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 Cyber Intelligence Visualization **15**
2.1 Visualization Charts . . . 15
2.1.1 Georeferenced visualizations and IP-Port mapping . . . 15

3 Sources of Intelligence **19**
3.1 Herramientas de Ciberconciencia Situacional . . . 19
3.1.1 Objetivos principales . . . 19
3.1.2 Diferenciación con otras herramientas . . . 19
3.1.3 Capacidades clave . . . 19
3.1.4 Requisitos operacionales . . . 19
3.2 Connection of Cyber Sensors . . . 20
3.3 SIEM . . . 21
3.4 Incident Response Systems . . . 21

4 Hybrid Situational Awareness **23**
4.1 Introducción . . . 23

II Sistemas Ciberfísicos **25**

5 Cyber-Physical Systems **29**
5.1 Introducción . . . 29
5.2 Componenetes de CPSs . . . 29
5.2.0.1 Industrial Control Systems . . . 29
5.3 Vulnerabilidades . . . 30
5.3.1 Vulnerabilidades más comunes . . . 31
5.4 Vulnerabilities Assessment . . . 31
5.4.1 Intrusion detection . . . 32
5.4.2 Exploits mitigación . . . 32

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 Cyber Intelligence Visualization **15**
2.1 Visualization Charts . . . 15
2.1.1 Georeferenced visualizations and IP-Port mapping . . . 15

3 Sources of Intelligence **19**
3.1 Herramientas de Ciberconciencia Situacional . . . 19
3.1.1 Objetivos principales . . . 19
3.1.2 Diferenciación con otras herramientas . . . 19
3.1.3 Capacidades clave . . . 19
3.1.4 Requisitos operacionales . . . 19
3.2 Connection of Cyber Sensors . . . 20
3.3 SIEM . . . 21
3.4 Incident Response Systems . . . 21

4 Hybrid Situational Awareness **23**
4.1 Introducción . . . 23

Chapter 1

Ciberconciencia Situacional

There are tasks (tareas) each monday. Each monday the lectures are asynchronous, and a task if given which lasts one or two weeks. The tarea may be commited by email if the deadline expires but it is preferrable 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 ciberspacio"* — Manuel Esteve

Un punto fundamental para saber lo que està pasando en el ciberspacio 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 ciberspacio". 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 misison 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

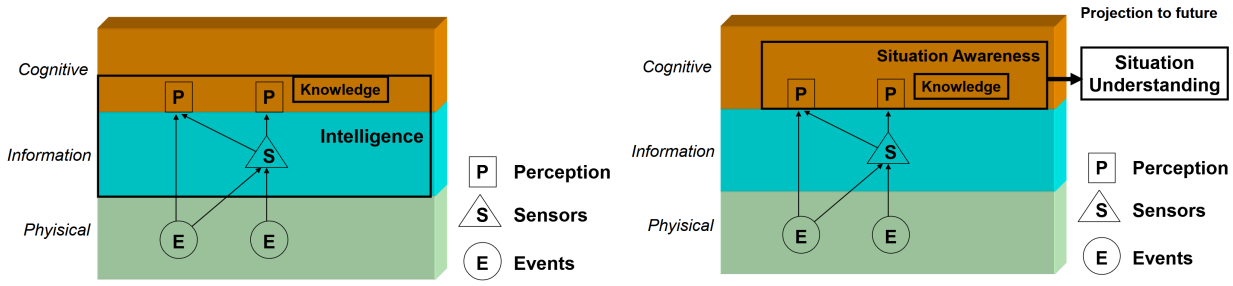


Figure 1.1: Producing Cyber Situational Awareness

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. Fullfillment 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 goverment 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 deccisions 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 situational se puede costruir a partir desde cuatro fuentes de información de cyber intelligence techniques:

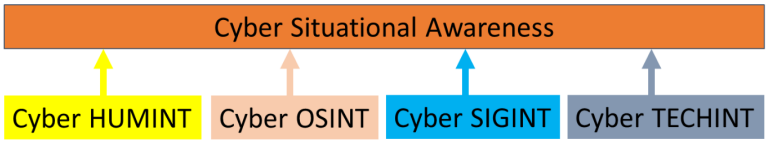


Figure 1.2: Cyber intelligence techniques

- 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 clasficadas 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*

Tarea 1 - Conceptos complementarios de Ciberconciencia Situacional

1. 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 si 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 scenarios de ataque y los de defensa: más precisamente, agregando raw event data se pueden identificar scenarios (secuencia de eventos)en una lista de ***use-cases***, y a partir da 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
   i. Este vídeo subraya la importacia de la ciberconciencia situaciónal 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
   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 situaciónal 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=T9bmqccjfkg
   i. **Attack scenario graphs** son una herramienta para visualizar los relaciones entre las vulnerabilidades de un sistema, y entonces cómo multi-step ataques pueden ser realizados.
   Estes 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. El video destaca el aspecto de "attack cascade" 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 2

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.

The needs for the cyber intelligence domain are pretty specific:

- ◇ Breakdown the overwhelming amount of data into manageable pieces to find the data we are actually interested in.
- ◇ Topological representations to show the relationships among the elements.
- ◇ Adapt the representation to the timing and pace of the cyberspace.
- ◇ Coupling cyber space domain data with physical domain data.

Es frequentemente necesario representar multi-dimensional data en un espacio 2D o 3D, y utilizar visualizaciones interactivas para permitir a los analistas analizar empezando por la información clave más relevante y siguiendo con datos más finos.

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

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

2.1 Visualization Charts

Area	Bar	BoxPlot	Bubble	Column
Doughnut	ErrorBar	FastLine	Funnel	Kagi
Line	Pie	Point	Polar	Radar
Range	Spline	StackedArea	StackedBar	StepLine

Table 2.1: Basic tecniques for Cyber Intelligence Visualization

Los investigadores y profesionales descubrieron que las técnicas de visualización existentes no satisfacen las necesidades de representación del ciberespacio, mientras que la *graph-based* visualización gráficos proporciona medios para mostrar datos interrelacionados multidimensionales en un gráfico de pocas dimensiones.
Una tecnica eficiente para reducir las dimensiones de los datos es utilizar el color.

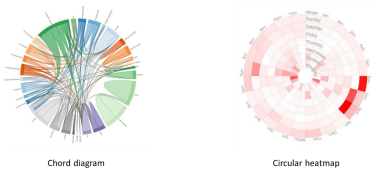
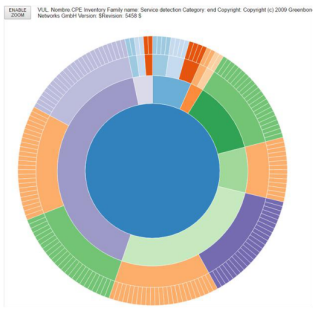


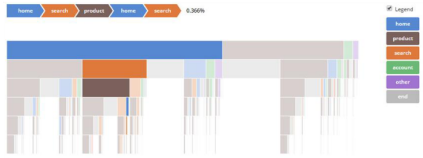
Figure 2.1: Relational color-based dimension reduction

2.1.1 Georeferenced visualizations and IP-Port mapping

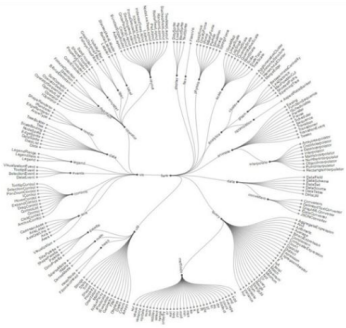
Hoy en día, mucha información del ciberespacio se acopla a magnitudes físicas del mundo real. Por ejemplo, si conocemos la localización de una dirección IP, podemos determinar de donde proviene el ataque. También es posible colorear un mapa según la distribución geográfica de los ataques.



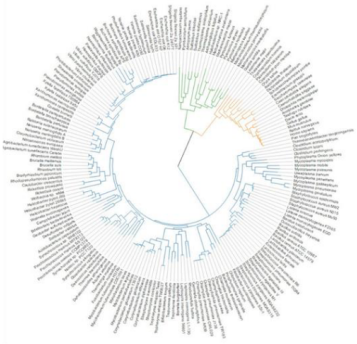
Zoomable sunburst



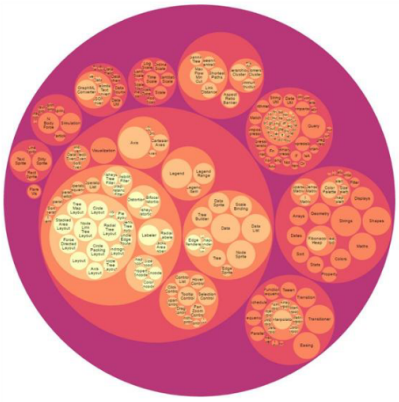
iSequence (1D zoomable sunburst)



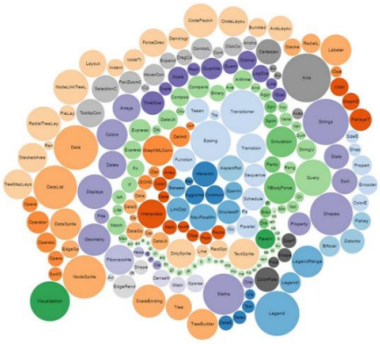
Radial dendogram



Complex tree view



Interactive circle packing (II)



Bubble chart

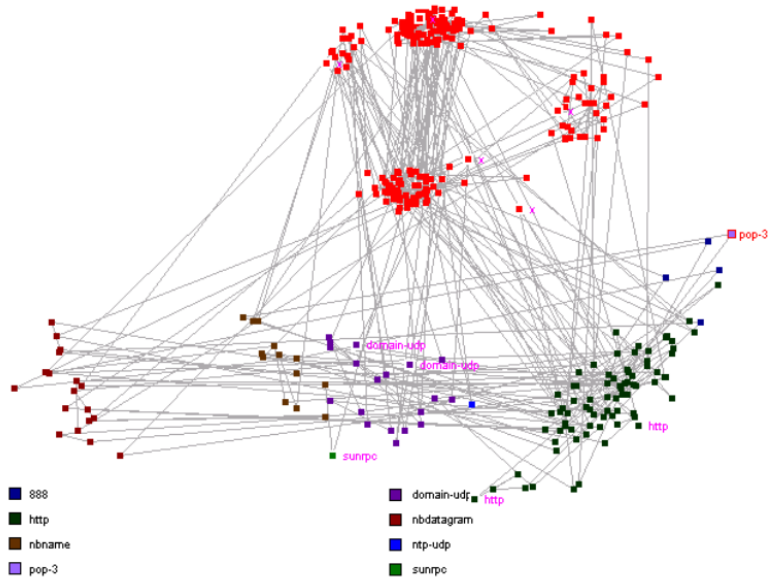


Figure 2.1: Graph-based visualización techniques

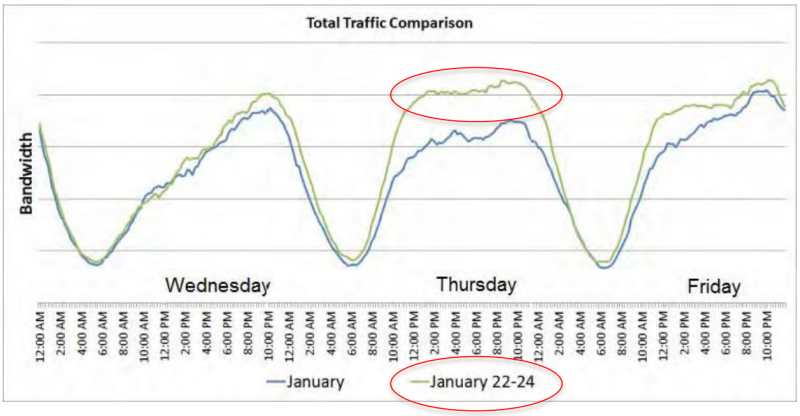


Figure 2.2: Según el profesor, este gráfico es muy importante porque muestra que para identificar lo que es *anormal*, es necesario saber lo que es *normal*.

Gráficos que muestran las conexiones abiertas a los puertos de un nodo de red, o entre nodos de red, pueden mostrar fácilmente la actividad de exploración.

Chapter 3

Sources of Intelligence

3.1 Herramientas de Ciberconciencia Situacional

Las herramientas de ciberconciencia situacional (CSA) son necesarias porque los sistemas de monitorización de ciberseguridad y las herramientas de ciberinteligencia generan enormes cantidades de información que resultaría imposible analizar manualmente. Este análisis manual sería laborioso y propenso a errores. Además, un problema crítico es que los analistas pueden "ahogarse en un mar de detalles" y perder la visión global de la situación.

3.1.1 Objetivos principales

Las herramientas de CSA deben mejorar el rendimiento, la cognición y la comprensión tanto para analistas como para responsables de toma de decisiones. Específicamente, ayudan a responder preguntas fundamentales como:

- ◇ ¿Hay algún ataque en curso? Si es así, ¿dónde está el atacante? ¿Cómo evoluciona la situación?
- ◇ ¿Cómo está afectando el ataque a la empresa o misión? ¿Cómo podemos evaluar el daño?
- ◇ ¿Cómo se espera que se comporten los atacantes? ¿Cuáles son sus estrategias?
- ◇ ¿Podemos predecir futuros plausibles de la situación actual?
- ◇ ¿Cómo creó el atacante la situación actual? ¿Qué intentaba conseguir?

3.1.2 Diferenciación con otras herramientas

Estas preguntas no pueden ser respondidas por otras herramientas de ciberseguridad o ciberinteligencia convencionales:

- ◇ Un IDS no proporciona percepción situacional, pues ésta va más allá de la simple detección de eventos
- ◇ Un SIEM puede correlacionar eventos, pero no proporciona un Common Operational Picture (COP) como paso previo para generar sensemaking
- ◇ Un sistema de detección de vulnerabilidades (VDS) produce una vista estática de vulnerabilidades, pero no la correlaciona con información de incidentes en tiempo real
- ◇ Las diferentes herramientas de inteligencia (HUMINT, OSINT, SIGINT, TECHINT) generan su propio tipo de conocimiento que debe ser correlacionado

3.1.3 Capacidades clave

Según la OTAN (Multinational Cyber Defence Capability Development), las herramientas de CSA deben incluir capacidades como:

- ◇ Visualizar listas de riesgos actuales, ordenados por impacto y con localización geográfica
- ◇ Generación de informes con diferentes niveles de detalle (drill down/roll up)
- ◇ Vistas jerárquicas personalizadas
- ◇ Seguridad de datos basada en unidad y localización
- ◇ Visualización de dependencias entre activos
- ◇ Agregación de incidentes por región geográfica o por red, con vistas enlazadas
- ◇ Generación y selección de cursos de acción posibles
- ◇ Fusión de datos de múltiples fuentes
- ◇ Gestión de vistas y paneles de control
- ◇ Capacidades avanzadas de visualización y simulación

3.1.4 Requisitos operacionales

El proyecto PANOPTESEC estableció requisitos fundamentales para estas herramientas, que incluyen:

- ◇ **Para fuentes y recolección de datos:** Interfaces estándar y no estándar para la recolección de datos de múltiples fuentes, capacidad de almacenar datos en bruto, recolección de información de configuración de sistemas, información sobre dispositivos, sistemas operativos, aplicaciones, topología de red, etc.
- ◇ **Para correlación de datos:** Motor de correlación de información que traduzca datos de múltiples fuentes a una representación común, identificación de elementos comunes, resolución de conflictos entre elementos informativos, creación de una vista unificada del sistema monitorizado y un modelo de impacto en la misión.
- ◇ **Para visualización:** Sistema que muestre la conciencia situacional de ciberdefensa en tiempo real, representando niveles de riesgo en estado estable y dinámico, impacto anticipado en la misión, detalles sobre sistemas críticos, información sobre topología de red, vulnerabilidades, rutas de ataque, y eventos de seguridad en tiempo real, así como acciones de mitigación propuestas.

3.2 Connection of Cyber Sensors

If we are to connect two systems to exchange data about assets (the same applies to threats, vulnerabilities, etc.) we have to agree on:

- ◇ What is an asset and what features and properties does it have
  - From a format perspective
  - Syntactically
  - Semantically
- ◇ How to exchange that data in an automatic and standard way between any given systems

This leads to the definition of standards for elements characterization and exchange, such as:

- ◇ SCAP - Security Content Automation Protocol
- ◇ Assets
  - ARF - Asset Reporting Format
  - AI - Asset Identification
  - CPE - Common Platform Enumeration
- ◇ Vulnerabilities
  - CVE - Common Vulnerabilities Enumeration
  - CVSS - Common Vulnerability Scoring System
  - CWE - Common Weakness Enumeration
  - OSVDB - Open Source Vulnerability Database
  - CVRF - Common Vulnerability Reporting Framework
- ◇ Threats
  - STIX - Structured Threat Information eXpression
  - TAXII - Trusted Automated eXchange of Indicator Information
  - MAEC - Malware Attribute Enumeration and Characterization
  - CAPEC - Common Attack Pattern Enumeration and Classification
  - CybOX - Cyber Observable eXpression
- ◇ etc…

Tipicamente, la comunicación entre sensores y sistemas se hace con XML (sorprendentemente predominante) o JSON, pero hay también enfoques basados en REST o proprietary APIs. El workflow planea de obtener informaciones de varios tipos de distintas fuentes, integrar las informaciones, correrlarlas, y finalmente generar ciberconciencia situacional.

Enfoques

1. Comunicación directa entre sistemas a través de uno exchange standard, como ARF o STIX
2. Federation/Middleware: un sistema centralizado que recibe datos de los sensores y los distribuye a otros sistemas
3. Subscription: hay un cloud de servidores para enviar datos a través de mecanismos propios.
   Por la mayor parte, estos sistemas son de pago y no open source.
4. Common Collaborative Repository: Se uploadean datos a un repositorio comúm confiable y autorizado, cómo algunos SIEMs, CVE, …

3.3 SIEM

SIEM stands for Security Information and Event Management. It is a system that collects and aggregates log data from many different sources, normalizes the data, correlates it, and then alerts based on rules and heuristics. Tipicamente es un elemento centralizado que gestiona una subred, o parte de una.

- Splunk
- QRadar
- OSSIM
- AlienVault USM (old)

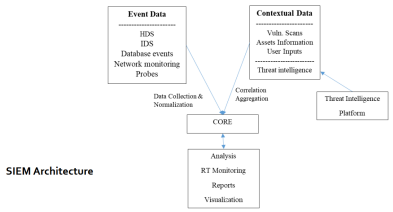


Figure 3.2: SIEM Architecture

3.4 Incident Response Systems

Based on existing ticketing systems, they allow insertion, storing and management of incidents on a central point, aiming at providing response coordination and proper management among interested parties.

They are designed to be integrated with TIPs (Threat Management Platform?) and SIEMs, and to help *Computer Incident Response Team* (CIRT) members carry out incident handling properly, providing workflow management and logs of what happened, when and how about the incident and the response.

Chapter 4

Hybrid Situational Awareness

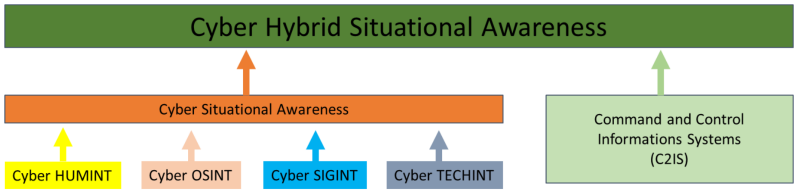


Figure 4.1: Cyber Hybrid Situational Awareness

4.1 Introducción

The cybersecurity decision makers will be able to jointly perceive the situation of physical world and cyber space domains as a unique decision making domain, as any decision taken in one domain affects the other three.

The main ideas to generate hybrid situational awareness are:

- ◇ Events in cyberspace (incidents, attacks…) produce effects in real-kinetic world, tan could affect to course of operations and mission development
- ◇ Events in physical world could produce effects in cyberspace, for instance a physical attack to a command post or to a electric grid infraestructure
- ◇ Cyberspace operations and kinetic operations are dependent
- ◇ Hybrid situational awareness is a fusion of cyber and physical situational awareness

Cada componente fisico tiene un componente ciber, y entonces lo que pasa en el mundo fisico afecta al mundo ciber y viceversa. La Conciencia Situacional híbrida es la fusión de la CS física y la CS ciber.

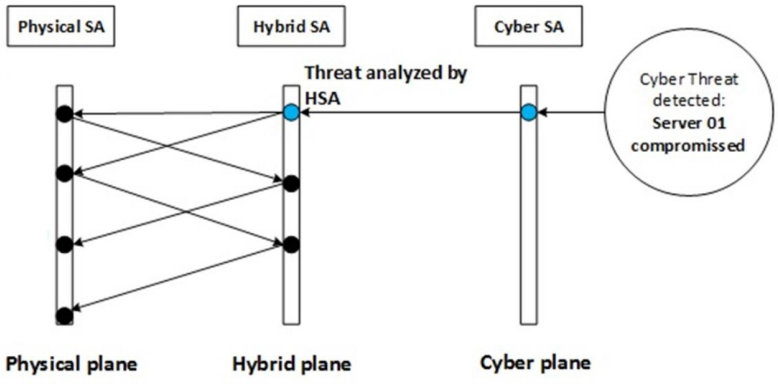


Figure 4.2: Example of Cyber event which produces an effect in the physical world

Part II

Sistemas Ciberfísicos

5 Cyber-Physical Systems **29**
5.1 Introducción . . . 29
5.2 Componenetes de CPSs . . . 29
5.3 Vulnerabilidades . . . 30
5.3.1 Vulnerabilidades más comunes . . . 31
5.4 Vulnerabilities Assessment . . . 31
5.4.1 Intrusion detection . . . 32
5.4.2 Exploits mitigación . . . 32

Chapter 5

Cyber-Physical Systems

5.1 Introducción

Definition 5.1 (CPS) *A cyber-physical system is a system of collaborating computational elements controlling physical entities*

Cyber-Physical System (CPS) is a generic term for a variety of control systems, such as SCADA (Supervisory Control and Data Acquisition) systems, ICSs (Industrial Control Systems), BCSs (Building Control Systems), and the global electrical smart grid

Definition 5.2 (CPS - 2) *A Cyber Physical System (CPS) is a network of interacting and collaborating computational elements controlling physical entities, including sensors, actuators, control processing units, and communication devices*

Definition 5.3 (CPS - 3) *CPS are systems used to monitor and control the physical world*

Definition 5.4 (CPS - 4) *CPS are IT systems that are integrated into physical world application*

Events out of temperatures

Consideremos un escenario en el que se mide la temperatura con un sensor. Para saber si la temperatura es alta o baja, se necesita un umbral, lo que se llama un **valor de referencia**. Esto permite de comparar la temperatura medida con el valor de referencia y tomar una decisión, como por ejemplo generar una alarma si la temperatura es demasiado alta.

5.2 Componenetes de CPSs

CPS tienen vulnerabilidades específicas, porque hay:

- ◇ Issolation asumption
- ◇ Increased connectivity
- ◇ Heterogeneity
- ◇ Long life cycle of components
  Hay softwares que todavía necesitan Windows XP

5.2.0.1 Industrial Control Systems

Sometimes are called SCADA (Supervisory Control and Data Acquisition) systems or DCS (Distributed Control Systems).

El ejemplo más común de ICS son las redes de PLC, por wired o wireless. Tradicionalmente, los PLCs se comunican con un SCADA a través ambos de un protocolo OT (Operational Technologies) de comunicación propietario y de los protocolos IT standard.
Tradicionalmente, la isolación era la mejor defensa para estos sistemas. Patching y updates son un problema, porque los sistemas no pueden ser apagados, y entonces no pueden ser parcheados.

SCADA systems se componen de 4 niveles:

1. Sensors and actuators
2. Distributed controllers, which include programmable logic controllers (PLCs), intelligent electronic devices (IEDs), and other forms of programmable automation controllers (PACs)

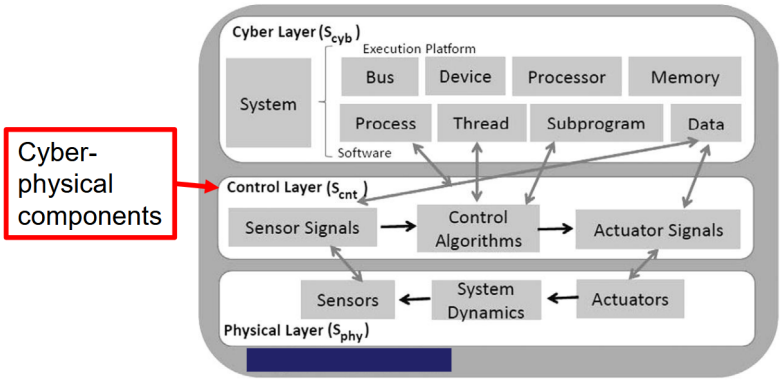


Figure 5.1: Cyberphysical Components

3. Supervisory and control systems, which encompasses systems that store process data, and implements control schemes to manage the lower levels
4. Human machine interfaces (HMIs), which enable the human operators to manage the physical process

Diferencias entre ICS y sistemas IT:

- ◇ Logic execution has a big impact on the physical environtment
- ◇ Edge devices are, at least, so relevant as hosts servers
- ◇ Computation resources of edge devices are usually very limited
- ◇ Safety is the most relevant design constrain
- ◇ Continuous availability and time-critically constrains
- ◇ Hard-Real time vs Soft-Real time vs Best-Effort systems

SCADA network components:

- ◇ Servers and workstations that are used by operators to interact with the field devices segment
- ◇ HMI software-based graphical user interface
- ◇ Monitoring of field devices
- ◇ Field devices data updating
- ◇ Historian systems
- ◇ Back up systems (similar to IT systems)

Field devices components:

- ◇ Programmable Logic Controllers (PLCs)
- ◇ Remote Terminal Units (RTUs)
- ◇ Intelligent Electronic Devices (IEDs)
- ◇ IEDs are microprocessor based devices as sensors, motors (actuators), brakes,lights, etc
- ◇ IEDs are controled by RTUs and PLCs by mean of field buses protocols (as PROFIBUS DP)
- ◇ RTUs monitor IEDs and transmit data to PLCs using ModBUS RTU and DNP3
- ◇ Sometimes, directed to the SCADA network using ModBUS TCP
- ◇ PLCs are control computers, with many types of I/O interfaces

Usual incidents in ICSs:

- ◇ Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation
- ◇ Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life
- ◇ Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects
- ◇ ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects
- ◇ Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment
- ◇ Interference with the operation of safety systems, which could endanger human life

5.3 Vulnerabilidades

1. Vulnerabilities inherent in the CPS product, or platform vulnerabilities
2. Vulnerabilities because of poor network design or configuration, or network equipment vulnerabilities

3. Vulnerabilities caused during the installation, configuration, and maintenance of the CPS, or management vulnerabilities

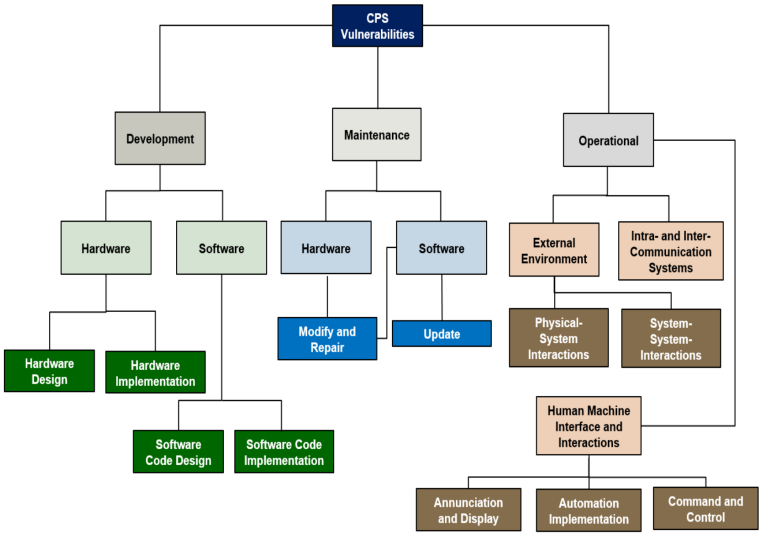


Figure 5.2: CPS Vulnerabilidades taxonomía

A la izquierda de la figura 5.2 hay una lista de vulnerabilidades son vulnerabilidades de plataforma, al centro hay vulnerabilidades de la gestión, y a la derecha vulnerabilidades operacionales.
Cómo hemos dicho antes, tipicamente es difícil actualizar el software para CPSs, esto es el motivo por el cual hay muchas vulnerabilidades relacionadas a la mantenimiento del software.

Las vulnerabilidades más comunes son:

- ◇ Improper Input Validation / Validación incorrecta de las entradas
- ◇ Permissions, Privileges and Access Control / Permisos, privilegios y control de acceso
- ◇ Improper Authentication / Autenticación incorrecta
- ◇ Insufficient Verification of Data Authenticity / Verificación insuficiente de la autenticidad de los datos
- ◇ Poor Code Quality / Código de baja calidad
- ◇ Security Configuration and Maintenance / Configuración y mantenimiento de la seguridad
- ◇ Credentials Management / Gestión de credenciales

5.3.1 Vulnerabilidades más comunes

La más explotada vulnerabilidad en CPSs es **Buffer Overflow**, que es tipicamente permitida por la falta de validación de las entradas: los programadores suelen tener en cuenta lo que debería ocurrir y lo que podría ocurrir por error, pero no todas las posibilidades maliciosas.

Malas prácticas de código permiten a los atacantes suministrar datos inesperados y modificar así la ejecución del programa. Esta vulnerabilidad se llama **Lack of Bounds Checking**.

Cross-Site scripting vulnerabilidades pueden ser explotadas para muchos tipos de ataques, como el **Cross-Site Request Forgery** (CSRF), que permite a un atacante ejecutar comandos en el contexto de un usuario autenticado. En general, el Cross-Site Scripting permite **Code Injection**.

5.4 Vulnerabilities Assessment

Para los CPS, los objetivos de seguridad están en orden inverso de prioridad, siendo la disponibilidad considerada la más importante, en lugar de la confidencialidad. El personal de la industria a menudo usa el término ”seguridad” para referirse a la disponibilidad y fiabilidad del sistema.

Nada debe hacerse en una red CPS activa que pueda interferir o interrumpir las operaciones críticas del sistema. En el entorno CPS, los objetivos de seguridad del mundo IT son reemplazados por la salud y seguridad humana, la disponibilidad del sistema, y la puntualidad e integridad de los datos. Esta es la principal diferencia entre las evaluaciones de seguridad de CPS y de IT.

Esta diferencia también se aplica a las estrategias de mitigación. Ninguna solución de ciberseguridad puede implementarse en la red CPS si interfiere con la respuesta del sistema. El equipo de evaluación cibernética debe trabajar

con el personal de la industria y los proveedores para realizar una evaluación efectiva sin comprometer la seguridad, disponibilidad o integridad del CPS.

CPS Vulnerabilities Assessment Execution Phases:

1. **Reconnaissance** - The first part of a cyber security assessment is to identify a target to attack.
2. **Exploration** - Once a target has been identified, the assessment team attacks the system
3. **Exploit development** - Once a problem has been identified, the assessment team may optionally develop an exploit for the vulnerability.
   All these phases have specific aspects in CPS vulnerabilities assessment

5.4.1 Intrusion detection

HIDS no se utilizan mucho en ICSs, porque —tipicamente— no se puede instalar software sobre CPS components. Entonces, se utilizan **Network IDS** basados sobre **anomalias**. La detección por firmas (signature-based) tiene buena precisión para IT sistemas, pero no lo es para ICSs, porque …// TODO

La detección por firmas (signature-based) tiene buena precisión para IT sistemas, pero no lo es para ICSs, porque tiene que depender de firmas conocidas y actualizadas, mientras que los protocolos y comportamientos en entornos ICS son muy específicos y a menudo propietarios.

Lateral Movements son muy comunes en ICSs, porque los atacantes pueden moverse lateralmente a través de la red para obtener acceso a otros sistemas, y entonces, **honeypots** son una defensa muy eficaz para detectar y monitorear estos movimientos. Los honeypots simulan componentes legítimos del sistema, atrayendo a los atacantes y permitiendo analizar sus técnicas sin comprometer los sistemas reales.

La segmentación de la red, junto con controles de acceso estrictos entre zonas, también es fundamental para limitar la capacidad de los atacantes de moverse lateralmente una vez que han comprometido un punto de entrada inicial en la red ICS.

5.4.2 Exploits mitigación

En general es muy difícil mitigar los exploits en CPSs, porque no se pueden aplicar parches a los sistemas.