ShadowGirl in CyberLand
— Episode 2 —
Decoding CyberLand - The Fundamentals of Cybersecurity

We delve into key topics such as the definition of cybersecurity, IT security, and information security. Understand the importance of the CIA Triad and DAD in maintaining security.

Learn about threats, vulnerabilities, and the ISC2 Code of Ethics. We also discuss critical regulations and standards like Privacy, GDPR, PII, PHI, HIPAA, ISO, NIST, and PCI DSS. Lastly, grasp the concept of non-repudiation.

Explore the world of cybersecurity with our comprehensive video at the bottom. 🎬 👇

Moreover, you can test your knowledge with our interactive quiz at the end. CyberLand is the perfect place for beginners, so stay tuned!

Topics that we will cover:

- 1️⃣ “Galactica’s Guide: Unraveling the Mysteries of Cybersecurity”
- 2️⃣ “Laser-Dogs vs Angry Cats: Understanding the CIA Triad in CyberLand”
- 3️⃣ “The Flip Side of CyberLand: DAD — The Angry Cats’ Perspective”
- 4️⃣ “Joker’s Interruption: A Deep Dive into Cyber Threats”
- 5️⃣ “The Art of Seduction: Joker, Galactica, and the Quest for Vulnerabilities”
- 6️⃣ “Ethics in CyberLand: Galactica’s Stand on the ISC2 Code”
- 7️⃣ “Galactica’s Privacy Talk: Unpacking GDPR”
- 8️⃣ “Decoding Acronyms with Galactica: PII, PHI, HIPAA, ISO, NIST, PCI DSS Explained”
- 9️⃣ “The Final Word: Non-Repudiation in CyberLand”
- 🔟 Quiz Time! → only in the video

GALACTICA: Hello, CyberLand! I'm Galactica, and welcome to the breaking news. ShadowGirl prepared the agenda for today, which is displayed on the screen.

ShadowGirl: Thank you Galactica! Today we're diving into the world of cybersecurity. Let's start with the first topic:

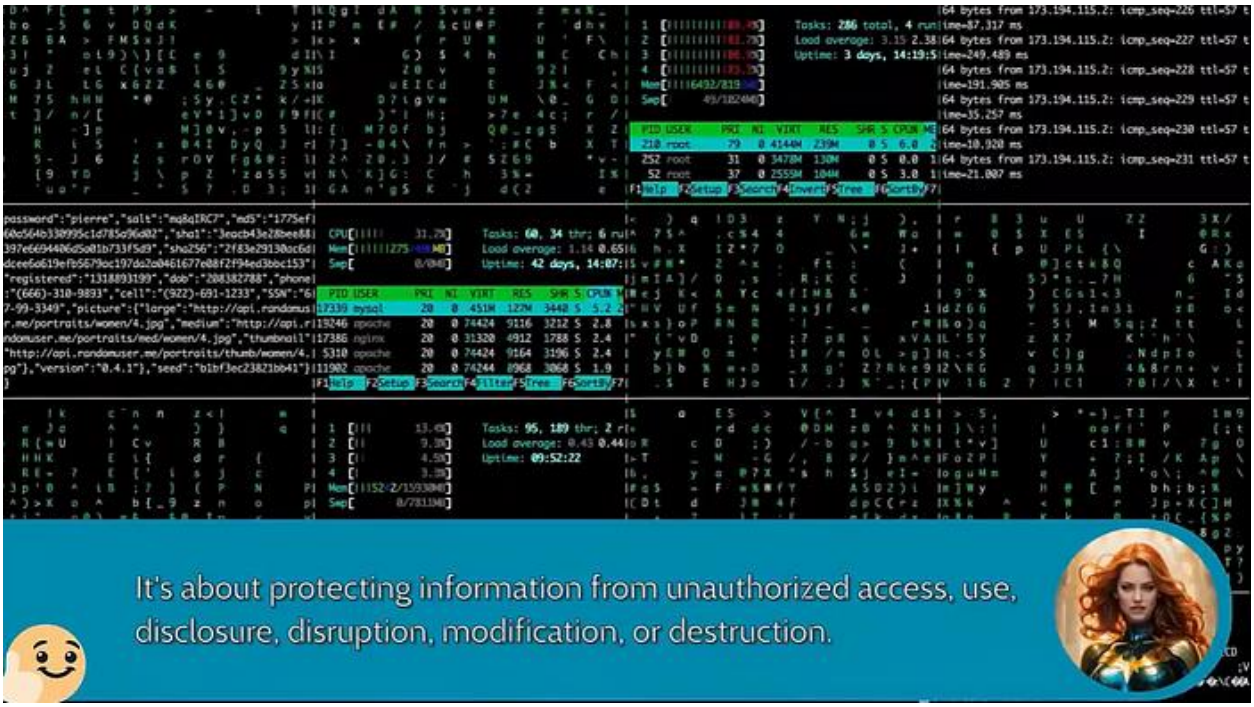
1. WHAT IS CYBERSECURITY? IT SECURITY? INFORMATION SECURITY?

GALACTICA: **Cybersecurity** is the practice of protecting systems, networks, and programs from digital attacks. This is like having a guard for your computer and online stuff. It keeps the bad guys from stealing or messing with your information.

IT Security is about safeguarding information in digital form. This is like having a guard for all things related to computers and technology in a company. It's not just about the internet, but also about making sure only the right people can access the right information on the computers.

ShadowGirl: And **Information Security**?

GALACTICA: It’s about protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction. This is about keeping all information safe, not just the stuff on computers. This could be papers in a filing cabinet or a conversation you have with a friend. It’s like making sure no one is eavesdropping on your conversations or going through your personal files.



ShadowGirl: As we venture deeper into CyberLand, we have the possibility to meet The Laser-Dogs Guardians.

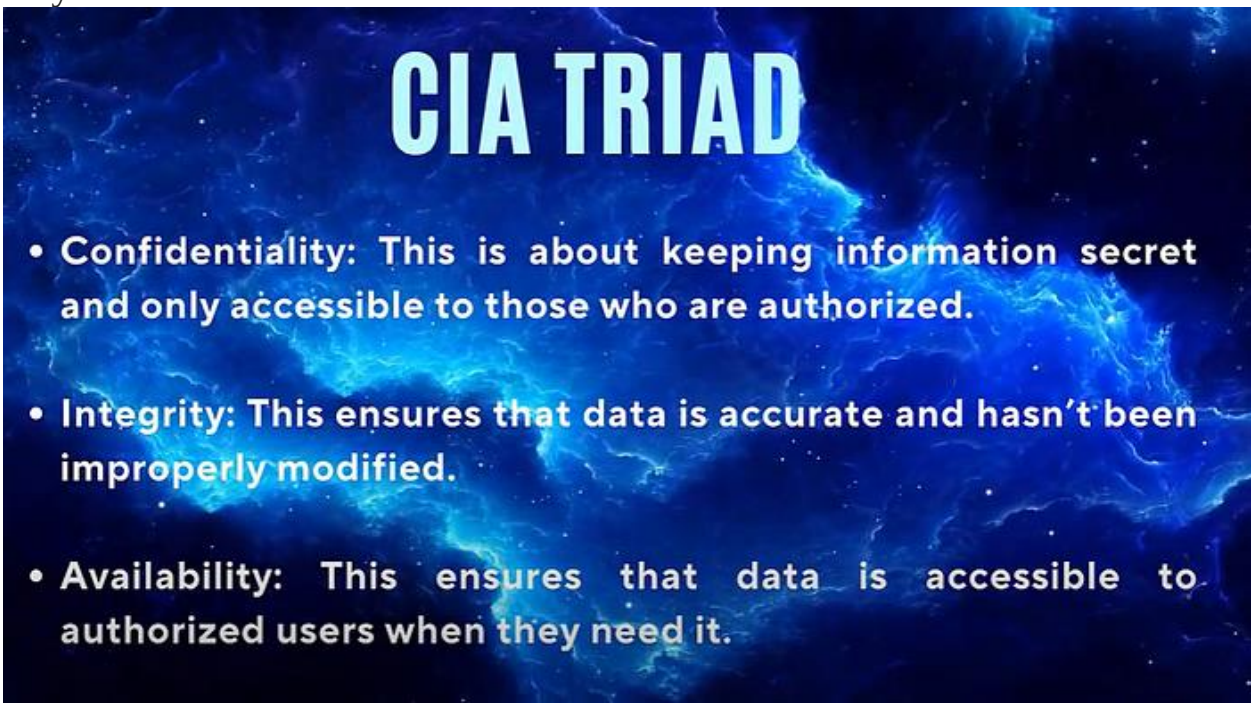
2. CIA TRIAD — LASER-DOGS OF CYBERLAND

GALACTICA: Yes! In CyberLand, The Laser-Dogs are the guardians of the CIA Triad — Confidentiality, Integrity, and Availability.

- **Confidentiality:** This is about keeping information secret and only accessible to those who are authorized.

- **Integrity:** This ensures that data is accurate and hasn't been improperly modified.

- **Availability**: This ensures that data is accessible to authorized users when they need it.



You will usually see the triangle reflected in the sky in CyberLand at night. They often fight with The Angry Cats of CyberLand to protect our data.

3. DAD (THE OPPOSITE OF CIA TRIAD) — ANGRY CATS OF CYBERLAND

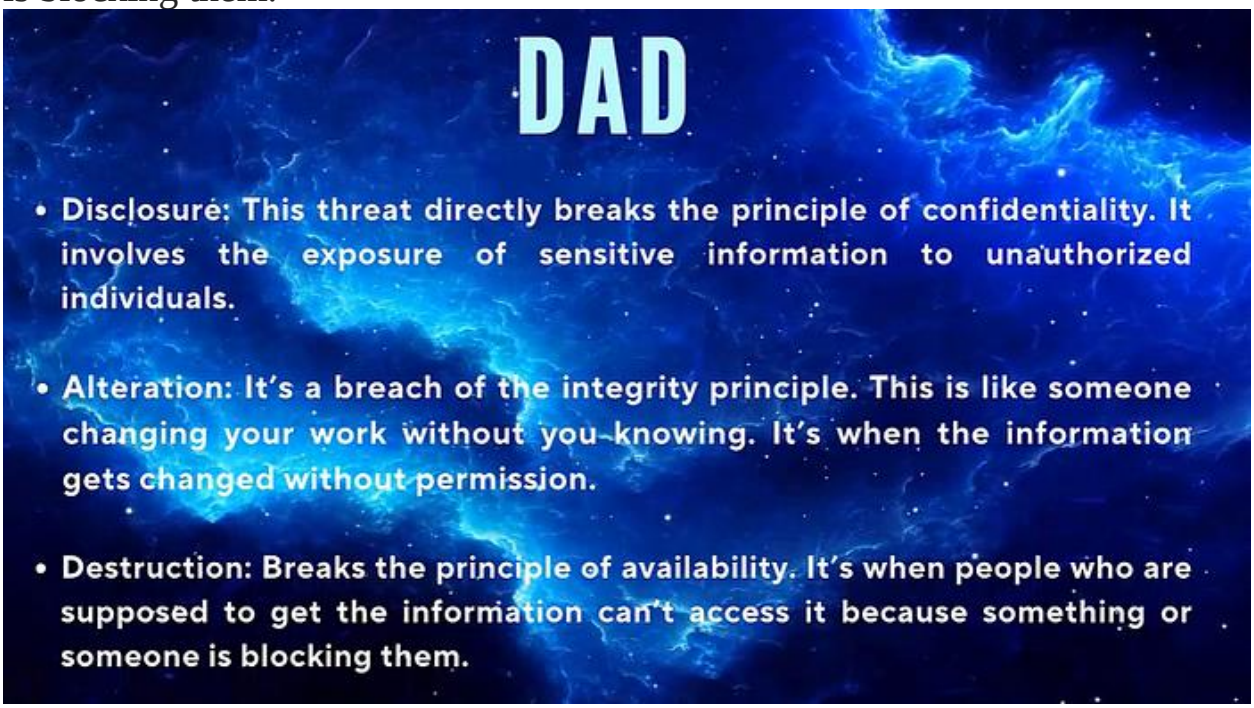
ShadowGirl: Hmm…The Angry Cats of CyberLand?

GALACTICA: Yes! On the other side (the opposite of CIA Triad), we have The Angry Cats, who represent DAD — Disclosure, Alteration, and Destruction. These Angry Cats are always trying to compromise our data.

- **Disclosure**: This threat directly breaks the principle of confidentiality. It involves the exposure of sensitive information to unauthorized individuals.

- **Alteration**: It’s a breach of the integrity principle. This is like someone changing your work without you knowing. It’s when the information gets changed without permission.

- **Destruction**: Breaks the principle of availability. It’s when people who are supposed to get the information can’t access it because something or someone is blocking them.



ShadowGirl: Thank you Galactica for summarizing CIA Triad and DAD! Let’s continue to our topics on the agenda. Next, we have two questions to highlight “What is a threat? What is a vulnerability?”. Please continue Galactica.

4. WHAT IS A THREAT?

(Joker interrupts the breaking news)

JOKER: Speaking of threats… Hello, Galactica! Did you miss me?

5. WHAT IS A VULNERABILITY?

GALACTICA: Joker, you're a perfect example of a threat — a potential cause of an unwanted incident. And if you're trying to find my vulnerabilities to hack CyberLand, you're out of luck. It's not ethical to exploit vulnerabilities for malicious purposes. Remember the ISC2 Code of Ethics?

JOKER: Yeah, you and your ethics… I'm not done here… I'll be back and you will be my queen.

(The agenda is back displayed)

ShadowGirl: Well, well, well…he knows how to make his entrance. He appeared when we were talking about threats and vulnerabilities.

GALACTICA: Yeah, a threat is any event or action that has the potential to harm an information system or the data it contains. For example, a hacker trying to gain unauthorized access to a system is a threat. It's like a burglar who might try to break into your house. A vulnerability is a weakness in a system that can be exploited by a threat. It's like a window left open in your house that a burglar could use to get in.

ShadowGirl: Also, you mentioned something about ethics?

GALACTICA: Yes! The ISC2 Code of Ethics guides all our actions in CyberLand. It's about protecting society, acting honorably, providing diligent and competent service, and advancing and protecting the profession.

Code of Ethics Preamble:

- The safety and welfare of society and the common good, duty to our principals, and duty to each other, require that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

- Therefore, strict adherence to this Code is a condition of certification.

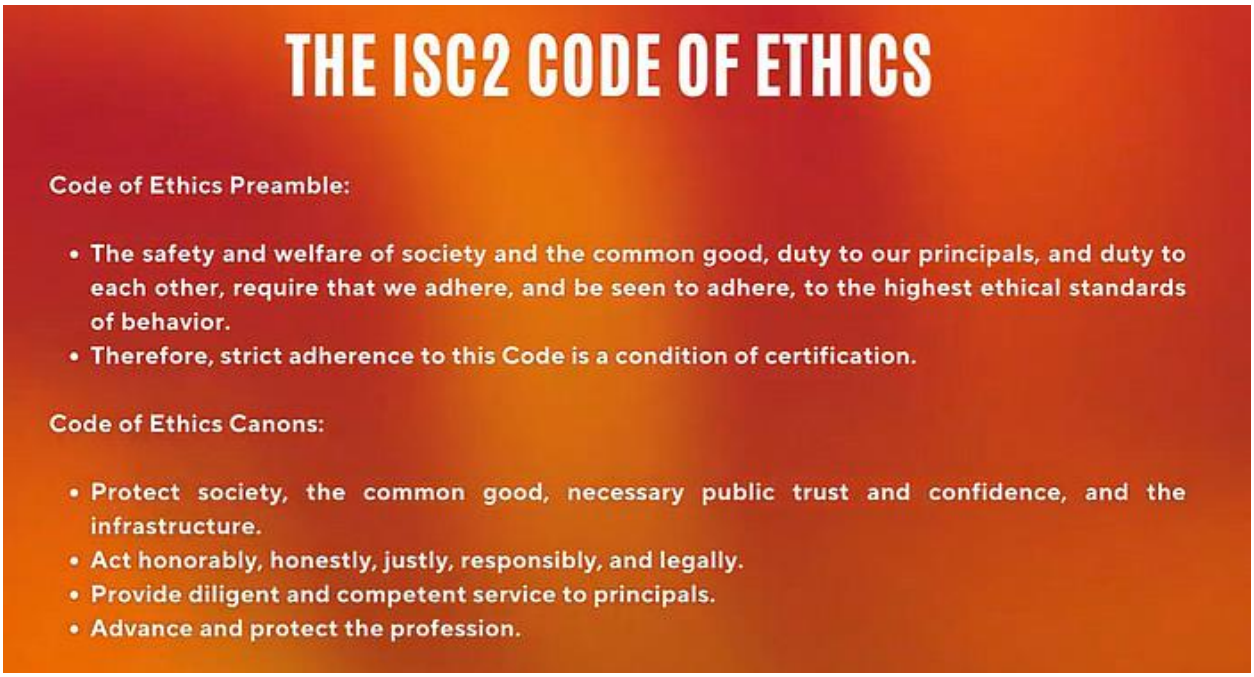
Code of Ethics Canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.

- Act honorably, honestly, justly, responsibly, and legally.

- Provide diligent and competent service to principals.

- Advance and protect the profession.



7. PRIVACY & GDPR

ShadowGirl: And let's not forget about privacy and GDPR. We must respect and protect personal data.

GALACTICA: Privacy is about keeping our personal information secret. In the digital world, privacy means making sure our personal information (like our name, address, or credit card number) doesn't get into the wrong hands.

There are many ways to protect our privacy and improve our cybersecurity. For example, we can use strong, unique passwords for our accounts. We can also be careful about what information we share online.

- GDPR stands for General Data Protection Regulation.

- It's a law from the European Union that helps protect people's private information.

- GDPR protects anyone who is in the European Union.

- It doesn't matter where you're from, if you're in the European Union, GDPR protects your personal information.

- GDPR applies to any company that has an office in the European Union, or any company outside the European Union that offers goods or services to people in the European Union.

- GDPR gives people the right to access, correct, and delete their personal information.

ShadowGirl: Quick question Galactica — Why did Joker say that you would be his queen?

GALACTICA: I look a lot like his dead wife, Miss CyberLand. She died in a plane crash. Miss CyberLand was the love of his life. Anyway, let's get back to those acronyms, shall we?

8. WHAT IS PII, PHI, HIPAA, ISO, NIST, PCI DSS?

ShadowGirl: Absolutely, Galactica! Let's continue with the acronyms displayed on the screen. These are all crucial in the world of cybersecurity.

GALACTICA: Yes, indeed! Let's explain each term:

1. In cybersecurity, Personally Identifiable Information, also known as **PII**, refers to any data that could be used to identify an individual. This includes direct identifiers like a person's full name, social security number, driver's license number, and indirect identifiers like race and place of birth. PII is one of the most valuable commodities in cybersecurity because if it falls into the wrong hands, it can be used for malicious purposes such as identity theft, fraud, or gaining unauthorized access to an individual's accounts. Therefore, protecting PII is a critical aspect of cybersecurity.

2. PHI stands for Protected Health Information. It refers to any individually identifiable health information that is created, received, maintained, or transmitted by a covered entity or business associate under HIPAA regulations. This can include medical records, conversations about treatment, billing information, and more. The goal is to protect patients' privacy and security.

3. HIPAA, or the Health Insurance Portability and Accountability Act, is a US law that protects your health information and gives you certain rights over your health information. Most people associate HIPAA with the Privacy, Security, and Breach Notification Rules of the Administrative Simplification Regulations. These rules protect the privacy and security of individually identifiable health information.

4. ISO stands for the International Organization for Standardization. It's a global body that develops and publishes international standards. These standards ensure that products, services, and systems are safe, reliable, and of good quality.

5. NIST or the National Institute of Standards and Technology, provides a Cybersecurity Framework for organizations to manage and reduce cybersecurity risk. It is a non-regulatory federal agency within the U.S. Department of Commerce. It's organized into five key functions: Identify, Protect, Detect, Respond, and Recover, which provide a comprehensive view of the lifecycle for managing cybersecurity risk.

6. PCI DSS stands for the Payment Card Industry Data Security Standard. It is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

In simple terms, PCI DSS is like a rulebook for businesses that handle credit card information. It tells them how to protect this information to prevent data theft and fraud. It includes practices like installing firewalls, encrypting data transmissions, and using anti-virus software.

So, if you're a business that takes card payments, PCI DSS is a set of rules you follow to make sure you're keeping your customers' card information safe. This helps build trust with your customers and protects your business from the potential costs and damage of data breaches.

ShadowGirl: Thank you very much Galactica for explaining these important acronyms in cybersecurity! One more thing we forgot to explain to the public. It's about **non-repudiation**.

GALACTICA: Yes, I forgot to explain that. In cybersecurity, **non-repudiation** is a digital guarantee that prevents a person from denying their actions related to a transaction or a digital message. It's like a registered letter in the digital world, where neither the sender nor the receiver can deny their part in the transaction. This is often achieved through digital signatures and encryption, which verify the source and integrity of the message. Therefore,

non-repudiation plays a crucial role in maintaining trust and accountability in digital communications.

ShadowGirl: I think we covered the agenda for today regarding the security principles in cybersecurity. The audience can explain the basic concepts in cybersecurity. Let's see if they pass the quiz prepared by our superhero Maximus.

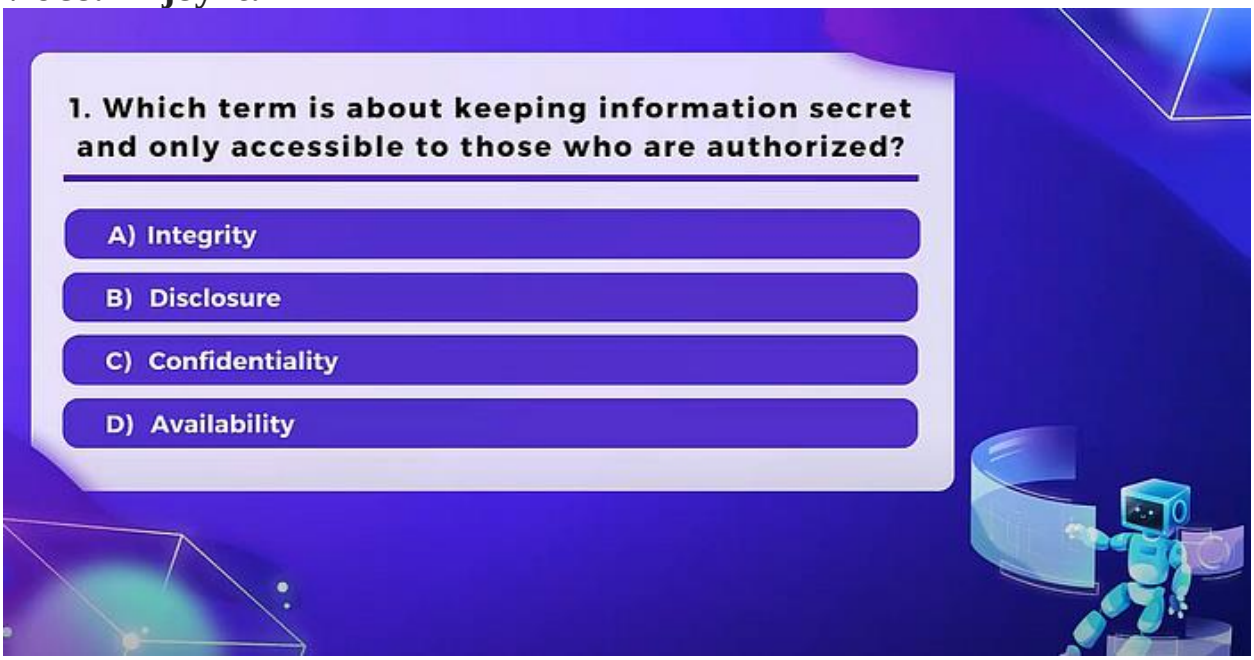
MAXIMUS: Hi! My name is Maximus. The girls explained the basic concepts of CyberLand. Let's see if you understood the terms. It's quiz time!

❗ **There is a short quiz included in the video**

🎬 **If you want to see the full video, click on the following link:**

[ShadowGirl in CyberLand — Episode 2 — Decoding CyberLand: The Fundamentals of Cybersecurity (youtube.com)]

Bonus: This is the first question from the quiz. For the rest, check the video. Enjoy it! 😉



Do you remember our cyber warrior from the first episode? He has a message for you at the end of the quiz.

> *Thanks and Regards,*
>
> *ShadowGirl* 🦸 😉