

Cybersituational Awareness - Appunti

Francesco Lorenzoni

Febrero 2025

Contents

- I Introduction to CS 5**
- 1 Ciberconciencia Situacional 9**
 - 1.1 Introducción 9
 - 1.2 Conciencia Situacional 9
 - 1.2.1 Situation Understanding 10
 - 1.2.2 Situational Awareness in Cyberspace 10
 - 1.3 Ciberconciencia situacional 11
 - 1.3.1 Vulnerabilidades 11
 - 1.3.2 Amenazas - Threats 11
- 2 Tarea 1 - Conceptos complementarios de Ciberconciencia Situacional 13**
- 3 Cyber Intelligence Visualization 15**

Part I

Introduction to CS

1	Ciberconciencia Situacional	9
1.1	Introducción	9
1.2	Conciencia Situacional	9
1.2.1	Situation Understanding	10
1.2.2	Situational Awareness in Cyberspace	10
1.3	Ciberconciencia situacional	11
1.3.1	Vulnerabilidades	11
1.3.2	Amenazas - Threats	11
2	Tarea 1 - Conceptos complementarios de Ciberconciencia Situacional	13
3	Cyber Intelligence Visualization	15

Chapter 1

Ciberconciencia Situacional

There are tasks (tarefas) each monday. Each monday the lectures are asynchronous, and a task if given which lasts one or two weeks. The tarea may be committed by email if the deadline expires but it is preferable to finish in time.

1.1 Introducción

1. Conciencia Situacional
 - i. Situational Awareness
 - ii. Situational Awareness in Physical World
 - iii. Situational Awareness in Cyberspace
2. Visualización
 - i. Cyberintelligence Visualization
 - ii. Visualization Charts
3. Herramientas de ciberconciencia situacional
 - i. Cybersituational Awareness Tools
 - ii. Sources on Intelligence
 - iii. Risk and Consequences Analysis
4. Conciencia situacional hibrida
 - i. Hybrid situational awareness
 - ii. Cyber-Hybrid Situational Awareness Tools
5. Seguridad de sistemas ciberfisicos y protección de infraestructuras críticas
 - i. Cyber-Physical Systems (CPS)

Un CPS es un sistema que tiene una parte cibernética y otra física. Así de sencillo, según el prof. Esteve.
 - ii. CPS Vulnerabilities
 - iii. Industrial Control Systems Cyberdefense
 - iv. Critical Infrastructure Protection

“Ciberconciencia situational significa Saber lo que està pasando en el ciberespacio” — Manuel Esteve

Un punto fundamental para saber lo que està pasando en el ciberespacio es la **visualización**. La visualización es una herramienta fundamental para la ciberconciencia situacional. En otras palabras, es necesario cabir lo que es importante que se visualice sobre el monitor pantalla (“videowall”) y lo que no.

1.2 Conciencia Situacional

Definition 1.1 (Situational Awareness) *Situational awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*

Está también otra definición de conciencia situacional, que se encuentra en el *United States Army Field* manual:

Definition 1.2 (Situational Awareness - II) *Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, competitive and other operations within the battlespace in order to facilitate decision making. An informational perspective and skill that fosters an ability to determine quickly the context and relevance of events that are unfolding*

Ambas definiciones pueden adaptarse al contexto cyber de Internet. De aquí se deriva la definición de *Cyber Situational Awareness* dada anteriormente “saber lo que está pasando en el ciberespacio”. Hay otras definiciones también:

Definition 1.3 (Cyber Situational Awareness) *Comprehensive cyber situation awareness involves three key areas: computing and network components, threat information, and mission dependencies*

MITRE

Definition 1.4 (Cyber Situational Awareness) *Gathering real-time information about an organization's computer networks in order to provide an effective response to an attack*

Computer Language Dictionary

1.2.1 Situation Understanding

Definition 1.5 (Situation Understanding) *Understanding involves having a sufficient level of knowledge to be able to draw inferences about the possible consequences of the situation, as well as sufficient awareness of the situation to predict future patterns*

Note that the following concepts related with situational awareness and are “similar” but they are not the same:

- ◇ Data
- ◇ Information
- ◇ Perceptions
- ◇ Intelligence
- ◇ Knowledge

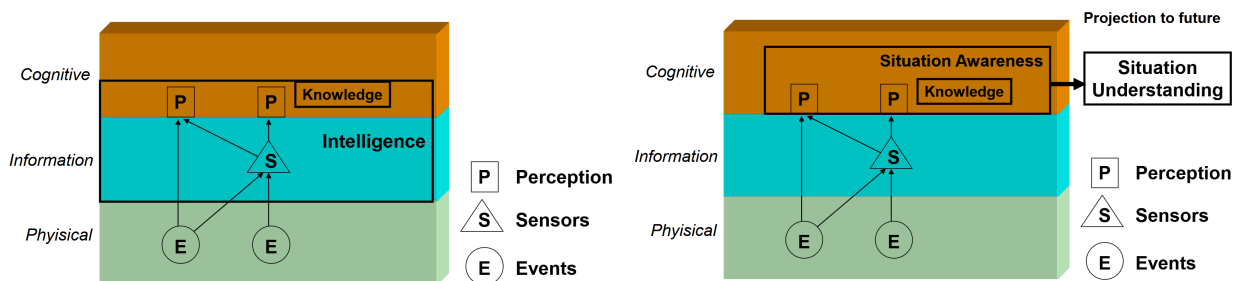


Figure 1.1: Producing Cyber Situational Awareness

1.2.2 Situational Awareness in Cyberspace

Cyber situational awareness involves three areas:

1. Networks and systems - *Network Awareness*
 2. Threats and incidents (including APT and any other kind of attacks) - *Threat Awareness*
 3. Fulfillment of the mission - *Mission Awareness*
- ◇ Network awareness:
 - Assets and configuration management
 - Vulnerabilities auditing
 - Patch management
 - Sharing of incident awareness
 - ◇ Threat awareness
 - Internal incidents and suspicious behavior tracking
 - Knowledge of external threats, by mean of intelligence activities
 - HUMINT, OSINT, SIGINT)
 - Share threat intelligence with government organizations (CERTs) or industry associations
 - ◇ Mission awareness:
 - Develop a Common Operational Picture to understand all dependences and components to operate/develop missions in cyberspace
 - Select the best response decisions during incident management
 - Risk assesment before any response task execution
 - Find out mission impact during forensic analysis, after incident
 - Ellaborate defense plannig for future incidents management

Situational awareness can be generated at three traditional military command and control **levels**:

1. Tactical

The main goal at this level is to visualize and take care of events and situations related with assets. Sometimes this is called also *Technical level*

2. Operational

Main goal at this level is to summarize tactical level details and putting them in context of impact to organization misión.

3. Strategical

Es fundamental cabir que la ciberconciencia situacional se puede costruir a partir desde cuatro fuentes de información de cyber intelligence techniques:



Figure 1.2: Cyber intelligence techniques

- ◇ Cyber HUMINT - Human Intelligence, una fuente de información, por ejemplo, son *usuarios*, que proporcionan información sobre los seres humanos
- ◇ Cyber OSINT - Open Source Intelligence
- ◇ Cyber SIGINT - Signal Intelligence
- ◇ Cyber TECHINT - Technical Intelligence

1.3 Ciberconciencia situacional

Aparte del conocimiento de la situación en general, ahora podemos centrarnos en lo que ocurre en el *ciberespacio*. Esto se llama *Cyber Situational Awareness*.

Associated información with assets:

- ◇ *Alarms*
- ◇ *Events*
- ◇ *Software*
- ◇ *Services*
- ◇ *Plugins*
- ◇ *Properties*
- ◇ *Netflow* (this is fundamental for the ciberconciencia situacional)
- ◇ *Groups*

1.3.1 Vulnerabilidades

Definition 1.6 (Vulnerabilities) *Security gaps that can be used by potencial attackers*

Vulnerabilidades son asociadas con los *assets*, propios o ajenos. Intrínsecamente todos los assets son propensos a haber vulnerabilidades, ahora o en el futuro, cuando algunos condiciones cambian.

Vulns son códifigadas y clasificadas en varios modos:

- ◇ Attack vectors
- ◇ Assets affected by X
- ◇ Exploitation easiness of effort tradeoff
- ◇ Criticallity
- ◇ Damage assessment if exploited

En general, así come si pueden caracterizar las vulnerabilidades:

- ◇ Vuln ID
- ◇ Asset
- ◇ Scan time
- ◇ Service
- ◇ Severity

1.3.2 Amenazas - Threats

Definition 1.7 (Threats) *Elements that can harm our protected system parts or as a whole. Pueden ser internal o external.*

Tenemos que caracterizar amenazas como:

- ◊ Kind
- ◊ Impact
- ◊ Probability
- ◊ Origin

MITRE es la más conocida organización que se dedica a la ciberconciencia situacional, y que ha desarrollado un framework para la ciberconciencia situacional. La MITRE attack matrix es una herramienta que permite visualizar las amenazas y los ataques que se pueden producir en un sistema.

Una amenazas no es sinonimo de *incidente*, que tiene una definición dedicada.

Definition 1.8 (Incident) *Un incidente es un evento que supera cierto umbral de peligro*

Chapter 2

Tarea 1 - Conceptos complementarios de Ciberconciencia Situacional

1. [youtube.com/watch?v=cVaX07btaiU](https://www.youtube.com/watch?v=cVaX07btaiU)

Este vídeo aborda el tema de la conciencia cibersituacional en la producción de OT. Entre los conceptos más relevantes mencionados se encuentran:

- i. El Monitoring se divide en *Event Monitoring* y *Network Monitoring*, el primero basado en una tecnología de *event collection* (SW) que se instala en los dispositivos que los generan, y el segundo basado en la *heurística* sobre el tráfico de red. El vídeo señala cómo la heurística puede conducir a veces a falsos positivos y entonces sea necesaria interpretación humana.
- ii. La importancia de definir ambos los escenarios de ataque y los de defensa: más precisamente, agregando raw event data se pueden identificar escenarios (secuencia de eventos) en una lista de *use-cases*, y a partir de uno *use-case*, un técnico humano puede buscar en un *runbook* lo que tiene que hacer para mitigar lo *use-case* de ataque.

2. [youtube.com/watch?v=Sn6c5s3WFWw](https://www.youtube.com/watch?v=Sn6c5s3WFWw)

- i. Este vídeo subraya la importancia de la ciberconciencia situacional especialmente para hacer frente a “*unknown threats*”, que no coinciden con ninguna regla o pattern específico ya conocido (algo como Zero-Day Vulnerabilities).

3. [youtube.com/watch?v=4geDznrTdbQ](https://www.youtube.com/watch?v=4geDznrTdbQ)

- i. Este vídeo introduce el tema de la **priorización**: en las organizaciones medianas y grandes, es habitual tener enormes cantidades de posibles amenazas, y es necesario priorizarlas para poder actuar de manera eficiente. La conciencia situacional puede ser de grande ayuda en este sentido.
- ii. **Common Operating Picture**, parece referirse a evitar mantener la información divisa en “silos”, y a entender cómo y qué datos agregar, para obtener una visión más completa de la situación. Esta agregación de datos puede variar según la “Mission” de la organización.

4. [youtube.com/watch?v=T9bmqqcjfkg](https://www.youtube.com/watch?v=T9bmqqcjfkg)

- i. Attack scenario graphs son una herramienta para visualizar las relaciones entre las vulnerabilidades de un sistema, y entonces cómo multi-step ataques pueden ser realizados.
Estos grafos pueden ser relacionados con software dependency graphs, para visualizar como uno step de ataque a un componente puede afectar otros componentes que dependen de él.
- ii. Destaca el aspecto en cascada de los ataques también al hablar de la superficie de ataque, cuya definición típica carece del concepto de daño de una brecha en la superficie al igual que los posibles pasos de ataque posteriores, limitándose a una visión más simple que sólo considera los entry points.
- iii. Otro aspecto mencionado es la importancia y la dificultad de agregar datos de diferentes fuentes, que ponen un desafío a la ciberconciencia situacional, así como la limitación de los modelos de scoring de las vulnerabilidades, que además de estar limitados por ellos mismos, necesitan ser relacionados con el contexto de la organización.

Chapter 3

Cyber Intelligence Visualization

Objetivo principal: producir para analistas y responsables de la toma de decisiones mecanismos útiles para comprender, de un vistazo, la información relevante y las tendencias dentro de las enormes cantidades de datos en bruto que les proporcionamos actualmente en las herramientas cibernéticas.

Las herramientas de ciber inteligencia generan una gran cantidad de datos, en gran parte testuale, y es necesario que los analistas sean capaces de procesarlos y entenderlos de manera rápida y eficiente.

Es frecuentemente necesario representar multi-dimensional data en un espacio 2D o 3D.

Los puntos clave de la visualización de la inteligencia cibernética son:

- ◇ Dimensionality reduction and complexity reduction.
- ◇ Assuming inherent non-linearities and couplings
- ◇ Tools and visualization techniques are needed to help in the iterative process: