This video and all related information and materials ("materials") are owned by Carnegie Mellon University. These materials are provided on an "as-is" "as available" basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM专利, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.


DM-0003080
Using Network Flow to Gain Cyber Situational Awareness

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Sidney Faber
Polling Question 1

How familiar are you with the concept of “Cyber Situational Awareness”?

- Sounds interesting, but I haven’t put much thought into it
- I’m familiar with situational awareness, but have never applied it to cyber
- It’s an important part of my work but I would like to better understand it
- I’ve studied and applied the concept extensively
Polling Question 2

What is your background?
   Executive management
   Technical management
   Operational leader (e.g., shift supervisor)
   Technical or operational staff
Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.

Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.
Cyber situational awareness is the subset of all situation awareness necessary to support taking actions in cyber.
Using Network Flow to Gain Cyber Situational Awareness
SEI Webinar
© 2015 Carnegie Mellon University
The Open System Model

ISO 7498 para 6.1.3 page 28
Figure 11 – Seven layer reference model and peer protocols
The Open System Model

ISO 7498 para 6.1.3 page 28

Figure 11 – Seven layer reference model and peer protocols
Cyber situational awareness is the subset of all situation awareness necessary to support taking actions in cyber.
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University

System Factors

Feedback

Cyber Environment

Network Flow

Environment

SITUATIONAL AWARENESS

Perception Comprehension Projection

Human – Computer Interface

Decisions

Cyber Actions

Cyber Environment

SYSTEM SITUATIONAL AWARENESS

Perception Comprehension Projection

Environment

Individual Factors
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University

SYSTEM SITUATIONAL AWARENESS

Perception  Comprehension  Projection

Cyber Environment

Environment

Feedback

Decisions  Cyber Actions

Individual Factors

SITUATIONAL AWARENESS

Network Flow

Perception  Comprehension  Projection

Human – Computer Interface

System Factors

Cyber Environment

Network Flow Table:

<table>
<thead>
<tr>
<th>sIP</th>
<th>dIP</th>
<th>sPort</th>
<th>dPort</th>
<th>pro</th>
<th>packets</th>
<th>flags</th>
<th>initF</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.105</td>
<td>198.51.100.6</td>
<td>49152</td>
<td>80</td>
<td>6</td>
<td>4</td>
<td>SRPA</td>
<td>S</td>
<td>outweb</td>
</tr>
<tr>
<td>198.51.100.6</td>
<td>192.168.1.105</td>
<td>80</td>
<td>49152</td>
<td>6</td>
<td>3</td>
<td>S PA</td>
<td>S  A</td>
<td>inweb</td>
</tr>
</tbody>
</table>
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University

SYSTEM SITUATIONAL AWARENESS

- Perception
- Comprehension
- Projection

Feedback

Decisions

Cyber Actions

System Factors

Environment

Cyber Environment

Individual Factors

Environment

Network Flow

Human – Computer Interface

SITUATIONAL AWARENESS

- Perception
- Comprehension
- Projection

Perception Comprehension Projection

Environment
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University

System Factors

Feedback

SYSTEM SITUATIONAL AWARENESS

Cyber Environment

Network Flow

Analytics

Human – Computer Interface

Decisions

Cyber Actions

Environment

Perception Comprehension Projection

SITUATIONAL AWARENESS

Individual Factors
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University

Sensing

Analytics

Human – Computer Interface

Situation Awareness

Decision Support
Polling Question 3:

What should we discuss in more detail?
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University

Sensing

System Factors

Analytics

Human – Computer Interface

Situation Awareness

Decision Support

Individual Factors
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar
© 2015 Carnegie Mellon University
Using Network Flow to Gain Cyber Situational Awareness

SEI Webinar

© 2015 Carnegie Mellon University
Using Network Flow to Gain Cyber Situational Awareness
SEI Webinar
© 2015 Carnegie Mellon University