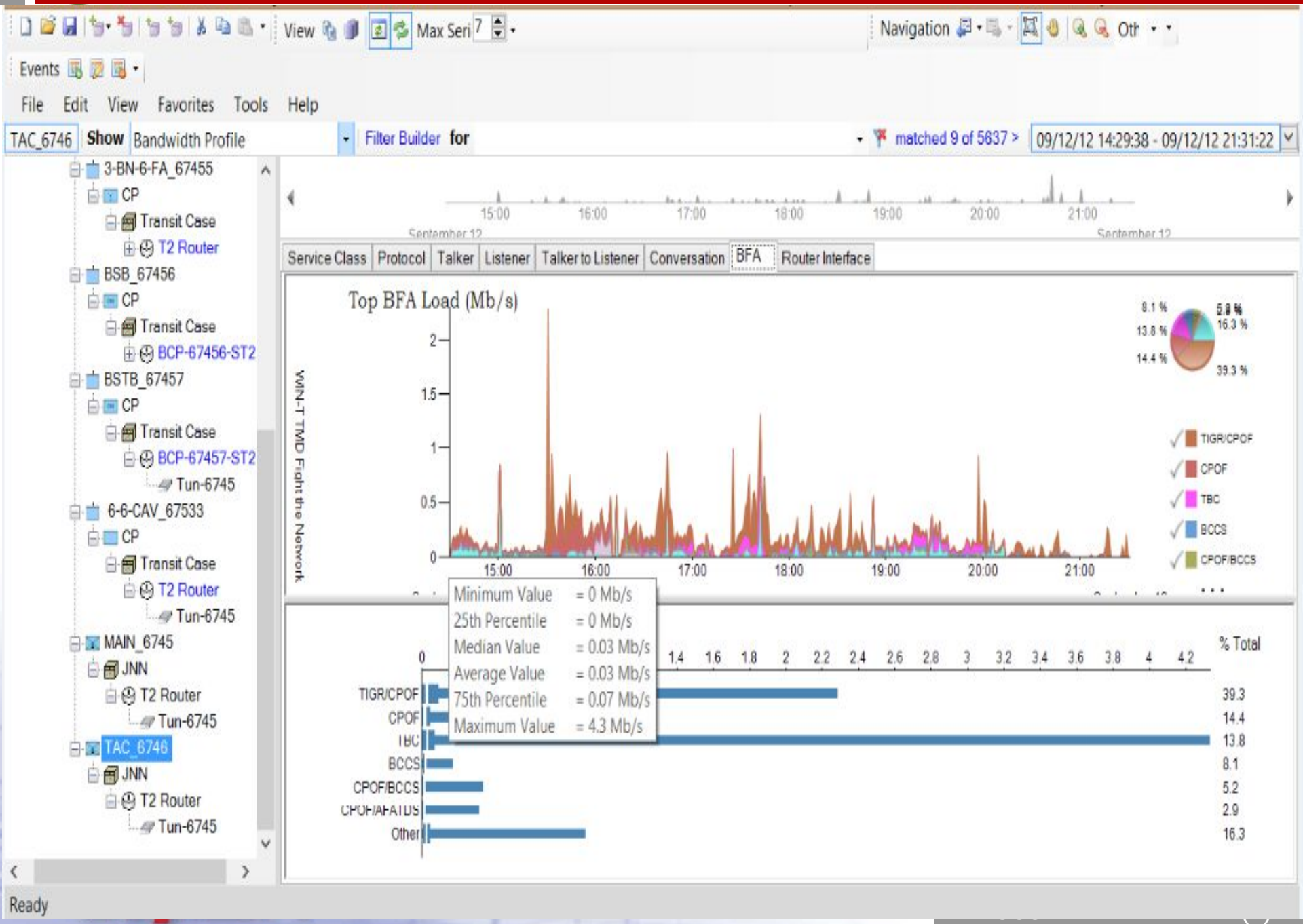


- Netflow
- SNMP
- Call Detail Records

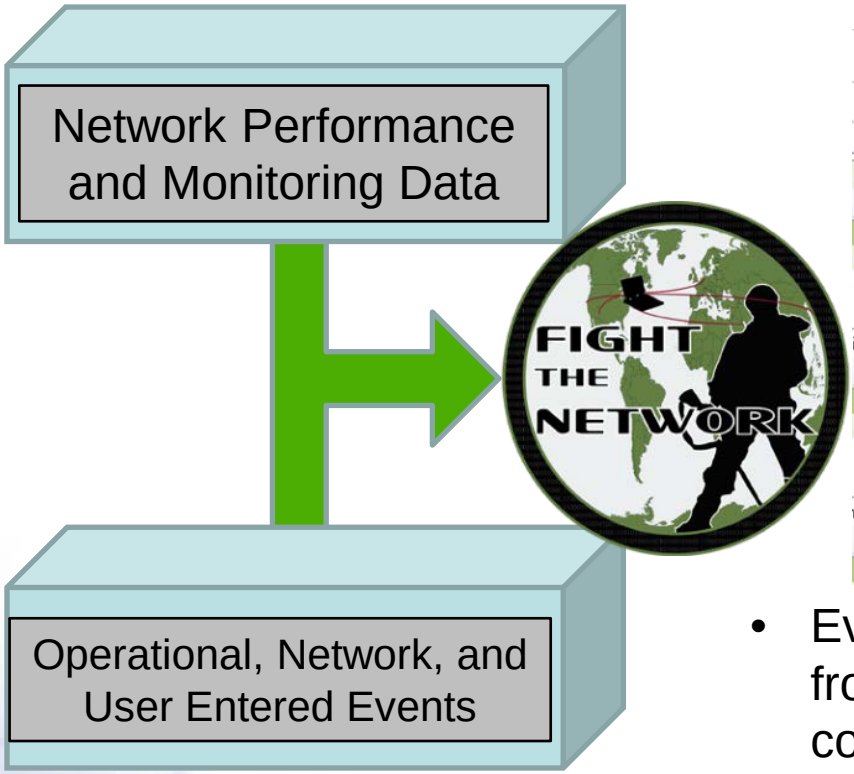
- Endpoint Definition
- Element Definition
- Unit Organizational Structure

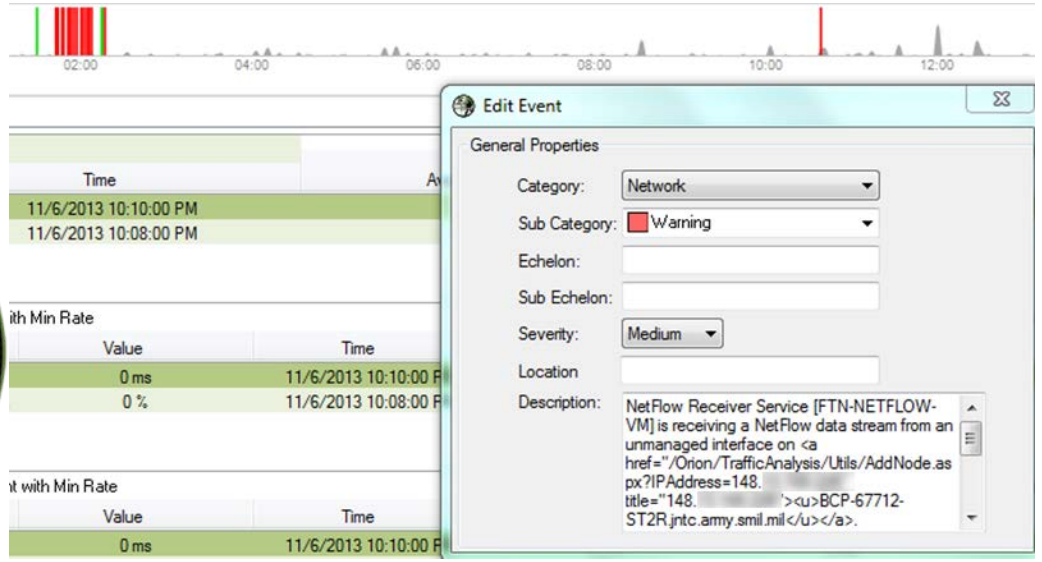
By incorporating key components of these different data sets,

- Present a unit hierarchy
- Filter at a very granular / specific level
- Analyze a specific network node/Echelon or group of nodes/Echelons
- Analyze data between nodes/Echelons
- Pinpoint problem nodes to isolate and resolve network problems
- Isolate and analyze activity at endpoints
- Track activity type (talker / listener) and endpoint type (client / server)

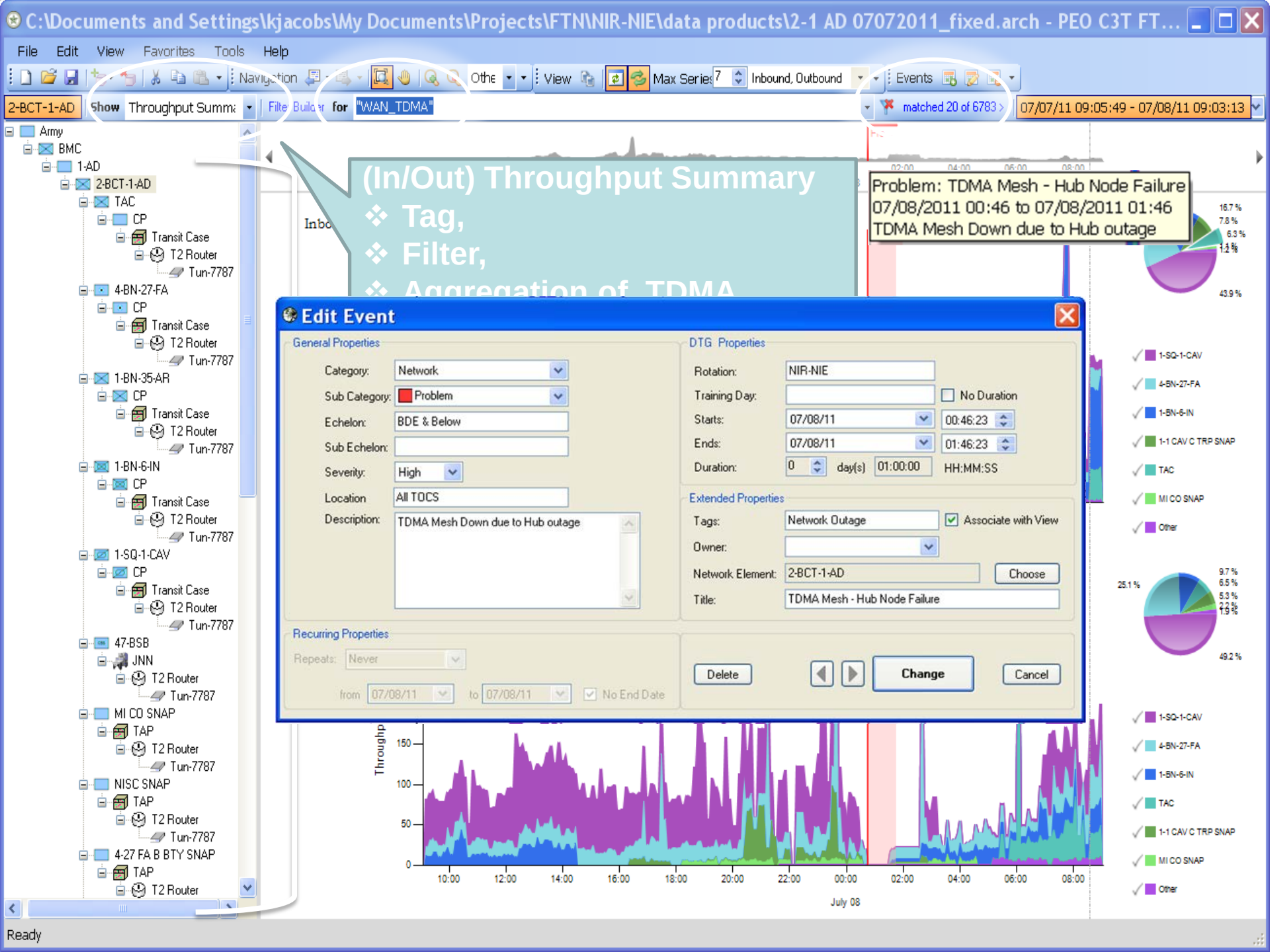

View
Max Seri 7
Navigation
Events
File Edit View Favorites Tools Help
TAC_6746 Show Bandwidth Profile
Filter Builder for
matched 9 of 5637 >
09/12/12 14:29:38 - 09/12/12 21:31:22
3-BN-6-FA_67455
CP
Transit Case
T2 Router
BSB_67456
CP
Transit Case
BCP-67456-ST2
BSTB_67457
CP
Transit Case
BCP-67457-ST2
Tun-6745
6-6-CAV_67533
CP
Transit Case
T2 Router
Tun-6745
MAIN_6745
JNN
T2 Router
Tun-6745
TAC_6746
JNN
T2 Router
Tun-6745
15:00 16:00 17:00 18:00 19:00 20:00 21:00
September 12
Service Class Protocol Talker Listener Talker to Listener Conversation BFA Router Interface
Top BFA Load (Mb/s)
WIN-T TMD Fight the Network
2 1.5 1 0.5 0
15:00 16:00 17:00 18:00 19:00 20:00 21:00
8.1 %
13.8 %
14.4 %
16.3 %
39.3 %
TIGR/CPOF
CPOF
TBC
BCCS
CPOF/BCCS
Minimum Value = 0 Mb/s
25th Percentile = 0 Mb/s
Median Value = 0.03 Mb/s
Average Value = 0.03 Mb/s
75th Percentile = 0.07 Mb/s
Maximum Value = 4.3 Mb/s
0 1.4 1.6 1.8 2 2.2 2.4 2.6 2.8 3 3.2 3.4 3.6 3.8 4 4.2
% Total
TIGR/CPOF 39.3
CPOF 14.4
TBC 13.8
BCCS 8.1
CPOF/BCCS 5.2
2.9
Other 16.3
Ready

Network Performance and Event Correlation

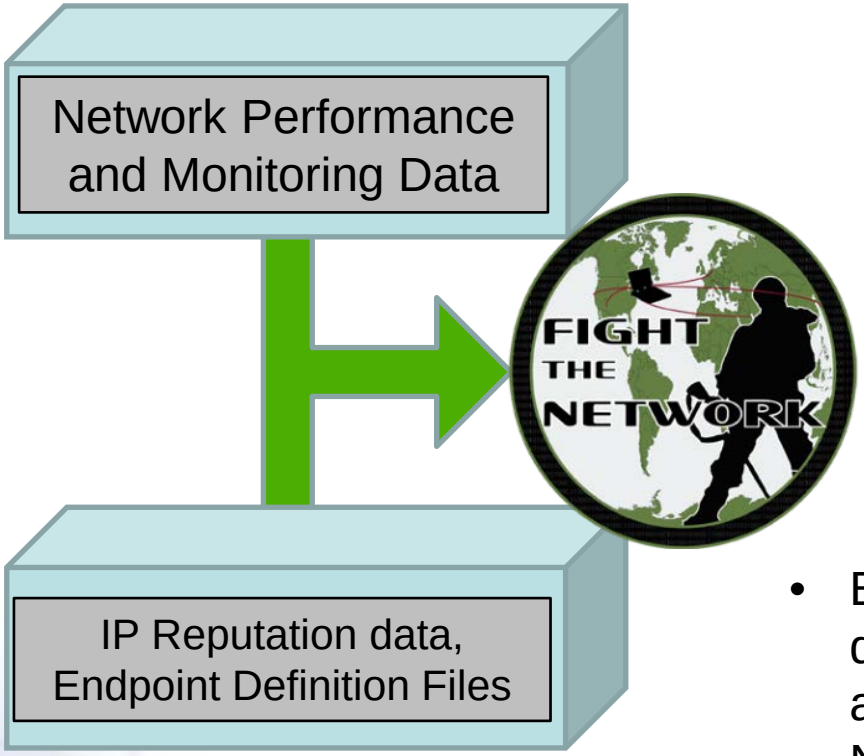




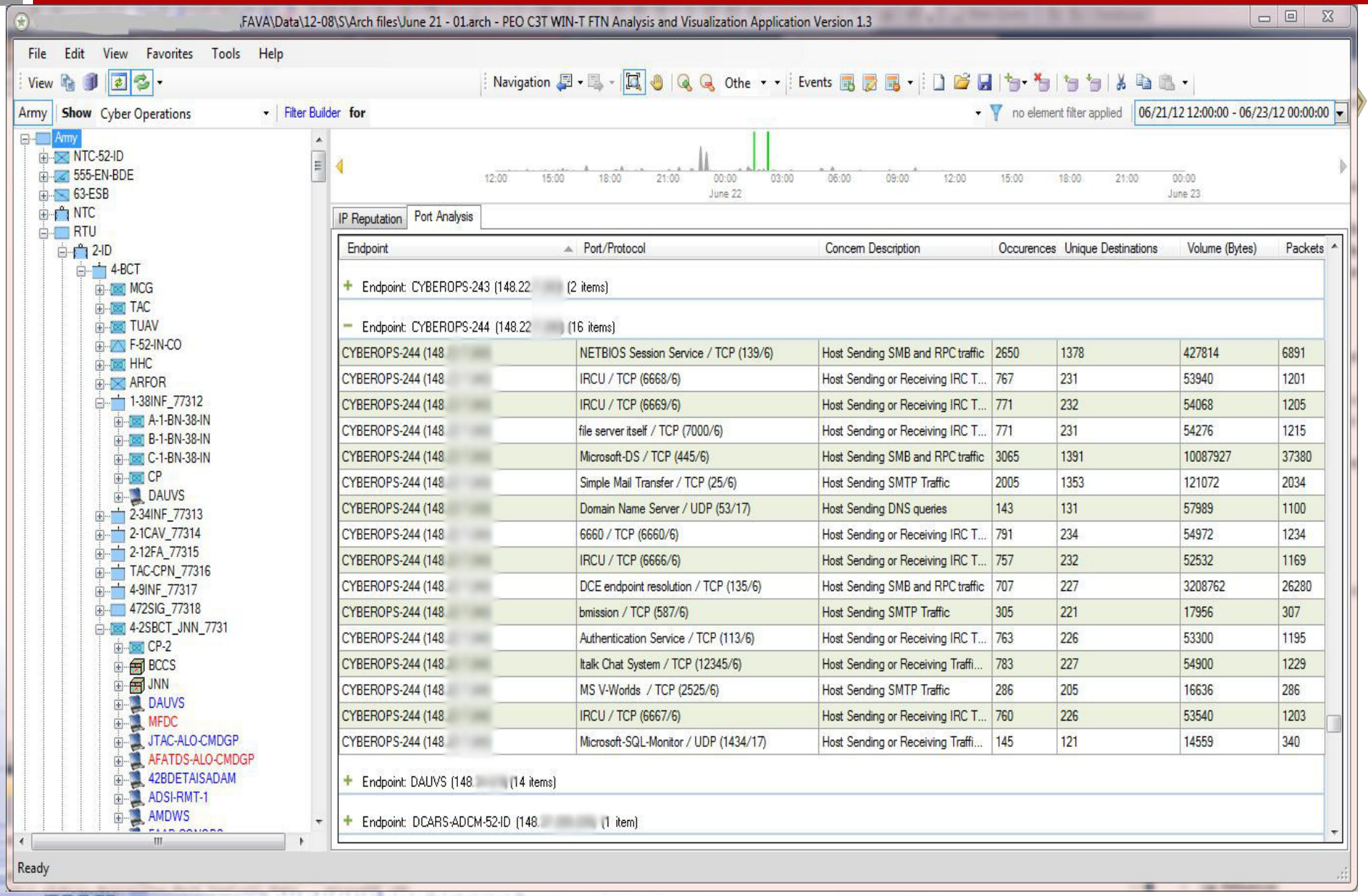
- Event data can be entered by the user, loaded from available event files, or extracted from the collector.
- On a timeline, this can effectively show cause-effect relationships between events and network behavior. (e.g. failures, network activity spike on a node correspond with mission execution, etc.)

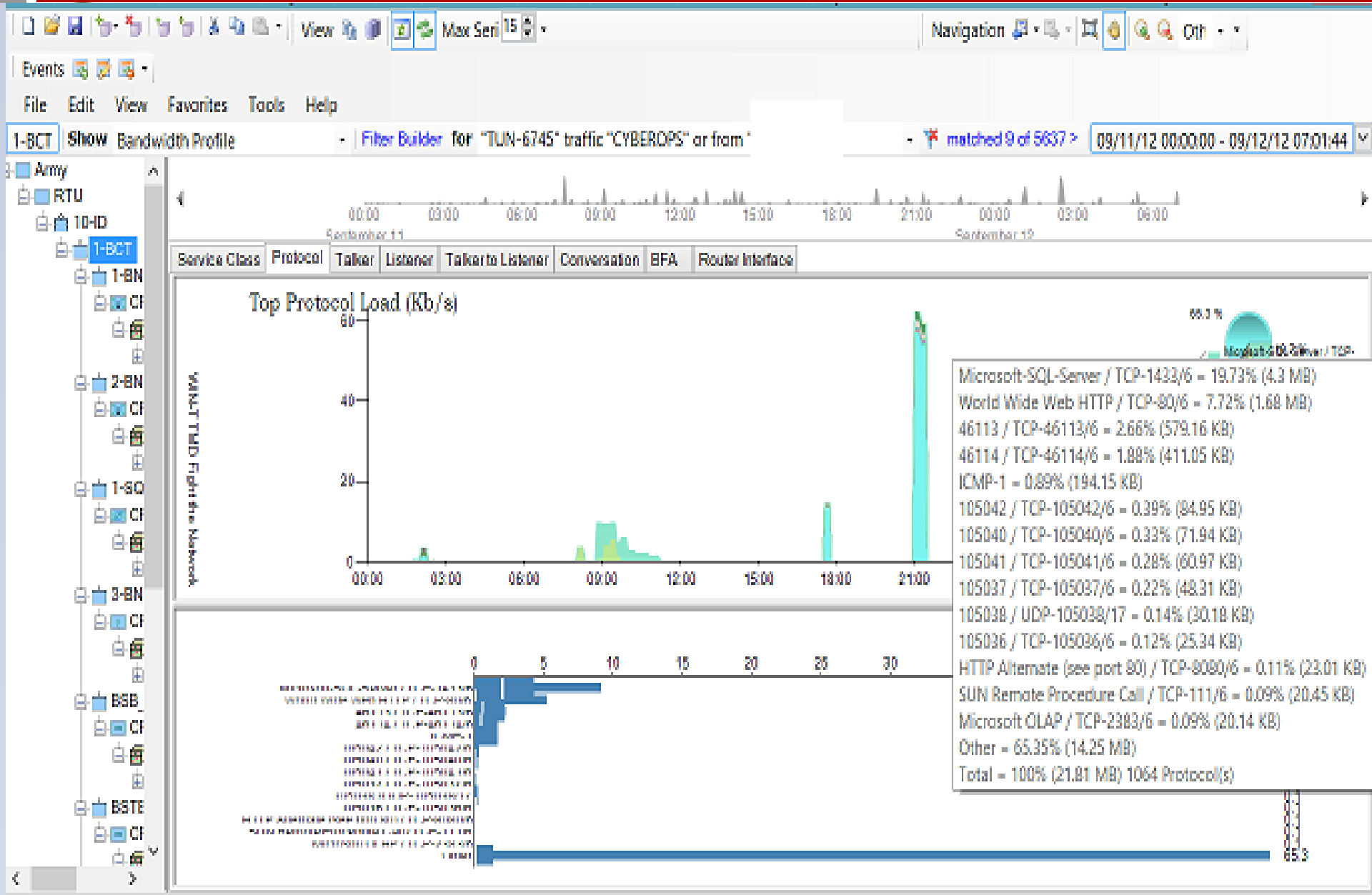

C:\Documents and Settings\kjacobs\My Documents\Projects\FTN\NIR-NIE\data products\2-1 AD 07072011_fixed.arch - PEO C3T FT...
File Edit View Favorites Tools Help
2-BCT-1-AD
Show Throughput Summa
Filter Builder for "WAN_TDMA"
matched 20 of 6783
07/07/11 09:05:49 - 07/08/11 09:03:13
(In/Out) Throughput Summary
Tag,
Filter,
Problem: TDMA Mesh - Hub Node Failure
07/08/2011 00:46 to 07/08/2011 01:46
TDMA Mesh Down due to Hub outage
Edit Event
General Properties
Category: Network
Sub Category: Problem
Echelon: BDE & Below
Sub Echelon:
Severity: High
Location All TOCS
Description: TDMA Mesh Down due to Hub outage
DTG Properties
Rotation: NIR-NIE
Training Day:
No Duration
Starts: 07/08/11 00:46:23
Ends: 07/08/11 01:46:23
Duration: 0 day(s) 01:00:00 HH:MM:SS
Extended Properties
Tags: Network Outage
Associate with View
Owner:
Network Element: 2-BCT-1-AD
Choose
Title: TDMA Mesh - Hub Node Failure
Recurring Properties
Repeats: Never
from 07/08/11 to 07/08/11 No End Date
Delete
Change
Cancel
Army
BMC
1-AD
2-BCT-1-AD
TAC
CP
Transit Case
T2 Router
Tun-7787
4-BN-27-FA
1-BN-35-AR
1-BN-6-IN
1-SQ-1-CAV
47-BSB
JNN
MI CO SNAP
TAP
NISC SNAP
4-27 FA B BTY SNAP
Throughp
150
100
50
0
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
July 08
1-SQ-1-CAV
4-BN-27-FA
1-BN-6-IN
1-1 CAV C TRP SNAP
TAC
MI CO SNAP
Other
Ready

Cyber Threat Analysis



- By importing available IP reputation databases which track “black” and “white” IP addresses, the application maps and labels Netflow to these hosts
- Additionally, by utilizing custom reports on port activity, a user can quickly identify unusual activity which can trigger an action to further investigate a possible cyber attack.


FAVA\Data\12-08\S\Arch files\June 21 - 01.arch - PEO C3T WIN-T FTN Analysis and Visualization Application Version 1.3
File Edit View Favorites Tools Help
View
Navigation
Othe
Events
Army
Show Cyber Operations
Filter Builder for
no element filter applied
06/21/12 12:00:00 - 06/23/12 00:00:00
Army
NTC-52-ID
555-EN-BDE
63-ESB
NTC
RTU
2-ID
4-BCT
MCG
TAC
TUAV
F-52-IN-CO
HHC
ARFOR
1-38INF_77312
A-1-BN-38-IN
B-1-BN-38-IN
C-1-BN-38-IN
CP
DAUVS
2-34INF_77313
2-1CAV_77314
2-12FA_77315
TAC-CPN_77316
4-9INF_77317
472SIG_77318
4-2SBCT_JNN_7731
CP-2
BCCS
JNN
DAUVS
MFDC
JTAC-ALO-CMDGP
AFATDS-ALO-CMDGP
42BDETAISADAM
ADSI-RMT-1
AMDWS
12:00 15:00 18:00 21:00 00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00 00:00
June 22
June 23
IP Reputation
Port Analysis
Endpoint
Port/Protocol
Concern Description
Occurences
Unique Destinations
Volume (Bytes)
Packets
Endpoint: CYBEROPS-243 (148.22 (2 items)
Endpoint: CYBEROPS-244 (148.22 (16 items)
CYBEROPS-244 (148 NETBIOS Session Service / TCP (139/6) Host Sending SMB and RPC traffic 2650 1378 427814 6891
CYBEROPS-244 (148 IRCU / TCP (6668/6) Host Sending or Receiving IRC T... 767 231 53940 1201
CYBEROPS-244 (148 IRCU / TCP (6669/6) Host Sending or Receiving IRC T... 771 232 54068 1205
CYBEROPS-244 (148 file server itself / TCP (7000/6) Host Sending or Receiving IRC T... 771 231 54276 1215
CYBEROPS-244 (148 Microsoft-DS / TCP (445/6) Host Sending SMB and RPC traffic 3065 1391 10087927 37380
CYBEROPS-244 (148 Simple Mail Transfer / TCP (25/6) Host Sending SMTP Traffic 2005 1353 121072 2034
CYBEROPS-244 (148 Domain Name Server / UDP (53/17) Host Sending DNS queries 143 131 57989 1100
CYBEROPS-244 (148 6660 / TCP (6660/6) Host Sending or Receiving IRC T... 791 234 54972 1234
CYBEROPS-244 (148 IRCU / TCP (6666/6) Host Sending or Receiving IRC T... 757 232 52532 1169
CYBEROPS-244 (148 DCE endpoint resolution / TCP (135/6) Host Sending SMB and RPC traffic 707 227 3208762 26280
CYBEROPS-244 (148 bmission / TCP (587/6) Host Sending SMTP Traffic 305 221 17956 307
CYBEROPS-244 (148 Authentication Service / TCP (113/6) Host Sending or Receiving IRC T... 763 226 53300 1195
CYBEROPS-244 (148 Italk Chat System / TCP (12345/6) Host Sending or Receiving Traffi... 783 227 54900 1229
CYBEROPS-244 (148 MS V-Worlds / TCP (2525/6) Host Sending SMTP Traffic 286 205 16636 286
CYBEROPS-244 (148 IRCU / TCP (6667/6) Host Sending or Receiving IRC T... 760 226 53540 1203
CYBEROPS-244 (148 Microsoft-SQL-Monitor / UDP (1434/17) Host Sending or Receiving Traffi... 145 121 14559 340
Endpoint: DAUVS (148 (14 items)
Endpoint: DCARS-ADCM-52-ID (148 (1 item)
Ready


File Edit View Favorites Tools Help
Events
Army
RTU
1-BCT
Show Bandwidth Profile
Filter Builder for "TUN-6745" traffic "CYBEROPS" or from '
matched 9 of 5637 >
09/11/12 00:00:00 - 09/12/12 07:01:44
Service Class
Protocol
Talker
Listener
Talker to Listener
Conversation
BFA
Router Interface
Top Protocol Load (Kb/s)
Microsoft-SQL-Server / TCP-1433/6 = 19.73% (4.3 MB)
World Wide Web HTTP / TCP-80/6 = 7.72% (1.68 MB)
46113 / TCP-46113/6 = 2.66% (579.16 KB)
46114 / TCP-46114/6 = 1.88% (411.05 KB)
ICMP-1 = 0.89% (194.15 KB)
105042 / TCP-105042/6 = 0.39% (84.95 KB)
105040 / TCP-105040/6 = 0.33% (71.94 KB)
105041 / TCP-105041/6 = 0.28% (60.97 KB)
105037 / TCP-105037/6 = 0.22% (48.31 KB)
105038 / UDP-105038/17 = 0.14% (30.18 KB)
105036 / TCP-105036/6 = 0.12% (25.34 KB)
HTTP Alternate (see port 80) / TCP-8080/6 = 0.11% (23.01 KB)
SUN Remote Procedure Call / TCP-111/6 = 0.09% (20.45 KB)
Microsoft OLAP / TCP-2383/6 = 0.09% (20.14 KB)
Other = 65.35% (14.25 MB)
Total = 100% (21.81 MB) 1064 Protocol(s)
Ready

FAVA Added Value

- Adds no additional infrastructure to the footprint
- Merges Data and Data Products (unit specific & custom)
  - ✓ Displays unit hierarchy in directory-like structure down to the router interface and host platform levels
  - ✓ Maps data products to Netflow data to identify mission command systems, roles, and echelon/location
  - ✓ Provides temporal & organizational context filtering to specific interfaces, routers, applications, Echelons, etc..
- Transparent to underlying tools – Adaptable to new/other underlying data collection and CyberOps Systems/Tools
- Bridges COTS gaps and an extensible platform for future development

FTN Take Aways

- Tactical Network & Services Subject Matter Expertize
- Transforms data into information and knowledge
  - Identify Configuration Issues
  - Detection of Performance Exceptions
  - Improved Cyber Operations Awareness
  - Warfighter Perspective
  - Etc.
- FAVA was developed to facilitate data integration and analysis and continues to evolve and grow
- Harvesting, archiving, and leveraging historical data
- NetFlow plays a big role

BACKUP

List of Acronyms

- C4ISR – Command, Control, Communications, Computers Intelligence, Surveillance, and Reconnaissance
- CERDEC – Communications Electronics Research, Development, and Engineering Command
- COTS – Commercial Off The Shelf
- FTN – Fight The Network
- FAVA – FTN Analysis and Visualization Application
- JRTC – Joint Readiness Training Center
- LDIF – LDAP Data Interchange Format
- LDAP – Go look that one up, I'm getting tired
- NetOps – Network Operations Support Systems
- NetFlow – Your at the wrong conference
- NTC – National Training Center
- SIGACTS – SIGnificant ACTivitieS
- SIP – Static IP Sheets
- SNMP – Simple Network Management Protocol
- S&TCD - Space and Terrestrial Communications Directorate
- WIN-T TMD -,Warfighter Information Network -Tactical Technical Management Division

Organizations FTN Supports

US Central Command

US Army, 82nd Airborne Division

US Forces - Afghanistan

US Army, 10th Mountain Division

US Army, 101st Airborne Division

Network Integration Evaluation

Joint Readiness Training Center

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

National Training Center

DOD CIO

ARMY TEAM C4ISR

FAVA Highlights

- Directly extracts data (SNMP, NetFlow, Call Detail, and Network Events) from COTS fielded collectors
- Provides context sensitive, general purpose analysis, visualization and reports capability
- Usable real-time or off-line
- Cyber Security Operations capability including IP Reputation, Network Forensics, Network Based Security Incident Detection and Response
- Exposes correlated data to other NetOps systems via Web Services
- Timeline visual event correlation
- Time and echelon context sensitive
- Growing and Evolving – Lower Tactical Internet, Defensive Cyber Ops Support,
- More, Better, Faster!

FAVA Capabilities

Data Initialization

- FAVA does a smart merge of all available data and creates a file that contains the merged architecture. The architecture is then displayed in a (hierarchical) tree view.
- The merged data files can be saved to and becomes portable (to another machine/location).

Timeline context

- Timeline range views can be customized from hours to months so a user can analyze detailed network activity or get a feel for the overall big picture.
- Events can be overlaid on the timeline to further explain network behavior

Element Detail

- Many network element properties from a number of data sources can be reviewed and edited.

FAVA Capabilities (cont.)

Exceptions

- Network errors / exceptions can be viewed and included in a report.
- Having the ability to drill into the details of these can help explain and resolve network problems.

Bandwidth Profile

- Netflow bandwidth data along with an outline of the SNMP throughput data can be viewed by echelon/element or by endpoints/applications
- Data can be viewed in many categories (Application, Talker / Listener, Conversation, Port/Protocol , Service Class, Direction, Router Interface, Sub Element), etc.

VOIP Profile (Call Detail Data)

- Call Detail data can be analyzed including Call Count, Call Duration, Packet Loss, Error Count and Jitter along with a summarization of all measures.
- Call Detail data can also be grouped differently for more effective impact (Caller, Receiver, Conversation, Sub Element, Call Manager, and Error Type)

FAVA Reporting

Endpoint Reporting

- Ability to view all endpoints and properties including drilldown capability to see router interfaces / endpoint relationships, and count of endpoints by interface.
- Having the ability to drill into the details of these can help explain and resolve network problems.

Cyber Operations Reporting

- Correlates NetFlow data against Blacklists from IP Reputation databases. This allows for viewing blacklisted IP addresses communicating with internal endpoints.
- Ability to load and manage IP Reputation black and white lists
- Displays Port analysis data in a intuitive fashion which allows the Warfighter to spot potentially malicious activity that would warrant further investigation

VOIP Reporting

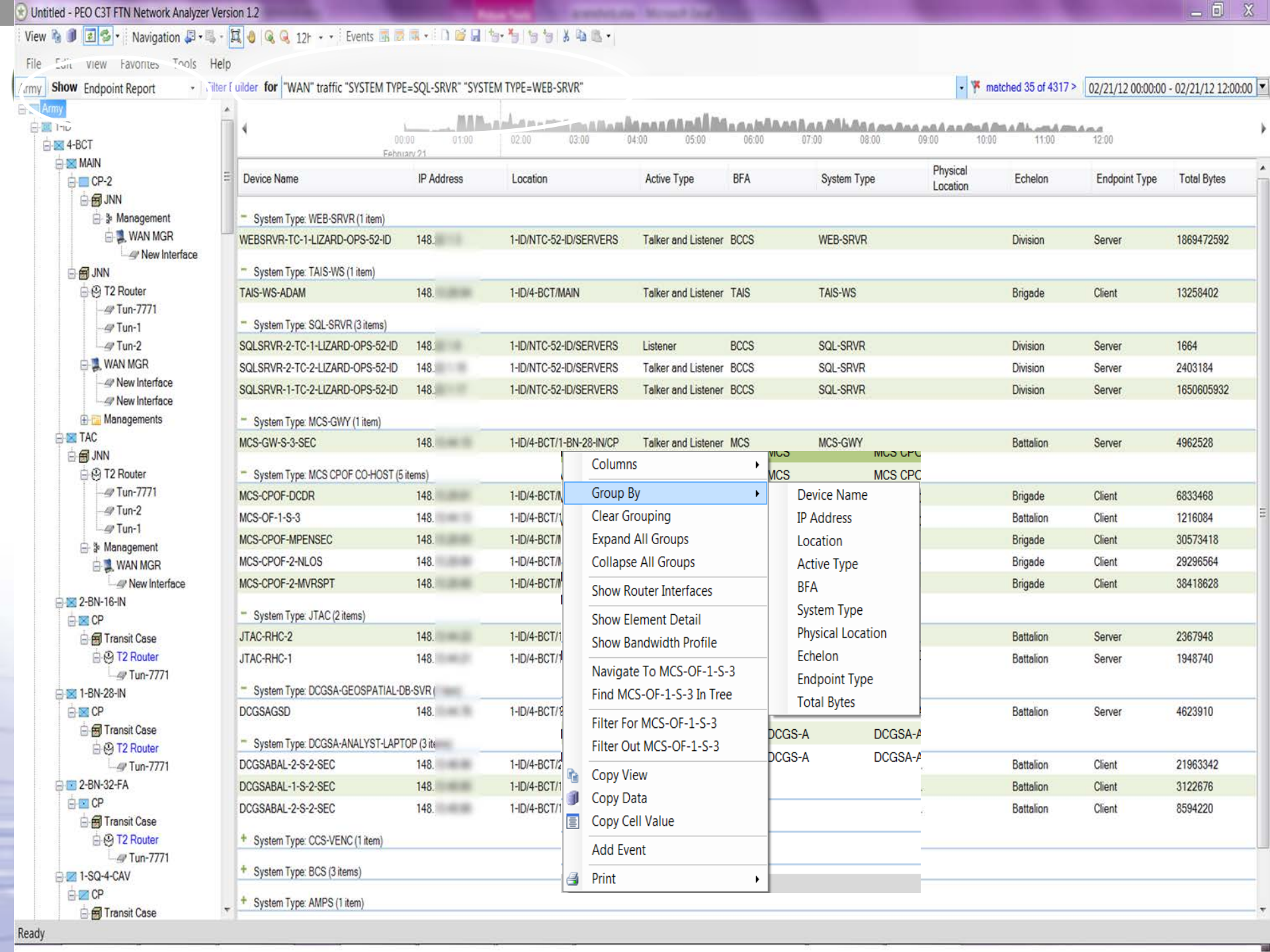
- Summarization data for each Call Server (Call Count, Call Duration, Error Count, Packet Received, Packet Sent, Packet Lost).
- Call and error detail for each call server.
- Reporting of endpoints monitored by call servers

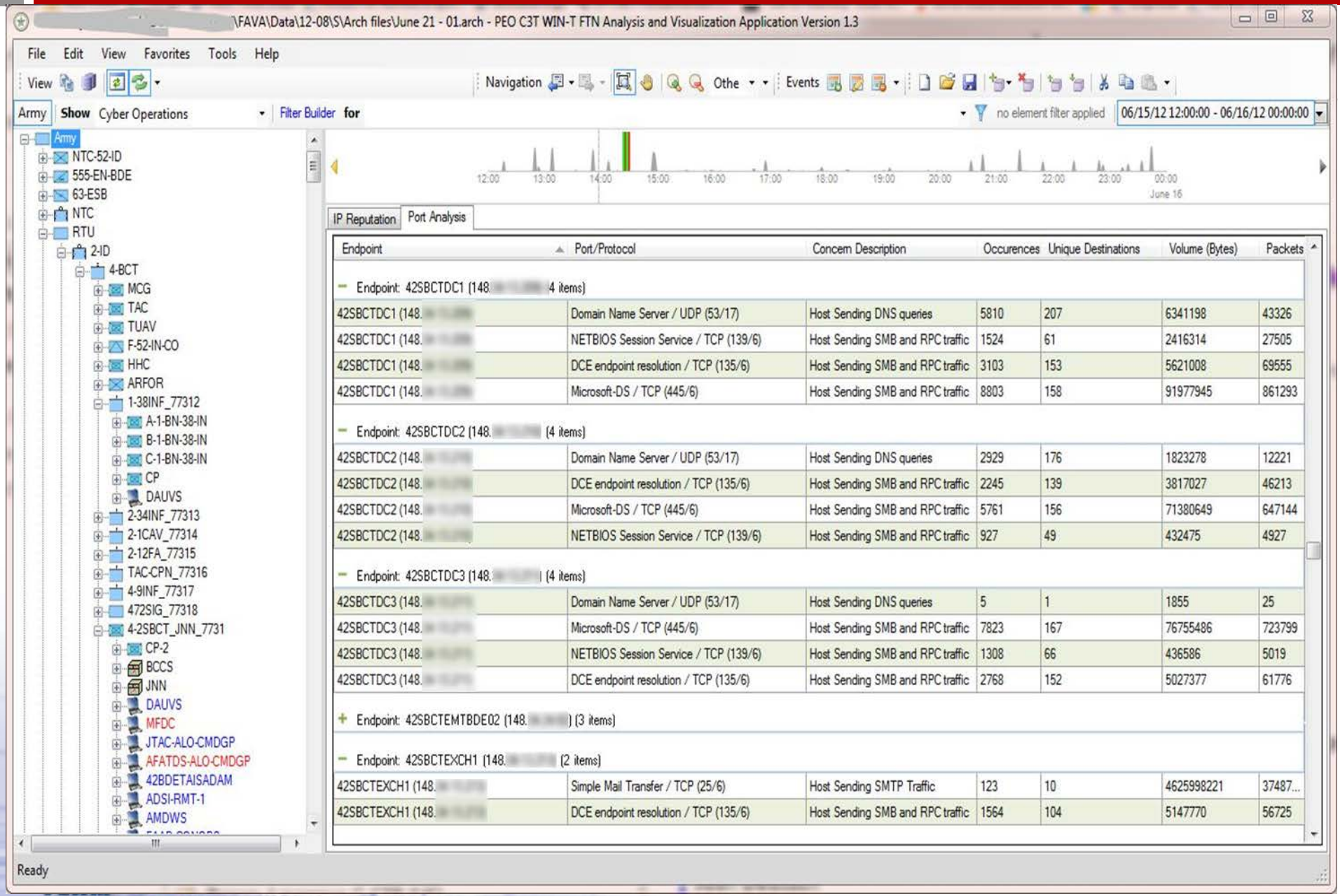
Current Process

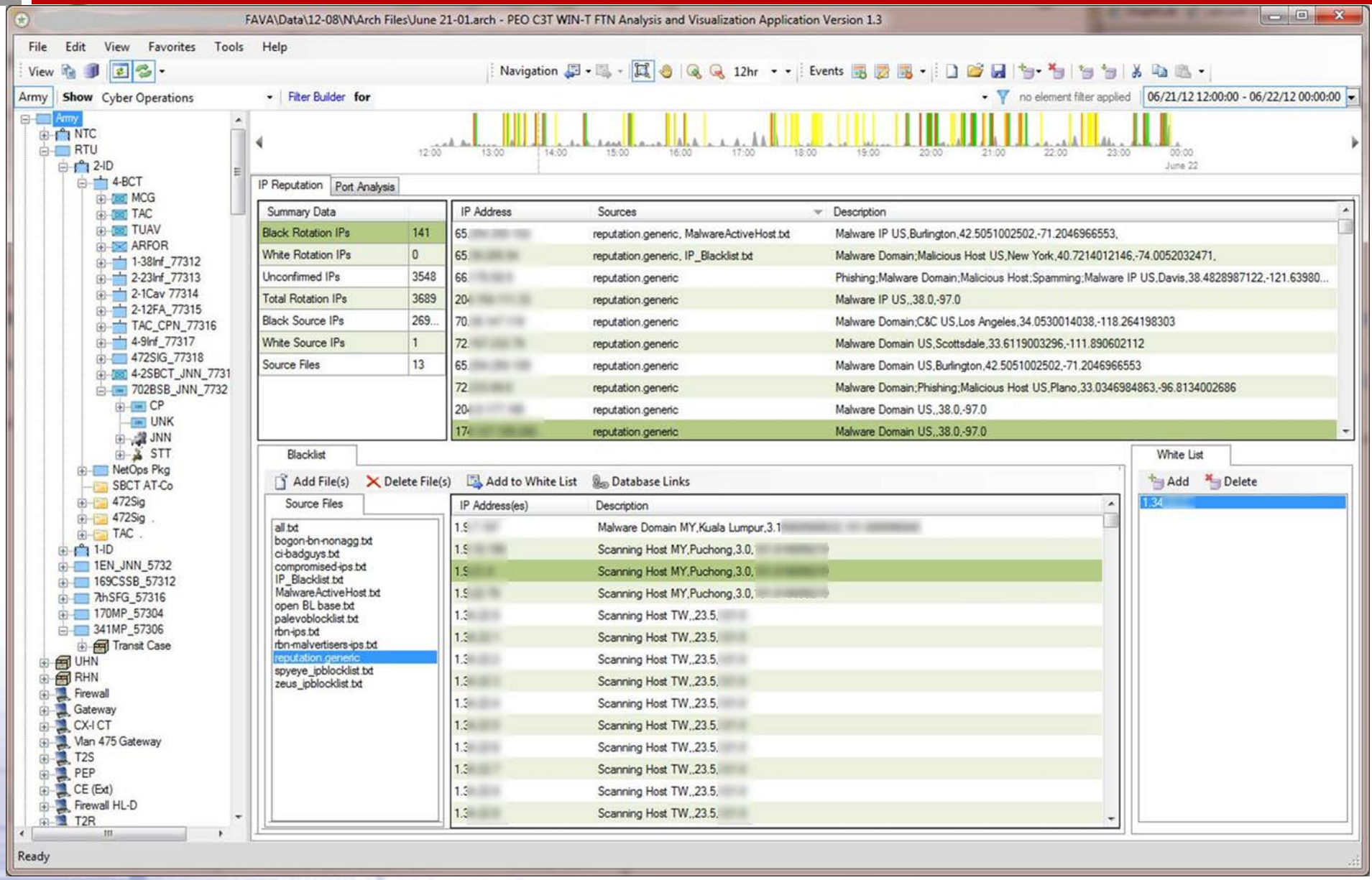
- Collecting data from various tools and data sources
  - Cisco (NetFlow, CDR), SNMP, Other Tools
  - Operational data (SIGACTS from CIDNE, collector events and traps, IP mapping templates, etc.)
  - Unit network and mission command host directory (Echelon, section/role, host name, IP address, etc)

- Focus on relevant network questions such as:
  - What are the applications?
  - Where are the applications?
  - Where are the users?
  - What is application architecture and design?

- FTN analysis and visualization is in real-time, providing direct feedback to units AND post event offline for further in depth analysis and visualization.


Untitled - PEO C3T FTN Network Analyzer Version 1.2
View
Navigation
Events
File
Edit
View
Favorites
Tools
Help
Show
Endpoint Report
for
"WAN" traffic "SYSTEM TYPE=SQL-SRVR" "SYSTEM TYPE=WEB-SRVR"
matched 35 of 4317 >
02/21/12 00:00:00 - 02/21/12 12:00:00
Army
4-BCT
MAIN
CP-2
JNN
Management
WAN MGR
New Interface
JNN
T2 Router
Tun-7771
Tun-1
Tun-2
WAN MGR
New Interface
New Interface
Managements
TAC
JNN
T2 Router
Tun-7771
Tun-2
Tun-1
Management
WAN MGR
New Interface
2-BN-16-IN
CP
Transit Case
T2 Router
Tun-7771
1-BN-28-IN
CP
Transit Case
T2 Router
Tun-7771
2-BN-32-FA
CP
Transit Case
T2 Router
Tun-7771
1-SQ-4-CAV
CP
Transit Case
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
February 21
Device Name
IP Address
Location
Active Type
BFA
System Type
Physical Location
Echelon
Endpoint Type
Total Bytes
System Type: WEB-SRVR (1 item)
WEBSRVR-TC-1-LIZARD-OPS-52-ID 148. 1-ID/NTC-52-ID/SERVERS Talker and Listener BCCS WEB-SRVR Division Server 1869472592
System Type: TAIS-WS (1 item)
TAIS-WS-ADAM 148. 1-ID/4-BCT/MAIN Talker and Listener TAIS TAIS-WS Brigade Client 13258402
System Type: SQL-SRVR (3 items)
SQLSRVR-2-TC-1-LIZARD-OPS-52-ID 148. 1-ID/NTC-52-ID/SERVERS Listener BCCS SQL-SRVR Division Server 1664
SQLSRVR-2-TC-2-LIZARD-OPS-52-ID 148. 1-ID/NTC-52-ID/SERVERS Talker and Listener BCCS SQL-SRVR Division Server 2403184
SQLSRVR-1-TC-2-LIZARD-OPS-52-ID 148. 1-ID/NTC-52-ID/SERVERS Talker and Listener BCCS SQL-SRVR Division Server 1650605932
System Type: MCS-GWY (1 item)
MCS-GW-S-3-SEC 148. 1-ID/4-BCT/1-BN-28-IN/CP Talker and Listener MCS MCS-GWY Battalion Server 4962528
System Type: MCS CPOF CO-HOST (5 items)
MCS-CPOF-DCDR 148. 1-ID/4-BCT/ Brigade Client 6833468
MCS-OF-1-S-3 148. 1-ID/4-BCT/ Battalion Client 1216084
MCS-CPOF-MPENSEC 148. 1-ID/4-BCT/ Brigade Client 30573418
MCS-CPOF-2-NLOS 148. 1-ID/4-BCT/ Brigade Client 29296564
MCS-CPOF-2-MVRSPT 148. 1-ID/4-BCT/ Brigade Client 38418628
System Type: JTAC (2 items)
JTAC-RHC-2 148. 1-ID/4-BCT/ Battalion Server 2367948
JTAC-RHC-1 148. 1-ID/4-BCT/ Battalion Server 1948740
System Type: DCGSA-GEOSPATIAL-DB-SVR
DCGSAGSD 148. 1-ID/4-BCT/ Battalion Server 4623910
System Type: DCGSA-ANALYST-LAPTOP (3 it
DCGSABAL-2-S-2-SEC 148. 1-ID/4-BCT/ Battalion Client 21963342
DCGSABAL-1-S-2-SEC 148. 1-ID/4-BCT/ Battalion Client 3122676
DCGSABAL-2-S-2-SEC 148. 1-ID/4-BCT/ Battalion Client 8594220
System Type: CCS-VENC (1 item)
System Type: BCS (3 items)
System Type: AMPS (1 item)
Columns
Group By
Clear Grouping
Expand All Groups
Collapse All Groups
Show Router Interfaces
Show Element Detail
Show Bandwidth Profile
Navigate To MCS-OF-1-S-3
Find MCS-OF-1-S-3 In Tree
Filter For MCS-OF-1-S-3
Filter Out MCS-OF-1-S-3
Copy View
Copy Data
Copy Cell Value
Add Event
Print
Device Name
IP Address
Location
Active Type
BFA
System Type
Physical Location
Echelon
Endpoint Type
Total Bytes
Ready


\FAVA\Data\12-08\S\Arch files\June 21 - 01.arch - PEO C3T WIN-T FTN Analysis and Visualization Application Version 1.3
File Edit View Favorites Tools Help
View
Navigation
Othe
Events
Army
Show Cyber Operations
Filter Builder for
no element filter applied
06/15/12 12:00:00 - 06/16/12 00:00:00
Army
NTC-52-ID
555-EN-BDE
63-ESB
NTC
RTU
2-ID
4-BCT
MCG
TAC
TUAV
F-52-IN-CO
HHC
ARFOR
1-38INF_77312
A-1-BN-38-IN
B-1-BN-38-IN
C-1-BN-38-IN
CP
DAUVS
2-34INF_77313
2-1CAV_77314
2-12FA_77315
TAC-CPN_77316
4-9INF_77317
472SIG_77318
4-2SBCT_JNN_7731
CP-2
BCCS
JNN
DAUVS
MFDC
JTAC-ALO-CMDGP
AFATDS-ALO-CMDGP
42BDETAISADAM
ADSI-RMT-1
AMDWS
12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00
June 16
IP Reputation
Port Analysis
Endpoint
Port/Protocol
Concern Description
Occurences
Unique Destinations
Volume (Bytes)
Packets
Endpoint: 42SBCTDC1 (148. 4 items)
42SBCTDC1 (148. Domain Name Server / UDP (53/17) Host Sending DNS queries 5810 207 6341198 43326
42SBCTDC1 (148. NETBIOS Session Service / TCP (139/6) Host Sending SMB and RPC traffic 1524 61 2416314 27505
42SBCTDC1 (148. DCE endpoint resolution / TCP (135/6) Host Sending SMB and RPC traffic 3103 153 5621008 69555
42SBCTDC1 (148. Microsoft-DS / TCP (445/6) Host Sending SMB and RPC traffic 8803 158 91977945 861293
Endpoint: 42SBCTDC2 (148. (4 items)
42SBCTDC2 (148. Domain Name Server / UDP (53/17) Host Sending DNS queries 2929 176 1823278 12221
42SBCTDC2 (148. DCE endpoint resolution / TCP (135/6) Host Sending SMB and RPC traffic 2245 139 3817027 46213
42SBCTDC2 (148. Microsoft-DS / TCP (445/6) Host Sending SMB and RPC traffic 5761 156 71380649 647144
42SBCTDC2 (148. NETBIOS Session Service / TCP (139/6) Host Sending SMB and RPC traffic 927 49 432475 4927
Endpoint: 42SBCTDC3 (148. (4 items)
42SBCTDC3 (148. Domain Name Server / UDP (53/17) Host Sending DNS queries 5 1 1855 25
42SBCTDC3 (148. Microsoft-DS / TCP (445/6) Host Sending SMB and RPC traffic 7823 167 76755486 723799
42SBCTDC3 (148. NETBIOS Session Service / TCP (139/6) Host Sending SMB and RPC traffic 1308 66 436586 5019
42SBCTDC3 (148. DCE endpoint resolution / TCP (135/6) Host Sending SMB and RPC traffic 2768 152 5027377 61776
Endpoint: 42SBCTEMTBDE02 (148. (3 items)
Endpoint: 42SBCTEXCH1 (148. (2 items)
42SBCTEXCH1 (148. Simple Mail Transfer / TCP (25/6) Host Sending SMTP Traffic 123 10 4625998221 37487...
42SBCTEXCH1 (148. DCE endpoint resolution / TCP (135/6) Host Sending SMB and RPC traffic 1564 104 5147770 56725
Ready


FAVA\Data\12-08\N\Arch Files\June 21-01.arch - PEO C3T WIN-T FTN Analysis and Visualization Application Version 1.3
File Edit View Favorites Tools Help
Navigation 12hr Events
Army Show Cyber Operations Filter Builder for
no element filter applied
06/21/12 12:00:00 - 06/22/12 00:00:00
Army
NTC
RTU
2-ID
4-BCT
MCG
TAC
TUAV
ARFOR
1-38Inf_77312
2-23Inf_77313
2-1Cav 77314
2-12FA_77315
TAC_CPN_77316
4-9Inf_77317
472SIG_77318
4-2SBCT_JNN_7731
702BSB_JNN_7732
CP
UNK
JNN
STT
NetOps Pkg
SBCT AT-Co
472Sig
472Sig .
TAC .
1-ID
1EN_JNN_5732
169CSSB_57312
7thSFG_57316
170MP_57304
341MP_57306
Transit Case
UHN
RHN
Firewall
Gateway
CX-I CT
Vlan 475 Gateway
T2S
PEP
CE (Ext)
Firewall HL-D
T2R
12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 June 22
IP Reputation
Port Analysis
Summary Data
Black Rotation IPs 141
White Rotation IPs 0
Unconfirmed IPs 3548
Total Rotation IPs 3689
Black Source IPs 269...
White Source IPs 1
Source Files 13
IP Address
Sources
Description
reputation.generic, MalwareActiveHost.txt
Malware IP US,Burlington,42.5051002502,-71.2046966553,
reputation.generic, IP_Blacklist.txt
Malware Domain;Malicious Host US,New York,40.7214012146,-74.0052032471,
reputation.generic
Phishing;Malware Domain;Malicious Host;Spamming;Malware IP US,Davis,38.4828987122,-121.63980...
reputation.generic
Malware IP US,,38.0,-97.0
reputation.generic
Malware Domain;C&C US,Los Angeles,34.0530014038,-118.264198303
reputation.generic
Malware Domain US,Scottsdale,33.6119003296,-111.890602112
reputation.generic
Malware Domain US,Burlington,42.5051002502,-71.2046966553
reputation.generic
Malware Domain;Phishing;Malicious Host US,Plano,33.0346984863,-96.8134002686
reputation.generic
Malware Domain US,,38.0,-97.0
reputation.generic
Malware Domain US,,38.0,-97.0
Blacklist
Add File(s)
Delete File(s)
Add to White List
Database Links
Source Files
all.txt
bogon-bn-nonagg.txt
ci-badguys.txt
compromised-ips.txt
IP_Blacklist.txt
MalwareActiveHost.txt
open BL base.txt
palevoblocklist.txt
rbn-ips.txt
rbn-malvertisers-ips.txt
reputation.generic
spyeye_ipblocklist.txt
zeus_ipblocklist.txt
IP Address(es)
Description
Malware Domain MY,Kuala Lumpur,3.1
Scanning Host MY,Puchong,3.0,
Scanning Host MY,Puchong,3.0,
Scanning Host MY,Puchong,3.0,
Scanning Host TW,,23.5,
White List
Add
Delete
1.34
Ready