Data and Network Security

(Master Degree in Computer Science and Cybersecurity)

Lecture 1

SAPIENZA
UNIVERSITÀ DI ROMA

What is this course about?

This course provides a comprehensive introduction to fundamental concepts, principles, and practices in cybersecurity focusing into emerging trends and future directions in the field.

https://sites.google.com/di.uniroma1.it/dns-sapienza/home

What is this course about?

This course provides a comprehensive introduction to fundamental concepts, principles, and practices in cybersecurity focusing into emerging trends and future directions in the field.

This course has a research oriented focus, and as such will treat various novel research works in the domain, and will also stimulate the students to carry out independent research and share knowledge with classmates.

Class hours

- **Monday**: 11:00-13:00 - Aula 201, D-Building
  - Start at 11:15
  - End at 12:45

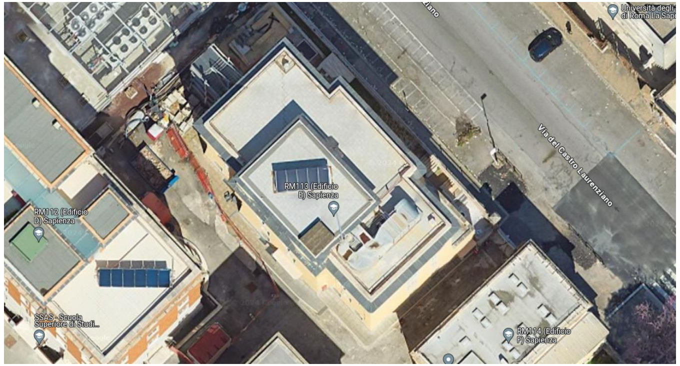
- **Thursday**: 08:00-11:00 - Aula 1L
  - Start at 08:15
    - Usually 15 min break (09:15-09:30)
  - End at 10:45

Office Hours

Monday: 14:00-16:00

Thursday: 13:00-17:00

***Send an email [hitaj.d@di.uniroma1.it] at least one day before to check availability.**


Università degli
di Roma La Sap
Via del Castro Laurenziano
RM113 (Edificio E) Sapienza
RM112 (Edificio D) Sapienza
SSAS - Scuola Superiore di Studi...
RM114 (Edificio F) Sapienza

Viale Regina Elena 295
E-building
First Floor, Room 101

Evaluation and Examination

The exam consists of an oral presentation, and in submitting a written report.

Evaluation and Examination

Each student (or group of st. max 2) will give a seminar on a topic of their choice from a list of possible topics, and answer questions from the other students in the classroom.

- Students' participation in the “questions & answers” phase will be considered in the final grade.

Evaluation and Examination

Students also have to deliver a report describing how and in what measure they intend to solve a cybersecurity problem, related to the topic of their seminar.

Evaluation and Examination

The final grade is calculated as follows:

- 45% Literature Analysis and active participation
- 45% Written research report
- 10% Active participation to Question & Answer section.

Evaluation and Examination

The final grade is calculated as follows:

- 45% Literature Analysis and active participation
- 45% Written research report
- 10% Active participation to Question & Answer section.

***If for any reason students do not turn in most of the required above tests, then those students will be required to take an oral exam on the entire course programme.**

The weight of this final oral exam = 100%.

Announcements and General Information

We will use Google Classroom to share lectures and general information.

https://forms.gle/pmJXszCseXoDycbG6

Cybersecurity / Data and Network Security?

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, alteration, or destruction. It encompasses various technologies, processes, and practices designed to safeguard information assets against a wide range of cyber threats.

Importance of DNS

- Data and Network security

Data

- **Data** and Network security

Data

- **Data** and Network security

- **Data is the lifeblood of businesses and organizations.**

Data

- **Data** and Network security

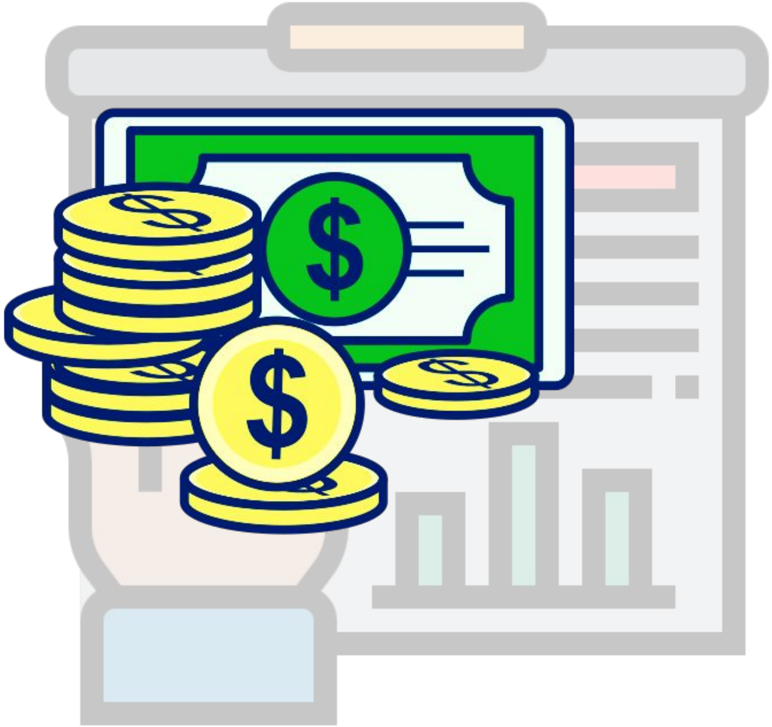
- **Data is the lifeblood of businesses and organizations.**
  - **Inventory management**
  - **Competitive adv.**
  - **Market share inc.**
  - **product /service improvement**
  - **…**

Data

- Data and Network security

- Data is the lifeblood of businesses and organizations.
  - Inventory management
  - Competitive adv.
  - Market share inc.
  - product /service improvement
  - …

Data =



Data loss/damage

- Financial loss
- Reputation damage
- Legal ramifications

Data loss/damage

- **Financial loss**
- Reputation damage
- Legal ramifications

Data loss/damage

- **Financial loss:**
  - theft of sensitive information, disruption of business operations, and remediation costs.

Data loss/damage

- Financial loss
- **Reputation damage**
- Legal ramifications

Data loss/damage

- **Reputation Damage:**
  - entities/organizations failing to protect data, risk damaging their reputation and losing the trust of customers, partners, and stakeholders

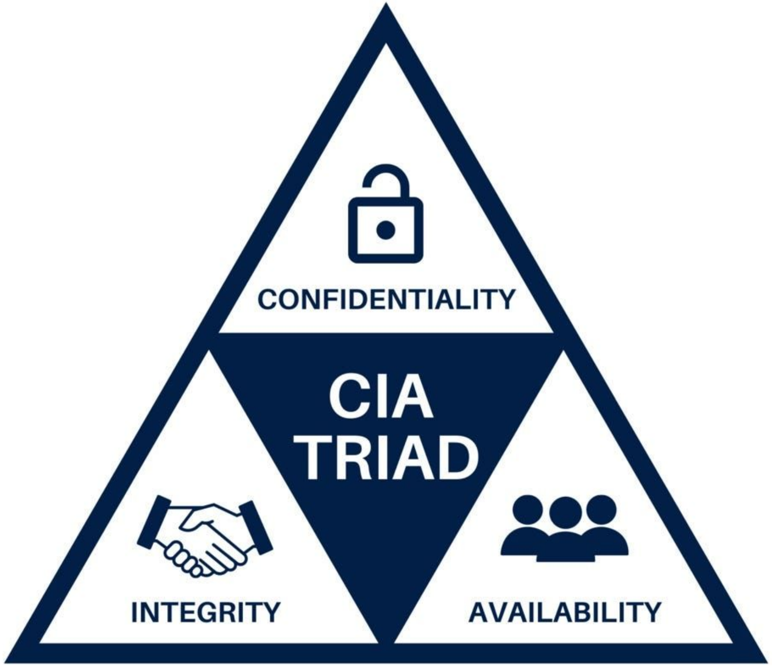
Data loss/damage

- Financial loss
- Reputation damage
- **Legal ramifications**

Data loss/damage

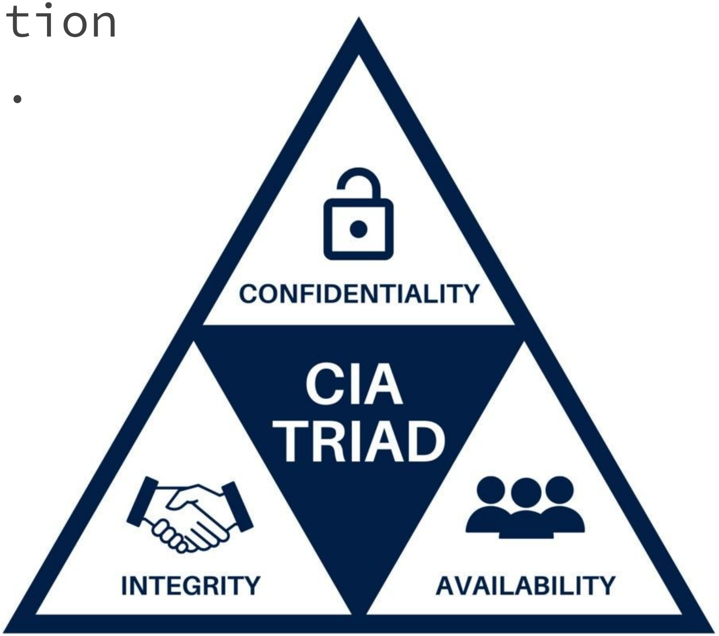
- **Legal ramification:**
  - Regulatory bodies impose strict requirements for data protection and privacy. Failure to comply with these regulations can lead to fines, lawsuits, and other legal consequences.

The goals of DNS



Confidentiality

Protecting sensitive information from unauthorized disclosure.



Confidentiality - measures to take

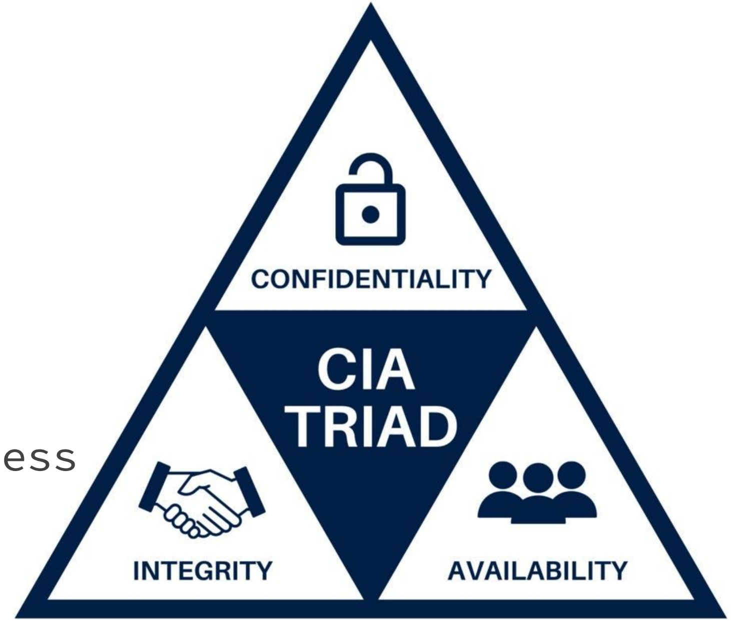
Protecting sensitive information from unauthorized disclosure.

- Encryption
- access controls
- data classification policies

CONFIDENTIALITY
CIA TRIAD
INTEGRITY
AVAILABILITY

Integrity

Ensuring the accuracy and trustworthiness of data by preventing unauthorized modifications



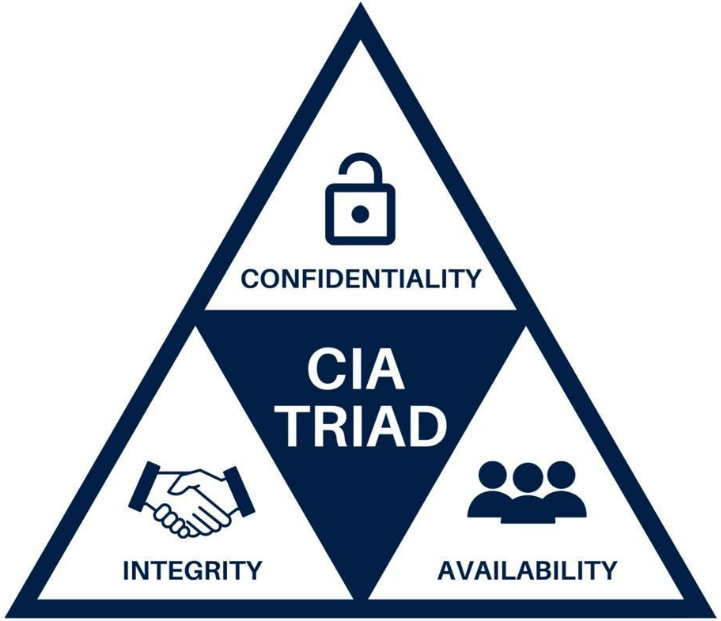
Integrity - measures to take

- Data validation
- Checksums
- Digital signatures
- Access controls

Ensuring the accuracy and trustworthiness of data by preventing unauthorized modifications

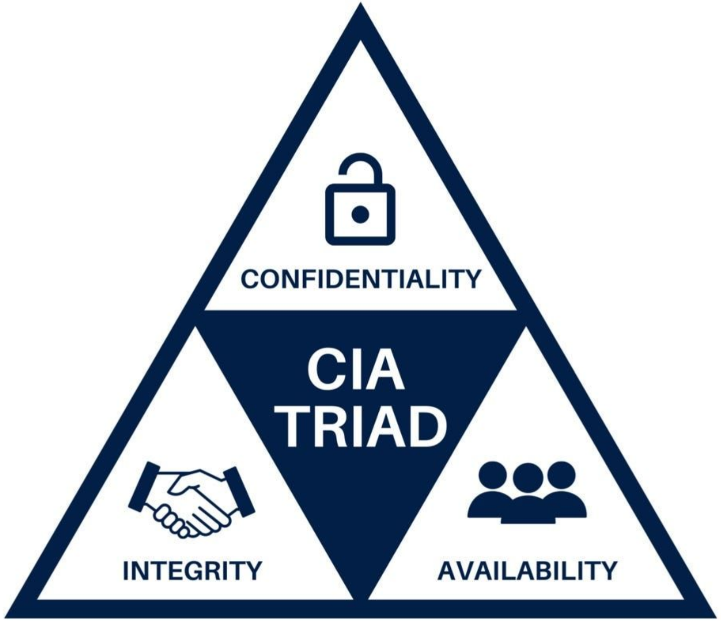
CONFIDENTIALITY
CIA
TRIAD
INTEGRITY
AVAILABILITY

Availability



Ensuring that data and resources are available and accessible to authorized users when needed.

Availability - measures to take

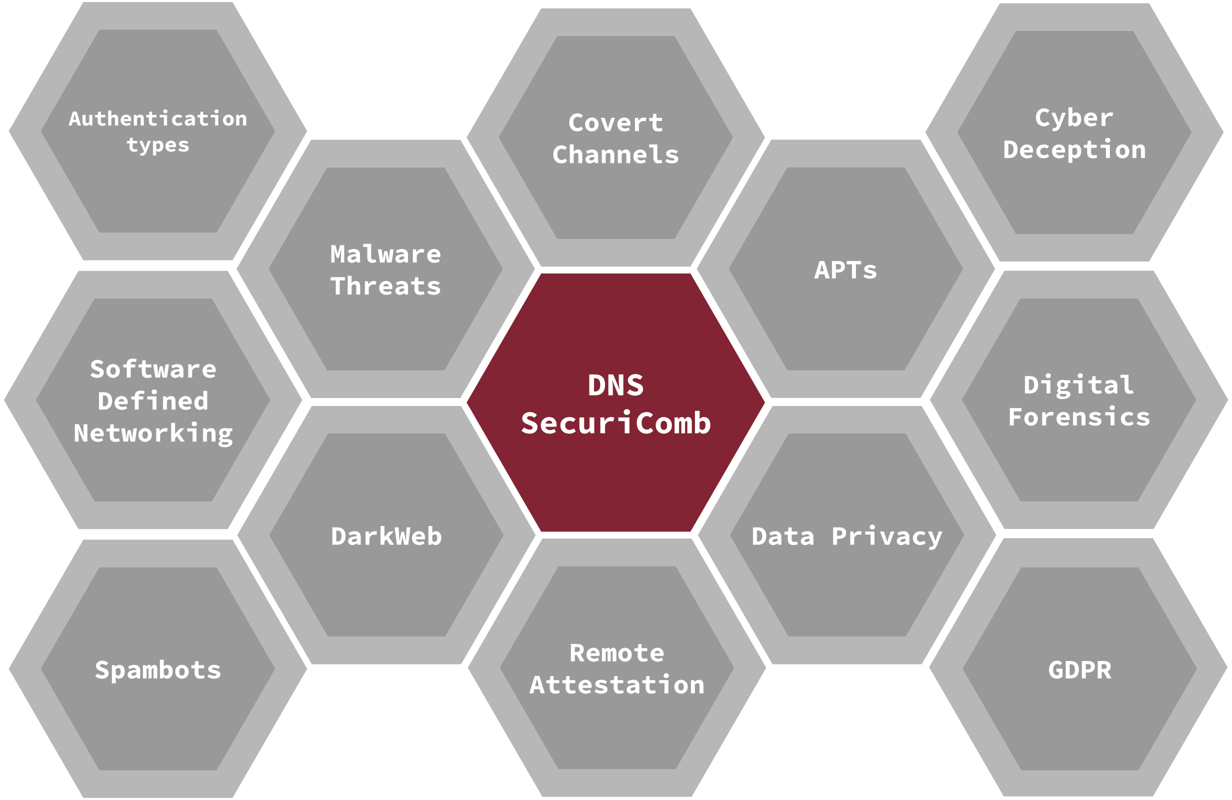


- Redundancy
- Fault tolerance
- Disaster recovery planning
- Denial of service protection

Ensuring that data and resources are available and accessible to authorized users when needed.

Course Syllabus

SecuriComb



Authentication types

Malware Threats

Covert Channels

APTs

Cyber Deception

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

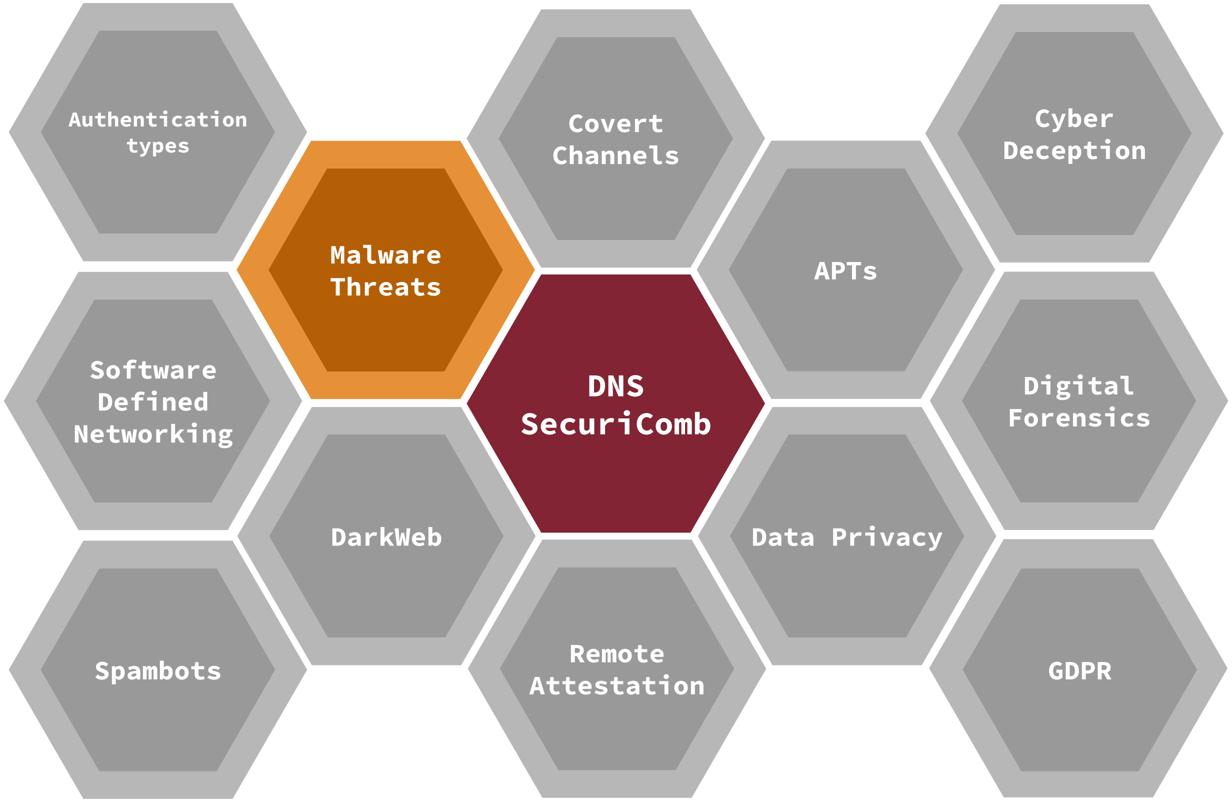
Data Privacy

Spambots

Remote Attestation

GDPR

SecuriComb



Authentication types

Malware Threats

Covert Channels

APTs

Cyber Deception

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

Data Privacy

Spambots

Remote Attestation

GDPR

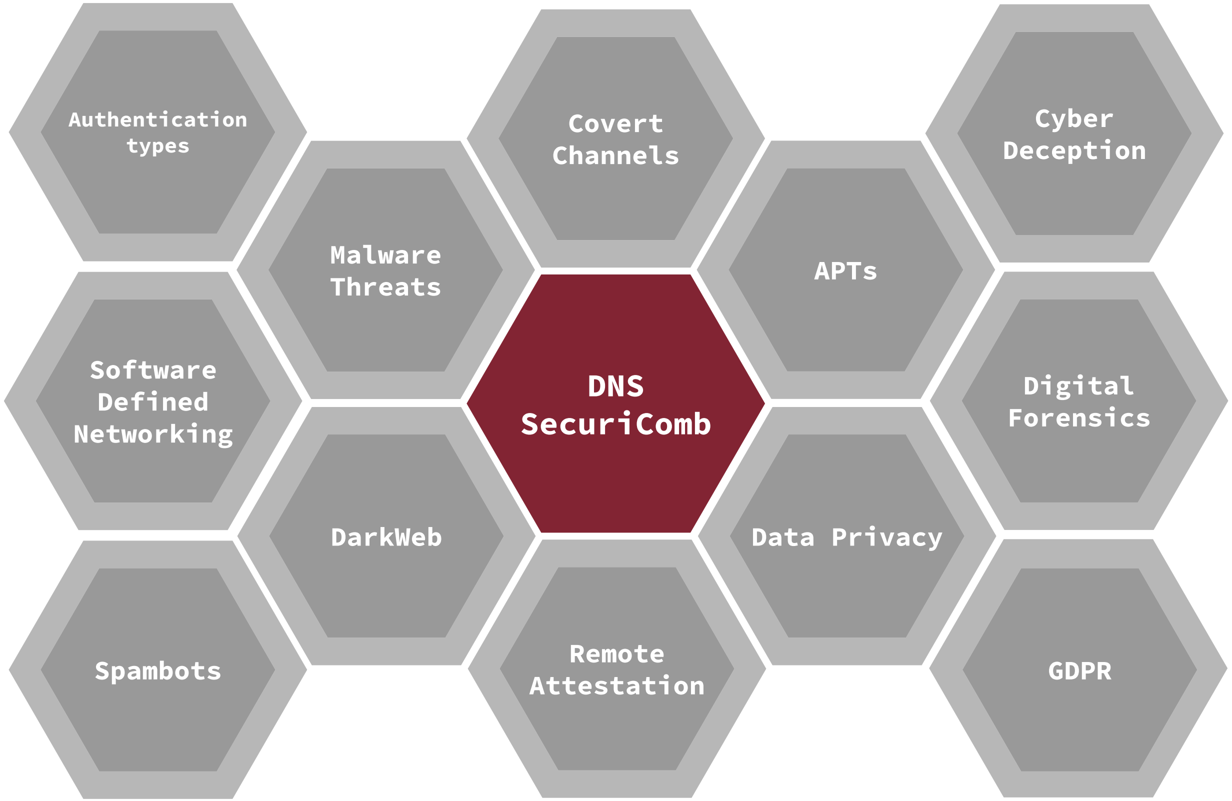
Malware Threats

Malware:

Type of software program or code specifically designed to infiltrate, damage, disrupt, or gain unauthorized access to computer systems, networks, or devices, often with malicious intent.

Broad category that encompasses various types of malicious programs, each with its own specific behavior and objectives.

SecuriComb



Authentication types

Covert Channels

Cyber Deception

Malware Threats

APTs

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

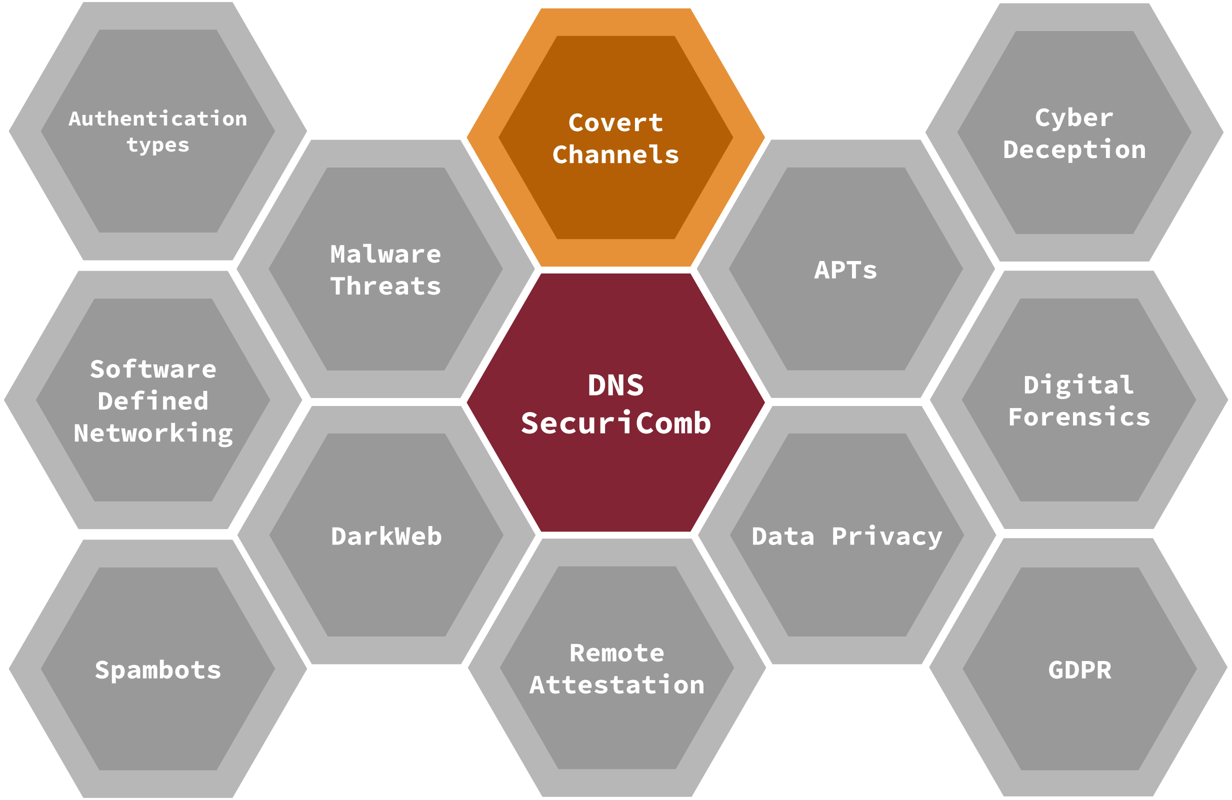
Data Privacy

Spambots

Remote Attestation

GDPR

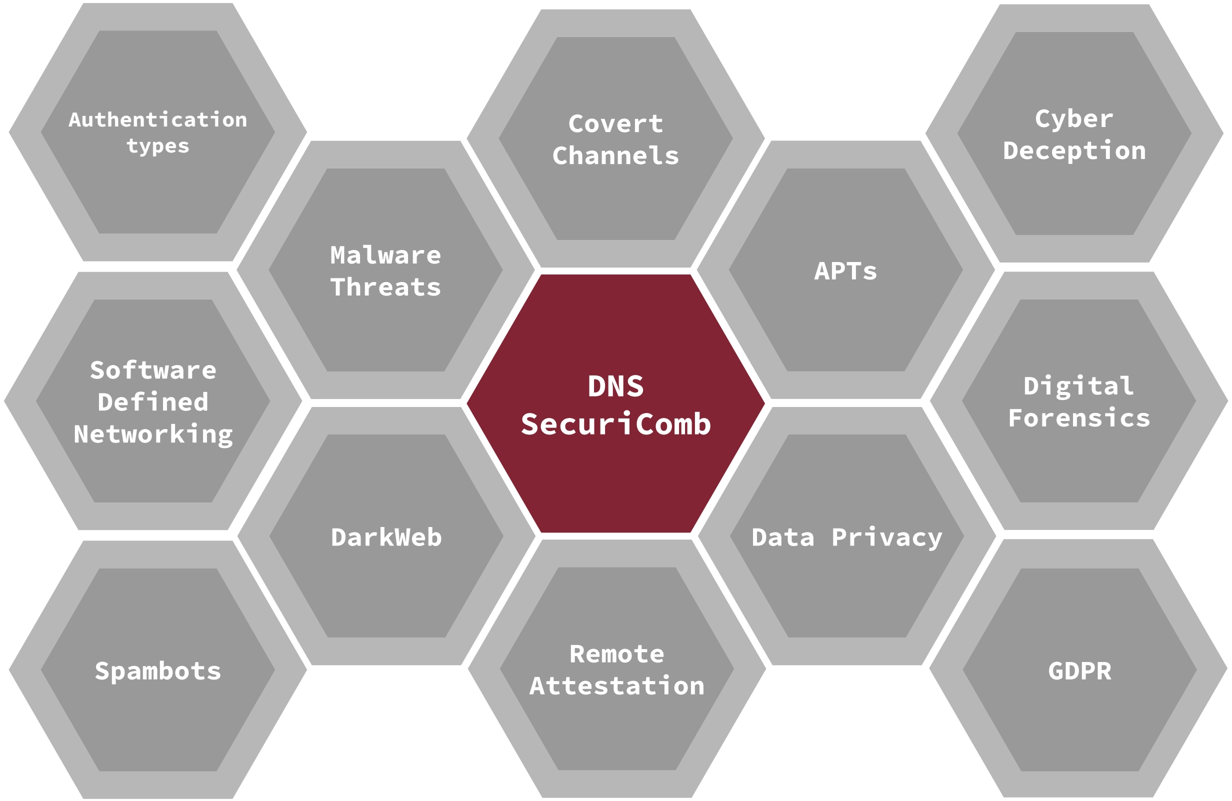
SecuriComb


Authentication types
Covert Channels
Cyber Deception
Malware Threats
APTs
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

Covert Channel

Indirect communication channel between unauthorized parties that violates some security policy by using shared resources in a way in which these resources are not initially designed, bypassing mechanisms that do not permit direct communication between these unauthorized parties in the process.

SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

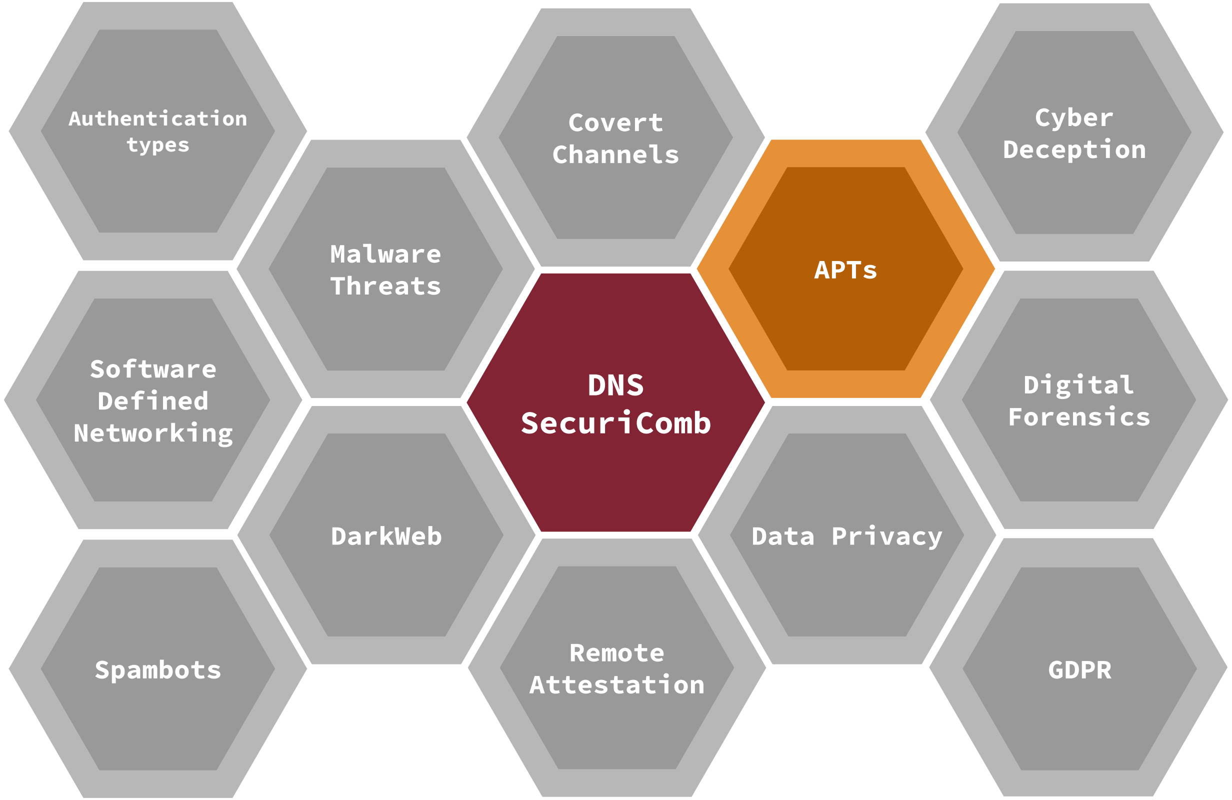
Data Privacy

Cyber Deception

Digital Forensics

GDPR

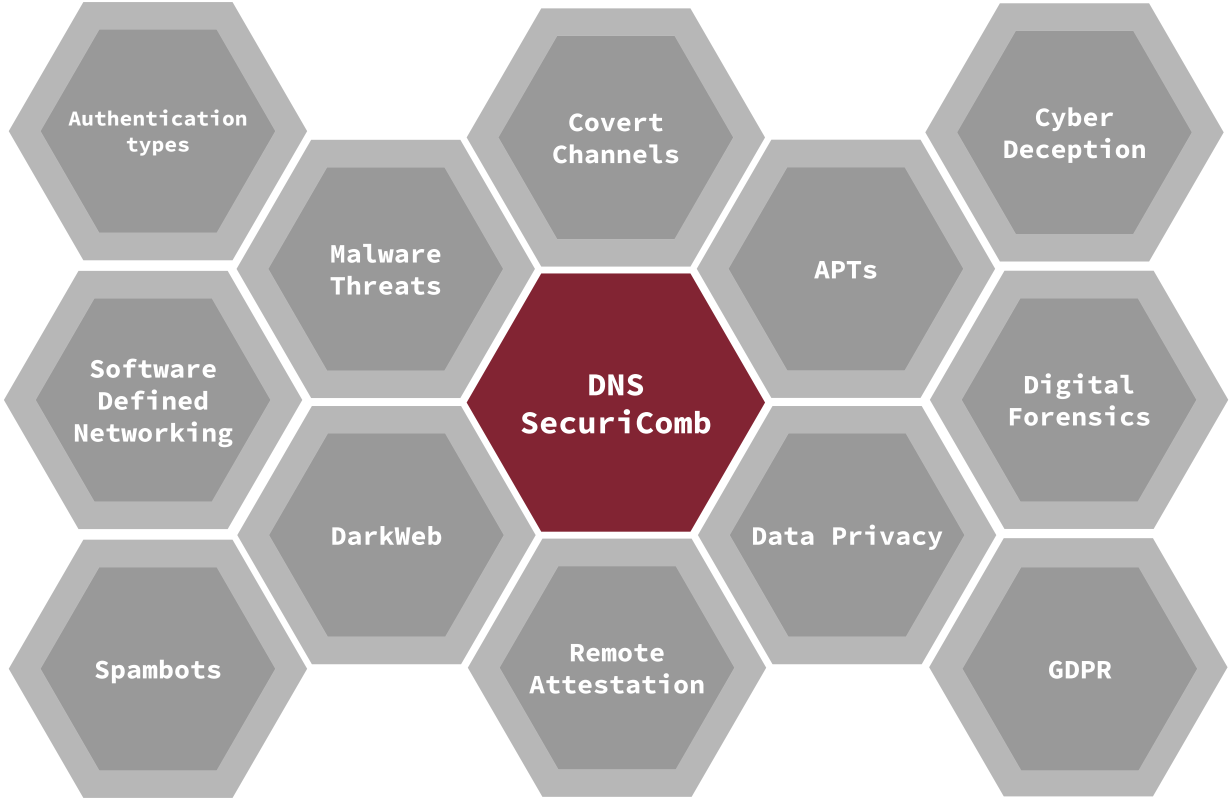
SecuriComb


Authentication types
Covert Channels
Cyber Deception
Malware Threats
APTs
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

Advanced Persistent Threats

Sophisticated, targeted cyber attack in which an unauthorized entity gains access to a network and remains undetected for an extended period.

SecuriComb



Authentication types

Covert Channels

Cyber Deception

Malware Threats

APTs

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

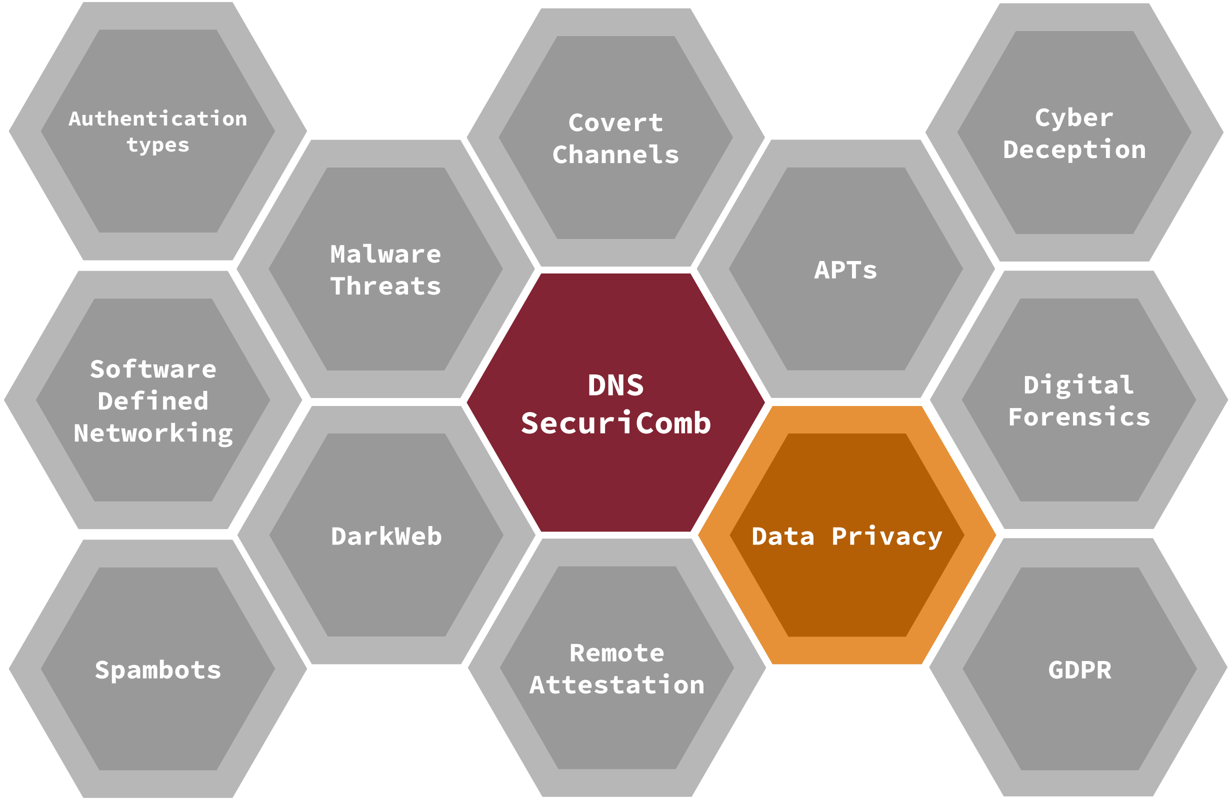
Data Privacy

Spambots

Remote Attestation

GDPR

SecuriComb



Authentication types

Covert Channels

Cyber Deception

Malware Threats

APTs

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

Data Privacy

Spambots

Remote Attestation

GDPR

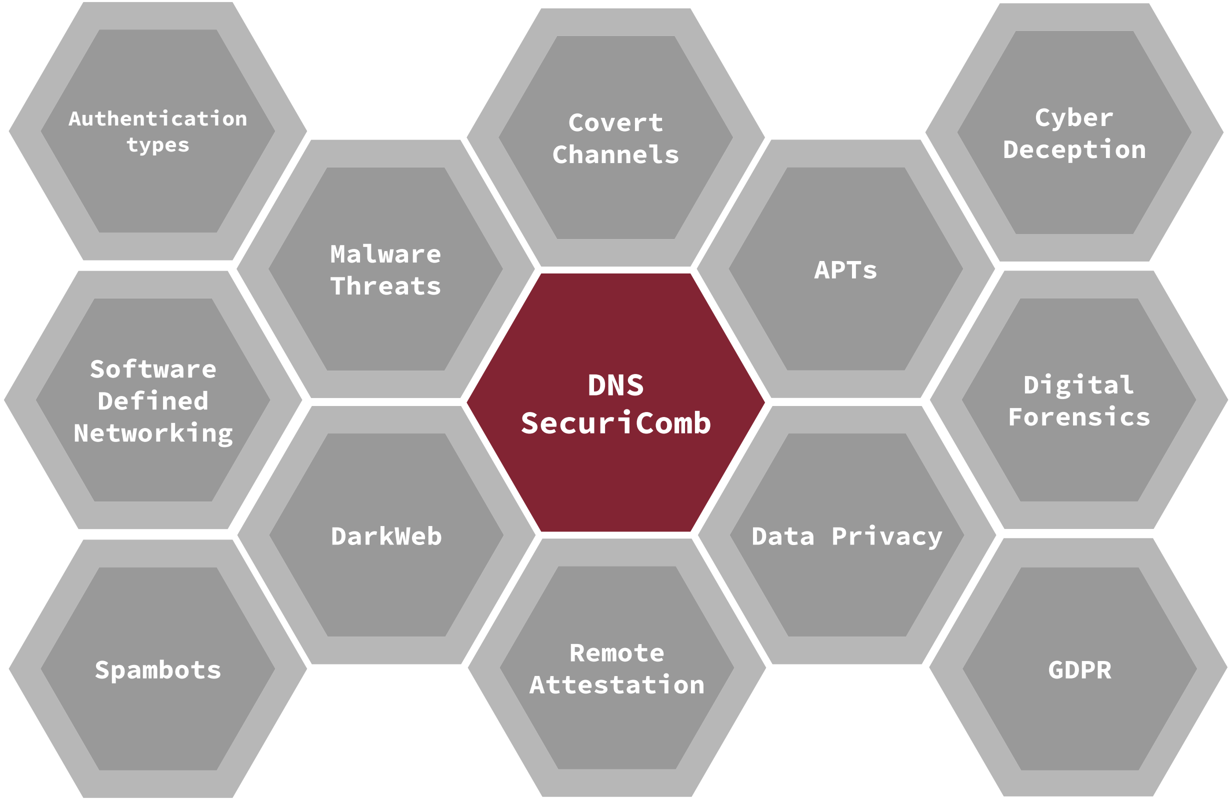
Sensitive properties of a dataset

DATASET

- Demographic Information:
  - Age, gender, ethnicity, income level.
- Behavioral Patterns:
  - Shopping habits, browsing history, social interactions.
- Personal Preferences:
  - Political affiliations, health conditions, lifestyle choices.

Disclosure of such properties can lead to privacy breaches, discrimination, or manipulation of individuals.

SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

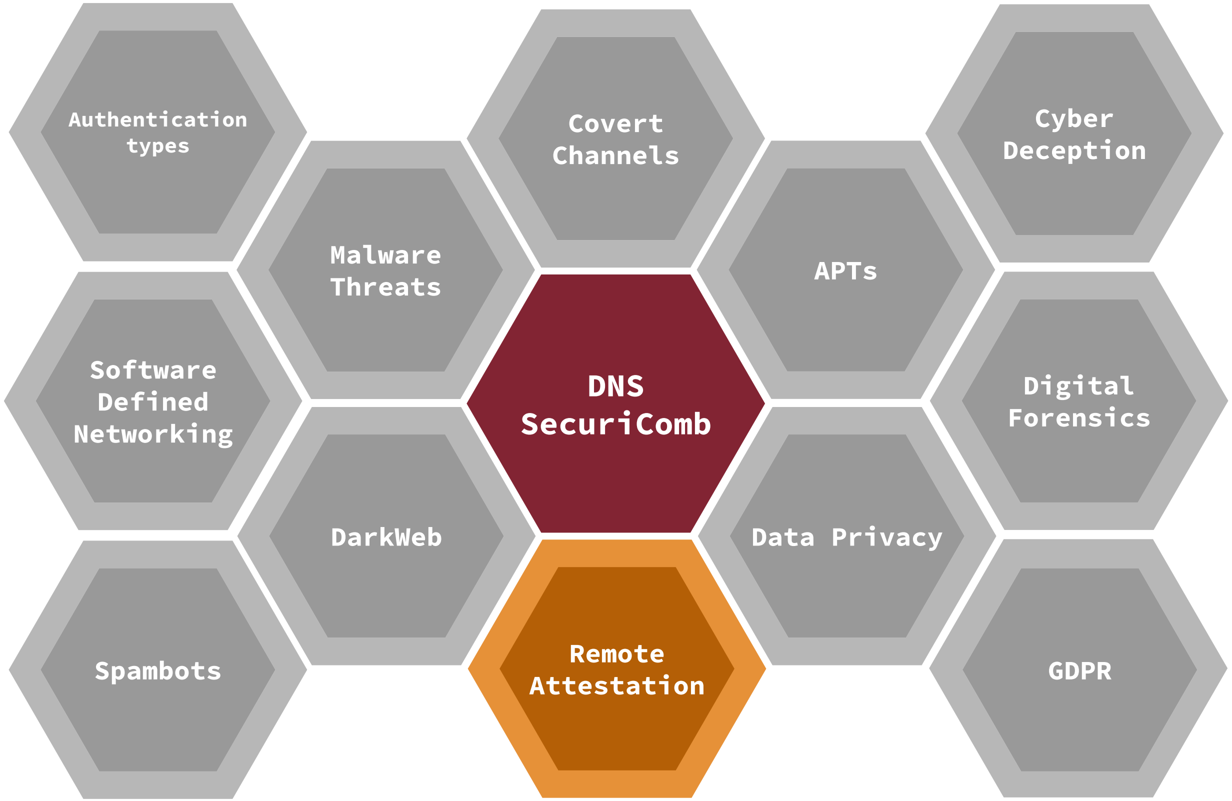
Data Privacy

Cyber Deception

Digital Forensics

GDPR

SecuriComb



Authentication types

Covert Channels

Cyber Deception

Malware Threats

APTs

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

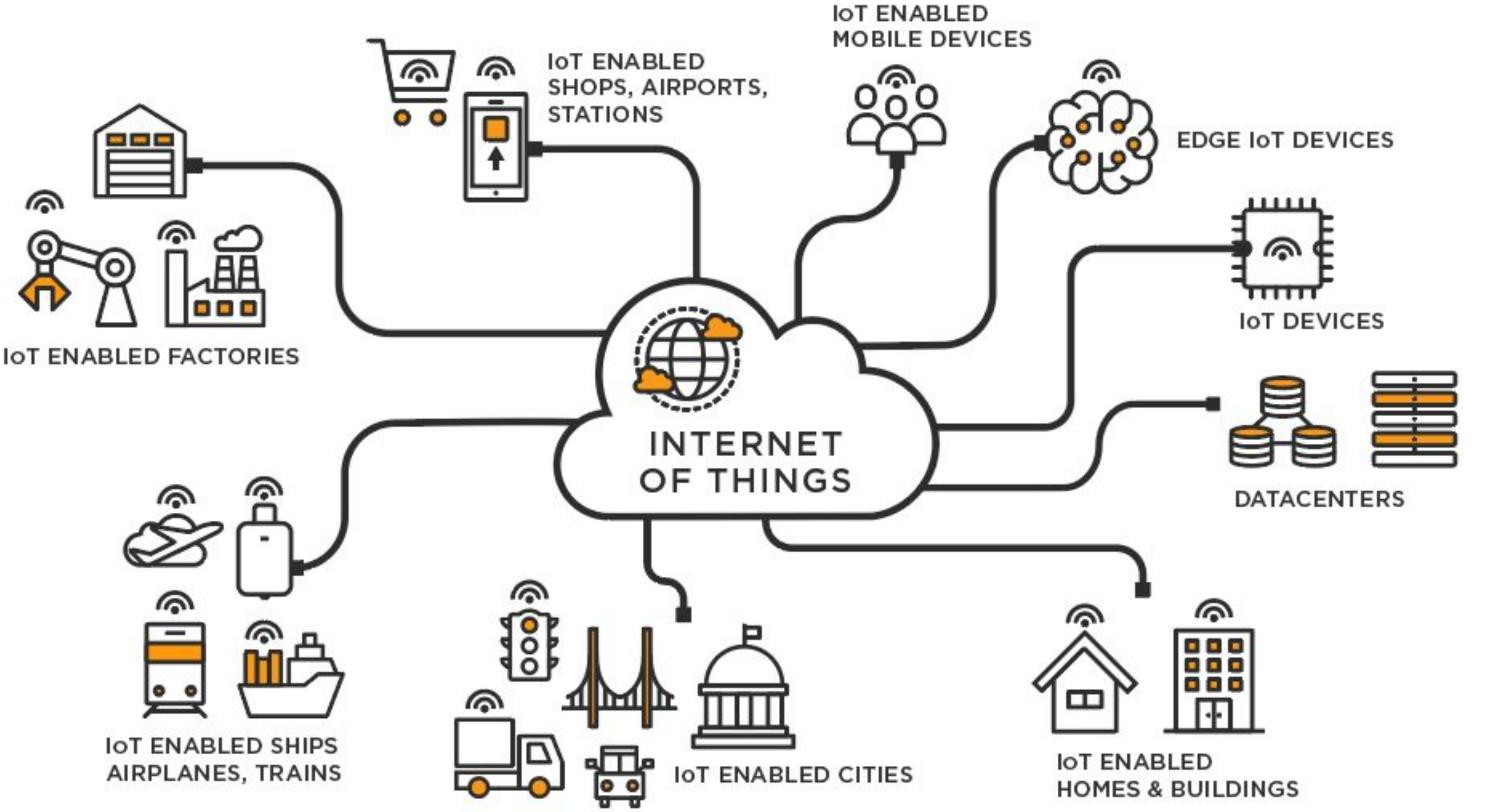
Data Privacy

Spambots

Remote Attestation

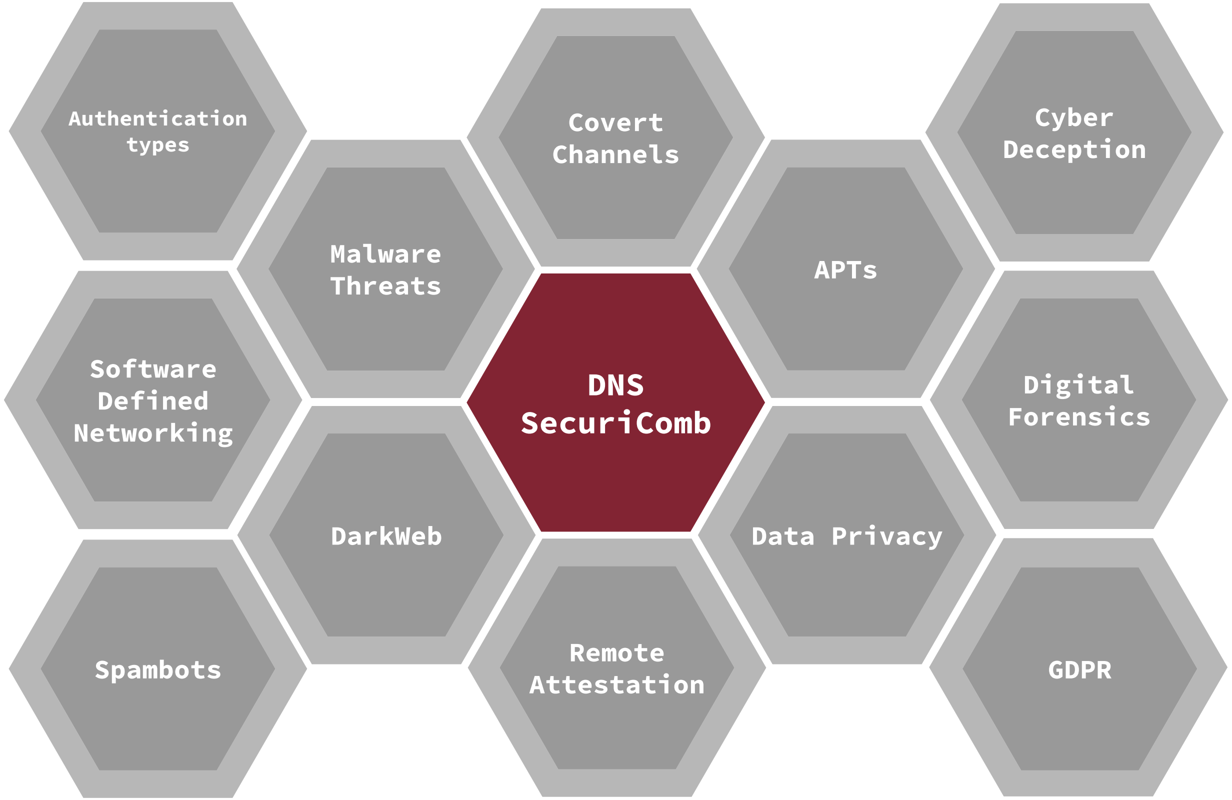
GDPR

Internet of Things (IoT)

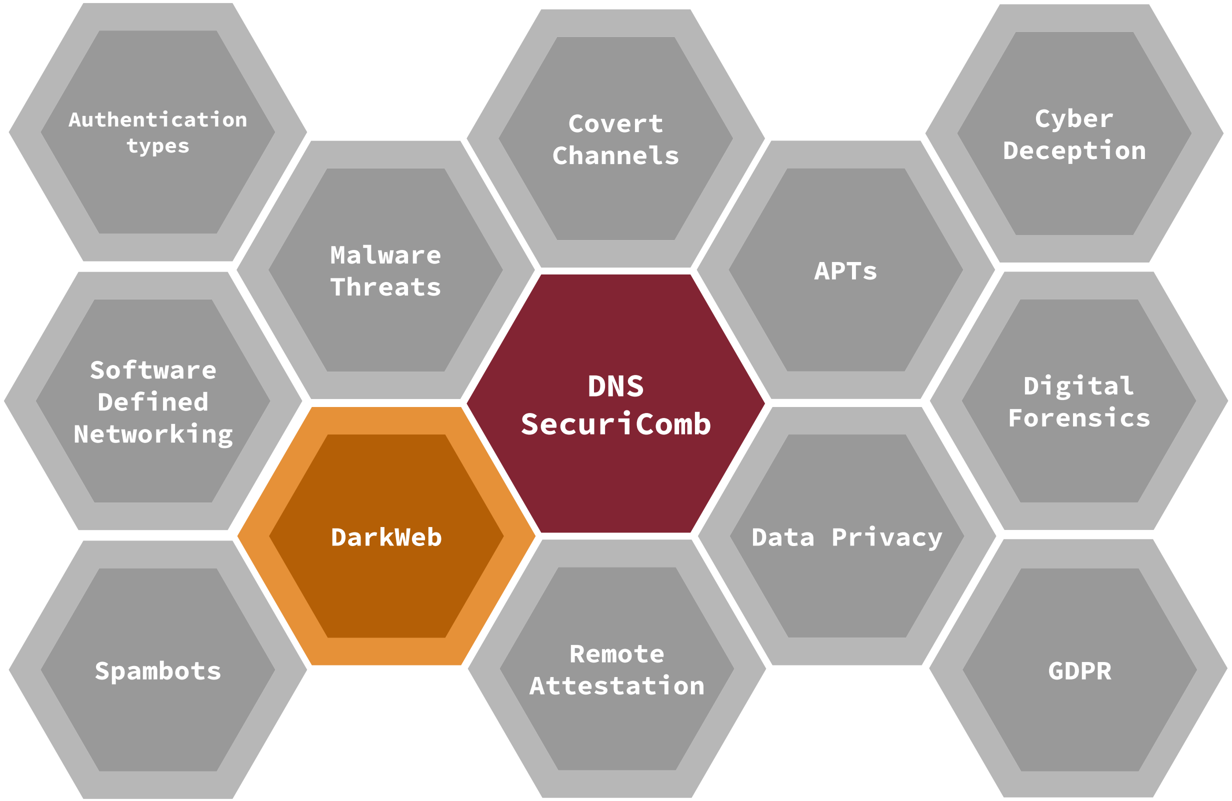


INTERNET OF THINGS
IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
DATACENTERS
IoT ENABLED FACTORIES
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

SecuriComb


Authentication types
Covert Channels
Cyber Deception
Malware Threats
APTs
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

Data Privacy

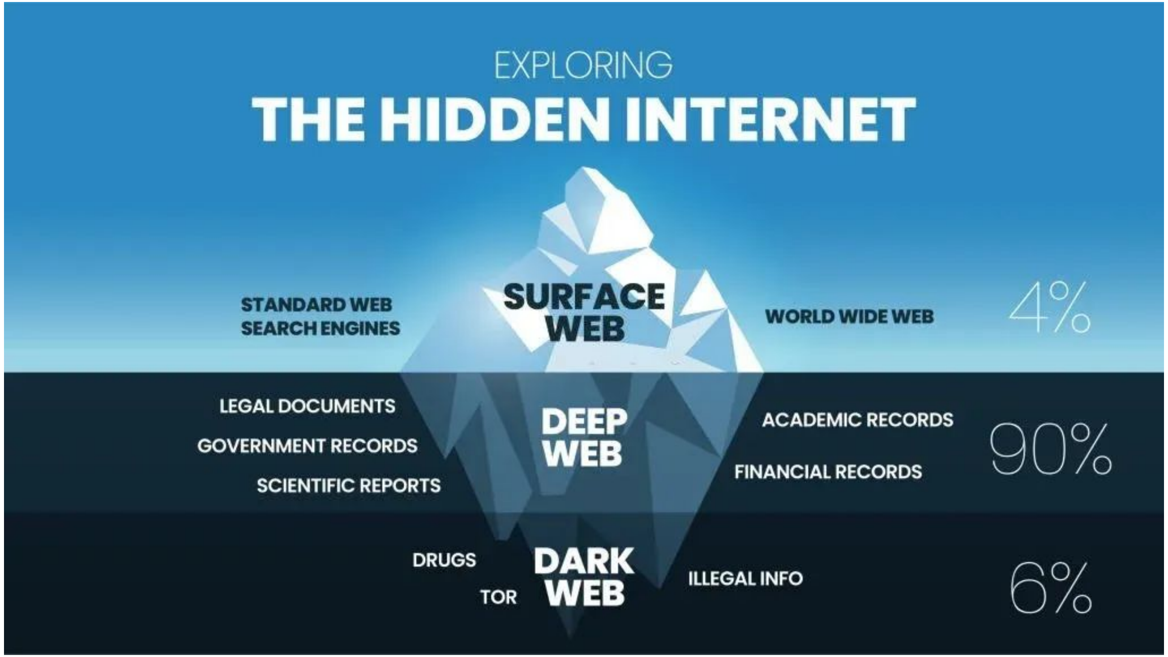
Cyber Deception

Digital Forensics

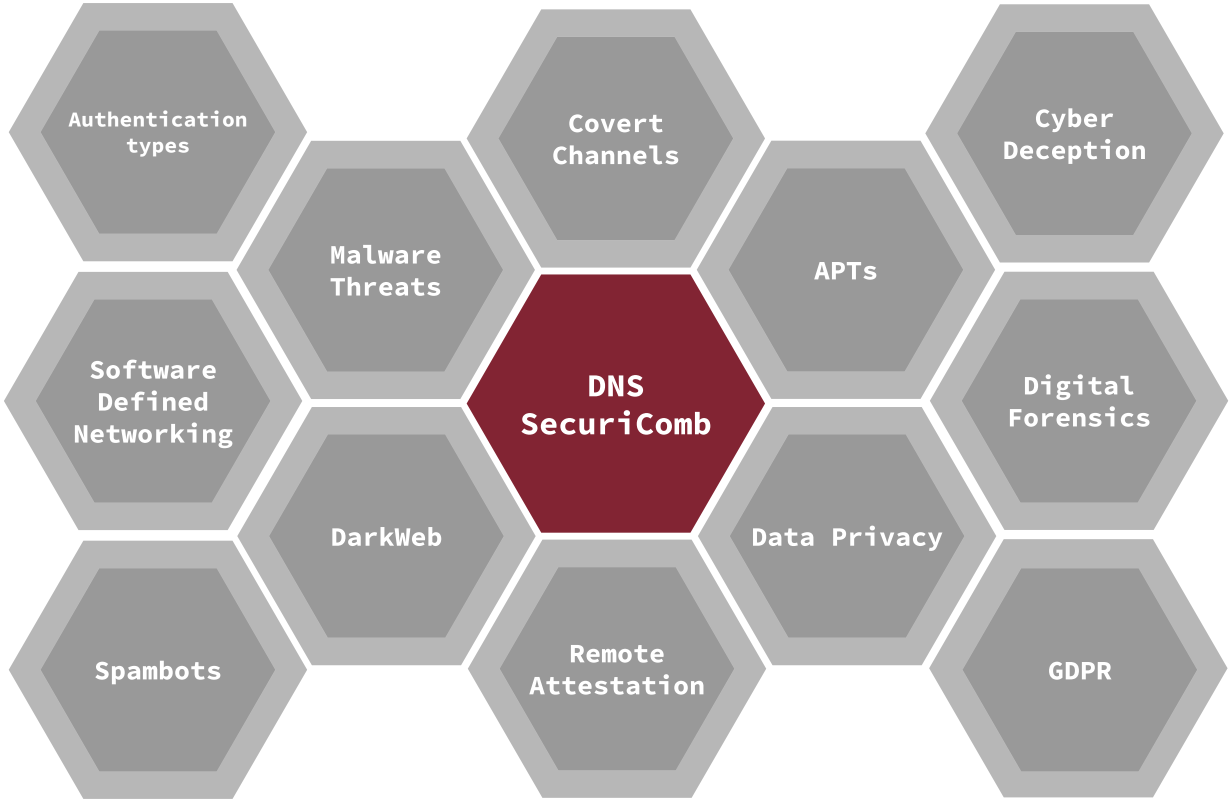
GDPR

Layers of the web

- The surface web
- The deep web
- The dark web



SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

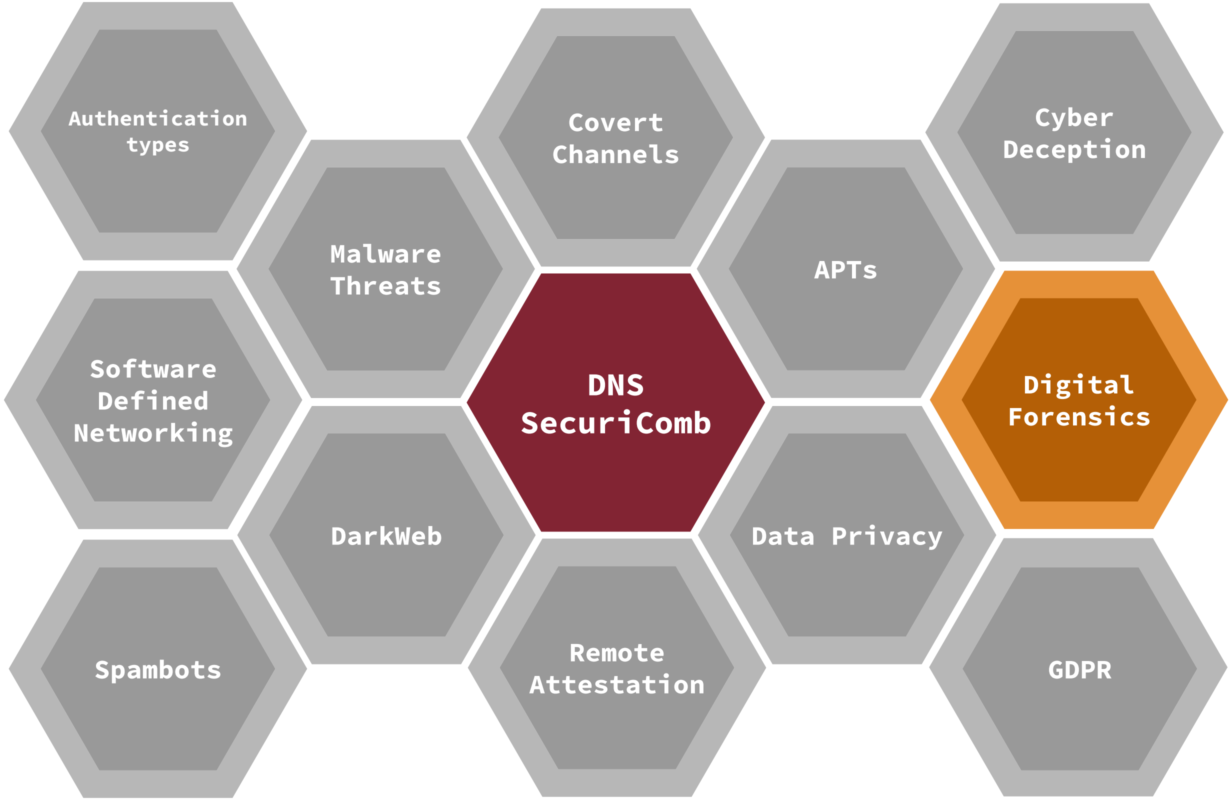
Data Privacy

Cyber Deception

Digital Forensics

GDPR

SecuriComb

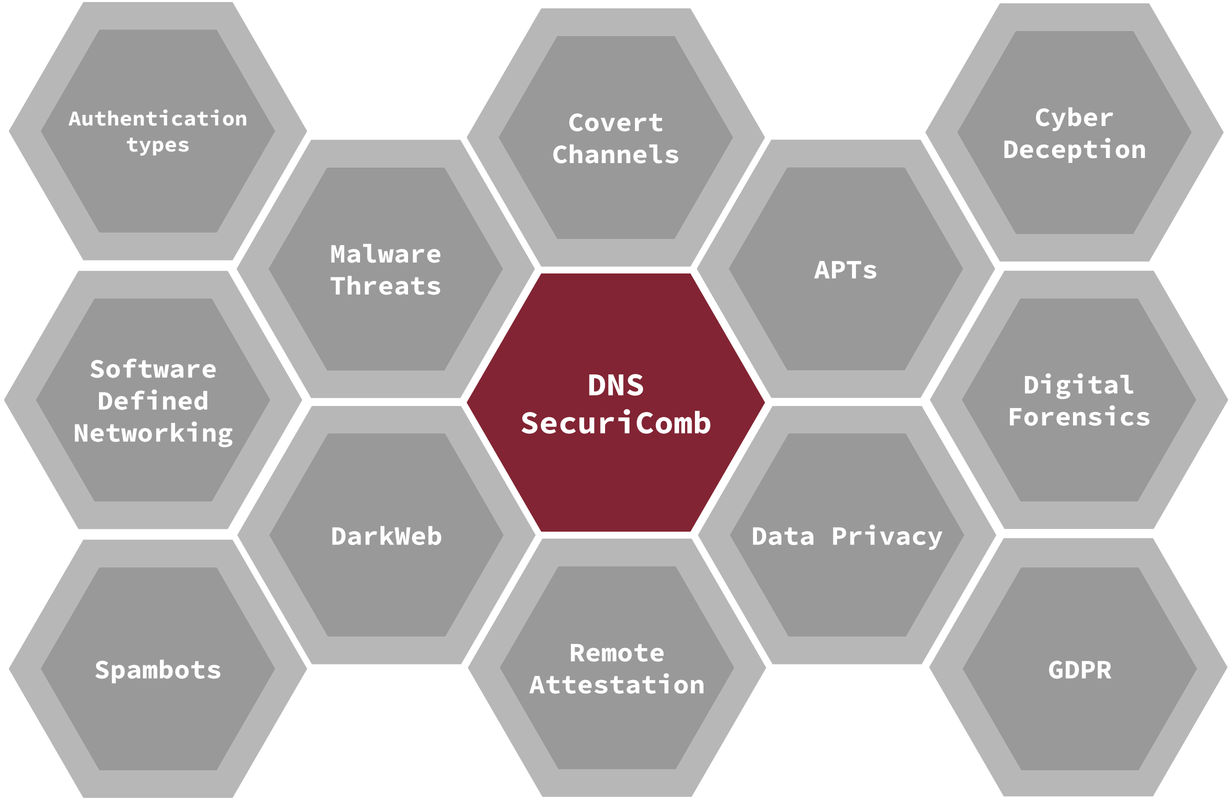

Authentication types
Malware Threats
Software Defined Networking
Spambots
DarkWeb
Covert Channels
DNS SecuriComb
Remote Attestation
APTs
Data Privacy
Cyber Deception
Digital Forensics
GDPR

Digital Forensics

Definition: branch of forensic science that deals with the identification, preservation, examination, analysis, and presentation of digital evidence derived from electronic devices and digital media.

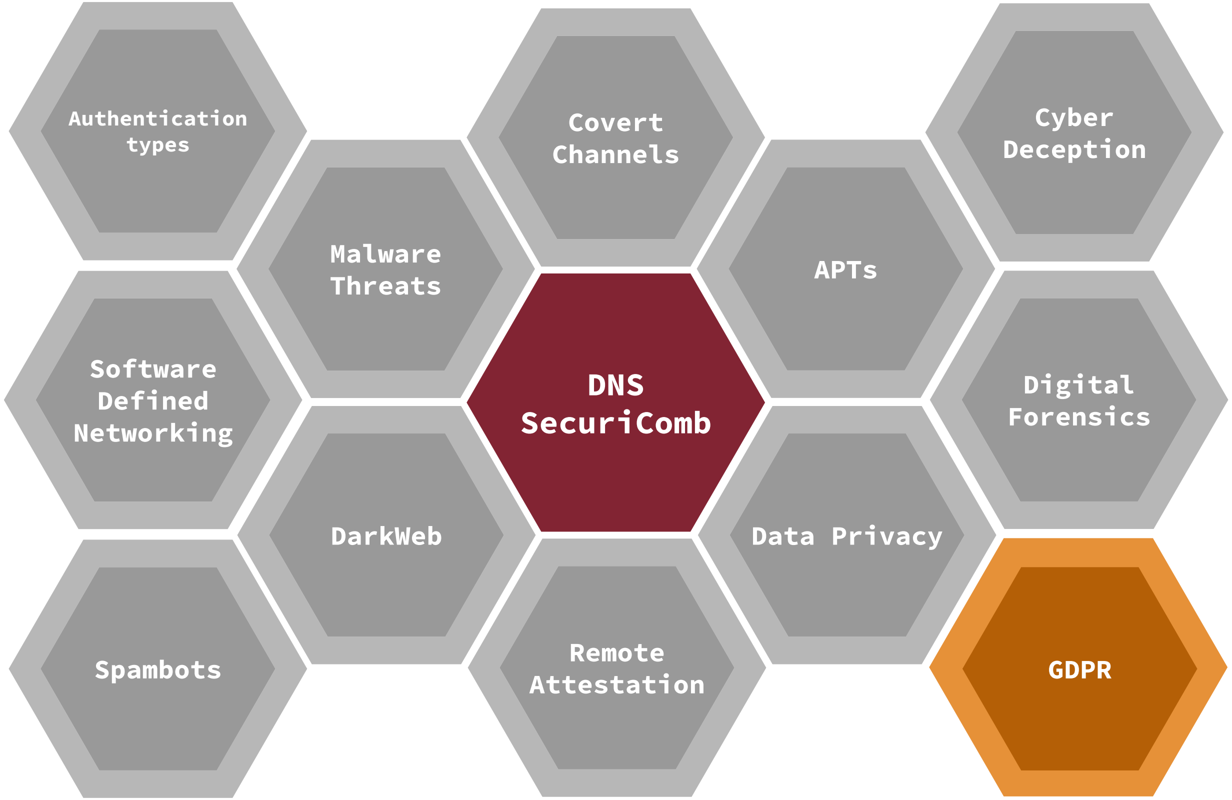
Goal: To explain current state of a digital artifact

SecuriComb



Authentication types
Covert Channels
Cyber Deception
Malware Threats
APTs
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

SecuriComb



Authentication types

Covert Channels

Cyber Deception

Malware Threats

APTs

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

Data Privacy

Spambots

Remote Attestation

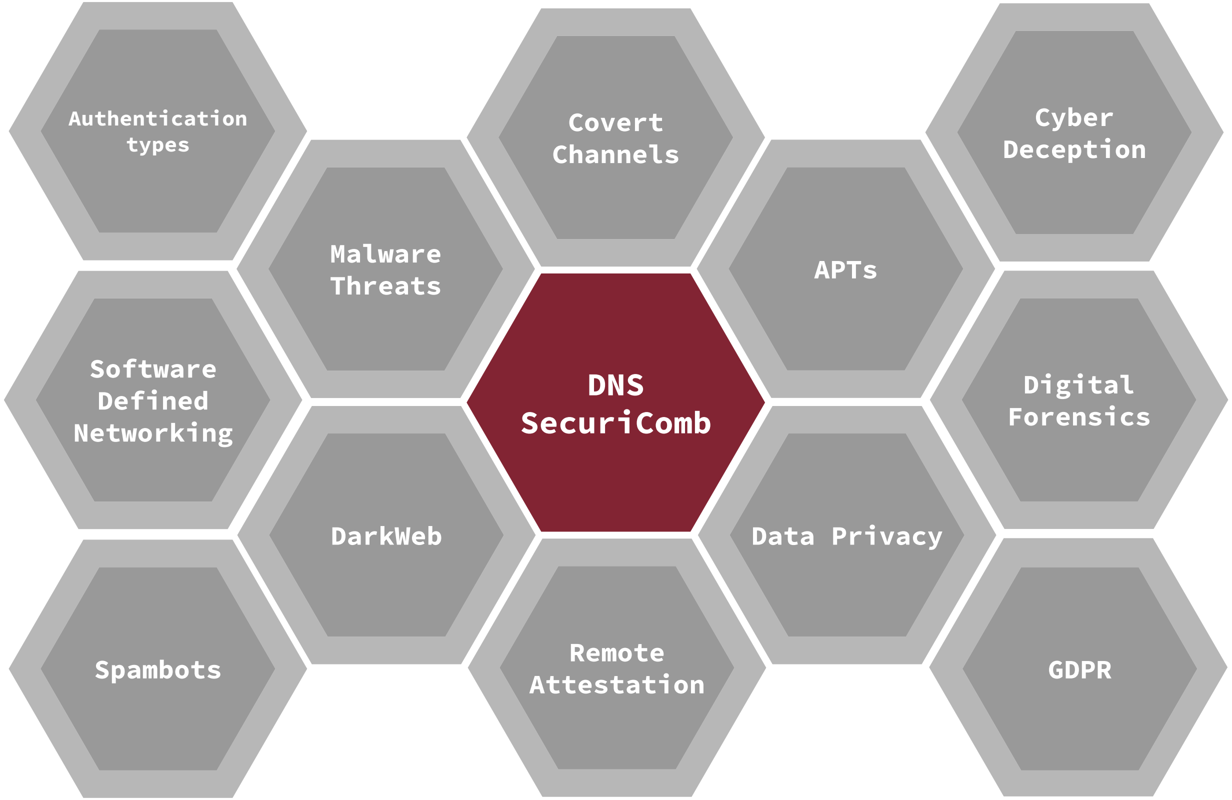
GDPR

GDPR - What?

GDPR is a European law which went into effect on May 25, 2018. The GDPR lays down rules relating to the protection of fundamental rights and freedoms of persons, and in particular their right to the protection of personal data.

It aims to improve consumer protection and general levels of privacy for individuals, includes mandatory reporting of data protection breaches and has an increased emphasis on gaining explicit consent to process information.

SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

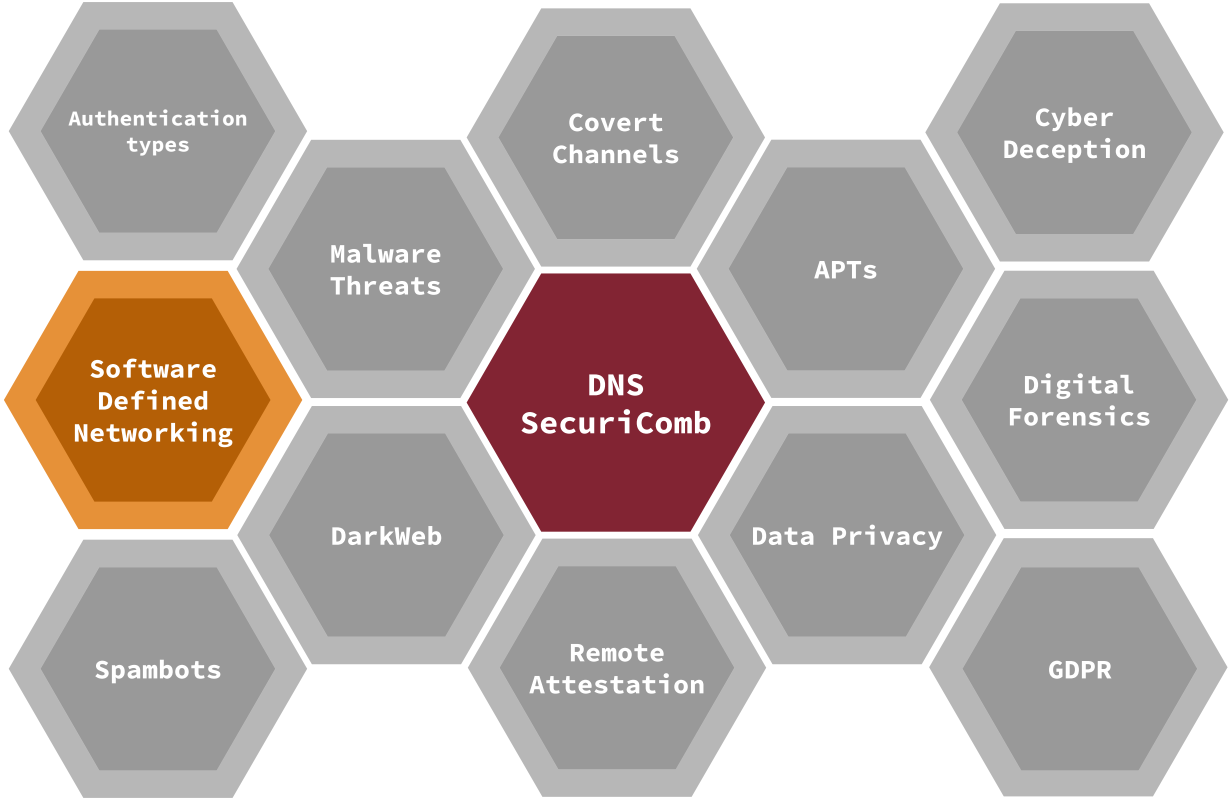
Data Privacy

Cyber Deception

Digital Forensics

GDPR

SecuriComb



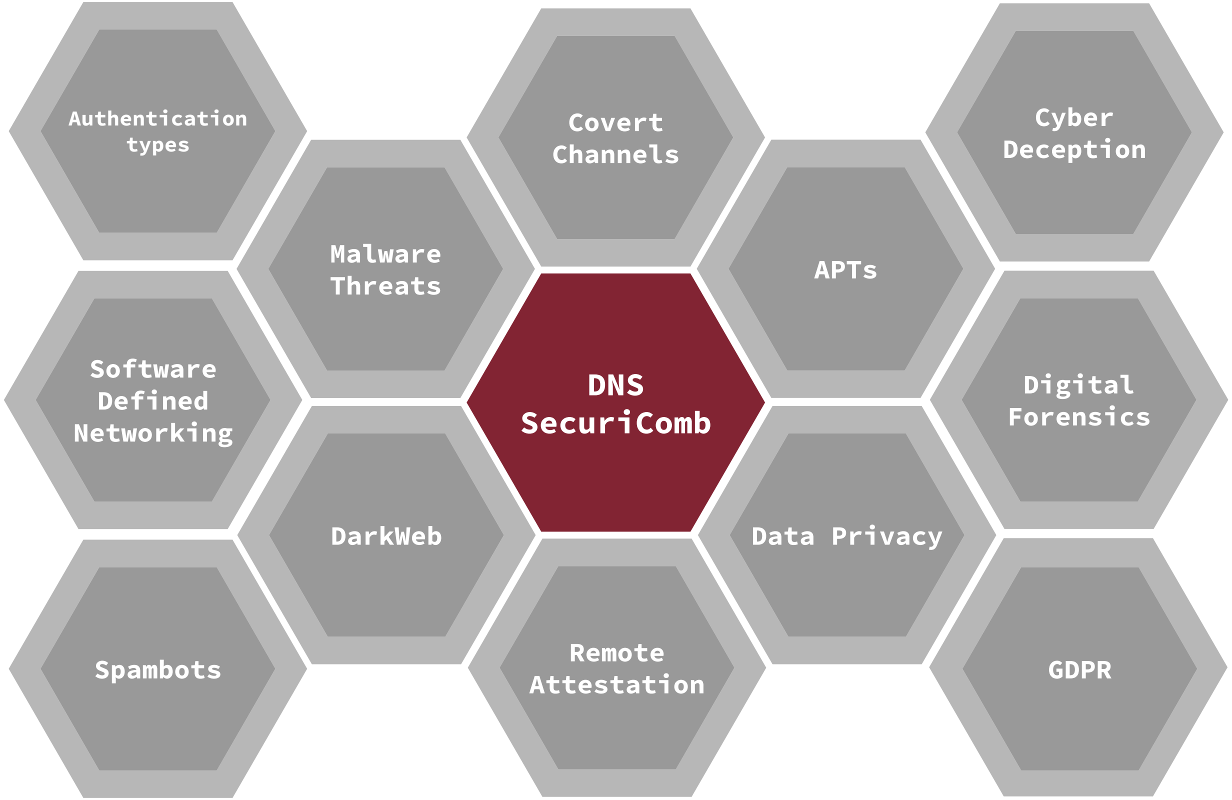
Authentication types
Covert Channels
Cyber Deception
Malware Threats
APTs
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

Traditional networking vs. SDN

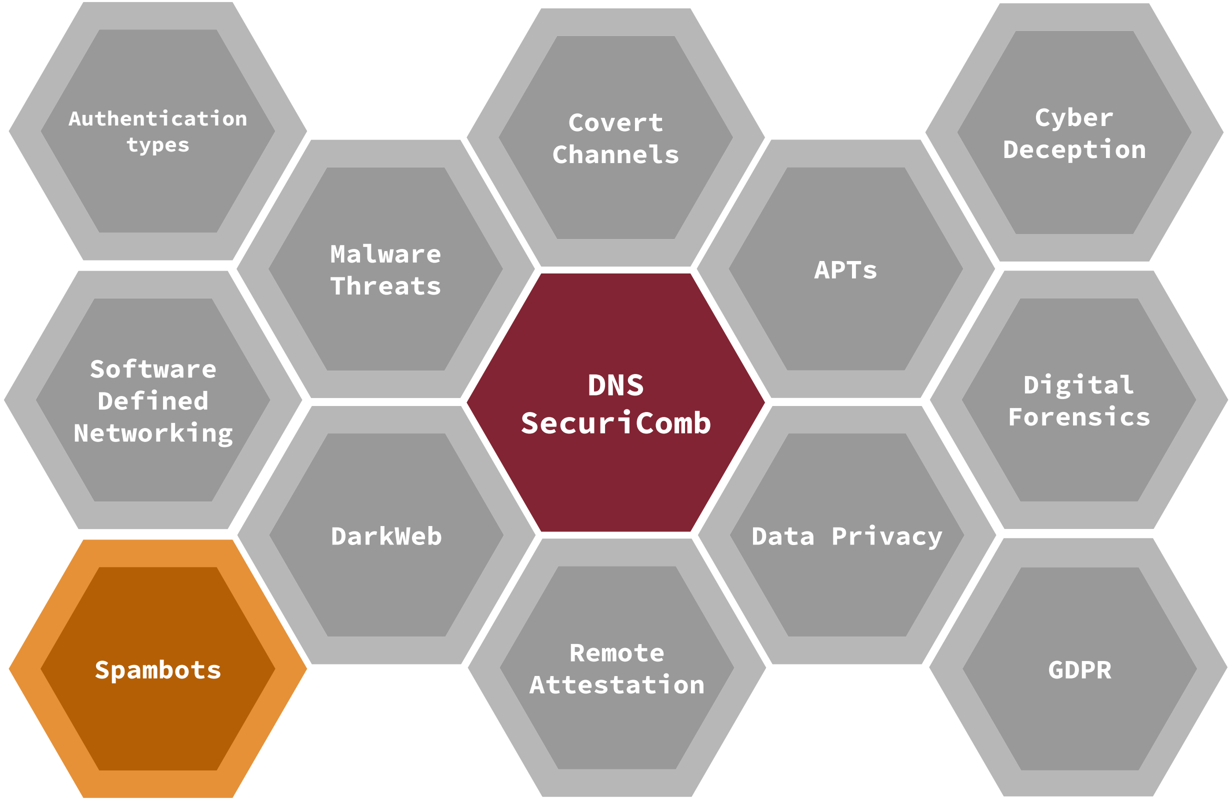
- In traditional networking, both the control plane (which determines how data packets are forwarded) and the data plane (which handles the actual forwarding of packets) are tightly integrated within network devices.

- SDN is the separation of control and data planes. This separation allows for programmability and automation of network configurations and policies. This enables network administrators to dynamically control and manage network traffic flows according to application requirements and business needs.

SecuriComb


Authentication types
Covert Channels
Cyber Deception
Malware Threats
APTs
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

SecuriComb


Authentication types
Covert Channels
Cyber Deception
Malware Threats
APTs
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

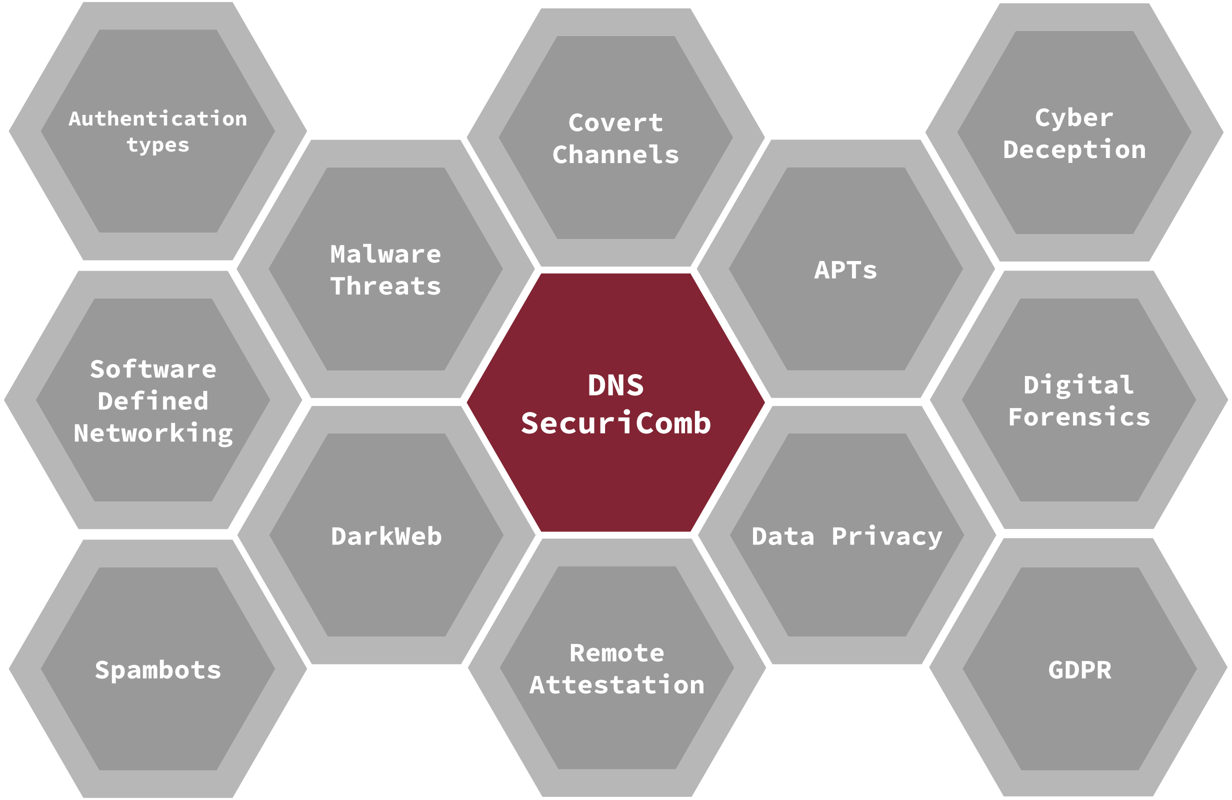
Social Bots - Spam bots

(Semi-)automated accounts with usually harmful intention designed to mimic human behavior on social media platforms.

Usual intentions:

- Misinformation spreading
- Stealing personal information/data
- Stock market manipulation
- Political influence

SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

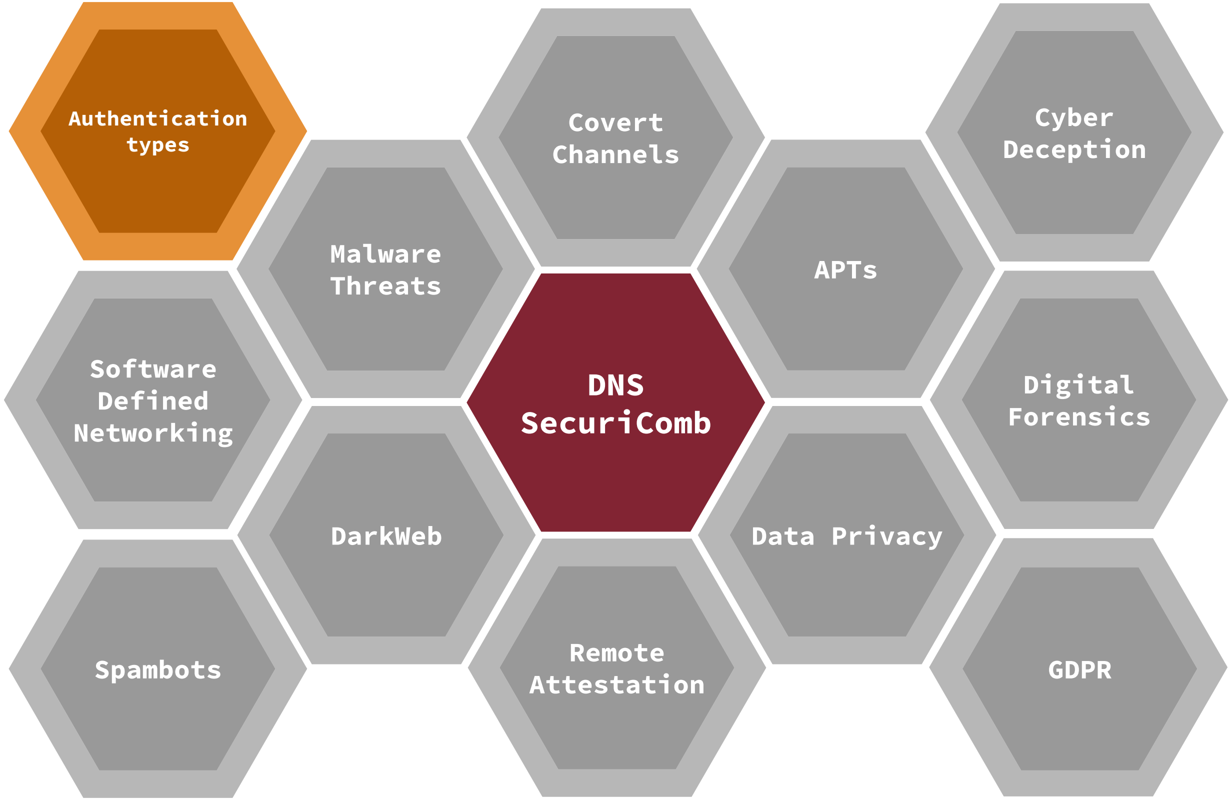
Data Privacy

Cyber Deception

Digital Forensics

GDPR

SecuriComb



Authentication types

Malware Threats

Covert Channels

APTs

Cyber Deception

Software Defined Networking

DNS SecuriComb

Digital Forensics

DarkWeb

Data Privacy

Spambots

Remote Attestation

GDPR

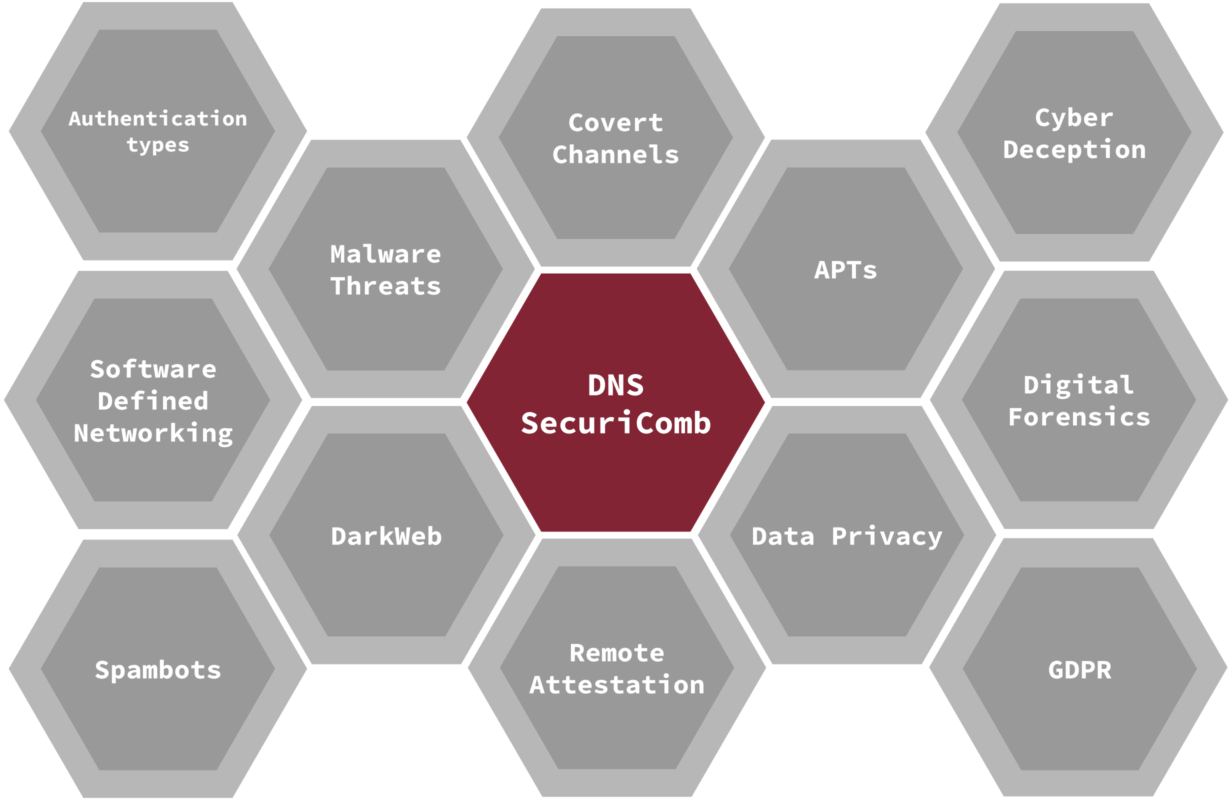
Authentication methods

Authentication is the process of verifying the identity of a user.

Objectives:

- Establish trust
- Prevent unauthorized access
- Protect sensitive information

SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

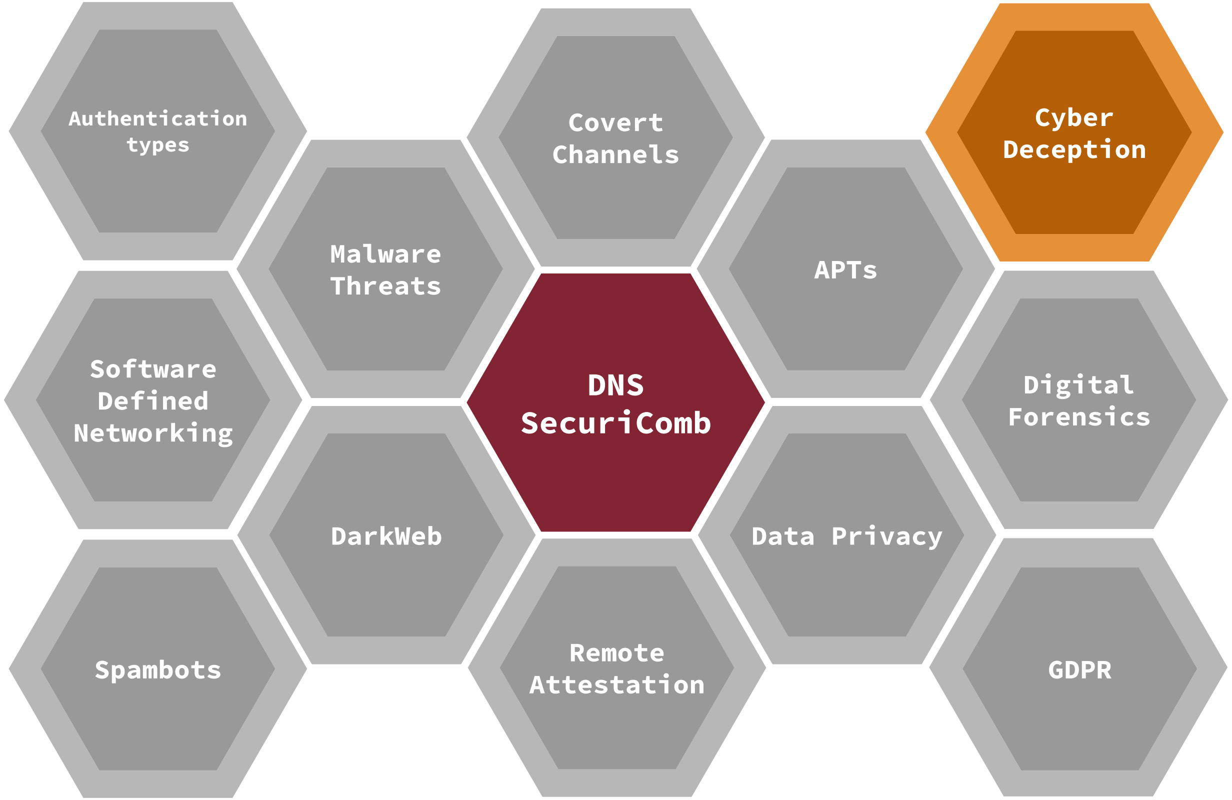
Data Privacy

Cyber Deception

Digital Forensics

GDPR

SecuriComb



Authentication types

Software Defined Networking

Spambots

Malware Threats

DarkWeb

Covert Channels

DNS SecuriComb

Remote Attestation

APTs

Data Privacy

Cyber Deception

Digital Forensics

GDPR

Cyber Deception

Cyber deception is a cybersecurity strategy designed to mislead and manipulate attackers who are attempting to breach an organization's network or systems.

It involves the deliberate creation of false information, decoys, traps, and other deceptive elements to divert, confuse, or delay attackers, ultimately enhancing the security posture of the organization.