THE TRANSFORMATION OF DEVOPS AND INFOSEC IN AIOT

Susie Su
Global Software Operations Architect
@Signify (Philips Lighting)

OPEN SOURCE

XPETERSUE

Susie Su

DevOps Manager

Global Software Operations Arch

@Signify (Philips Lighting)

14 years Software Development

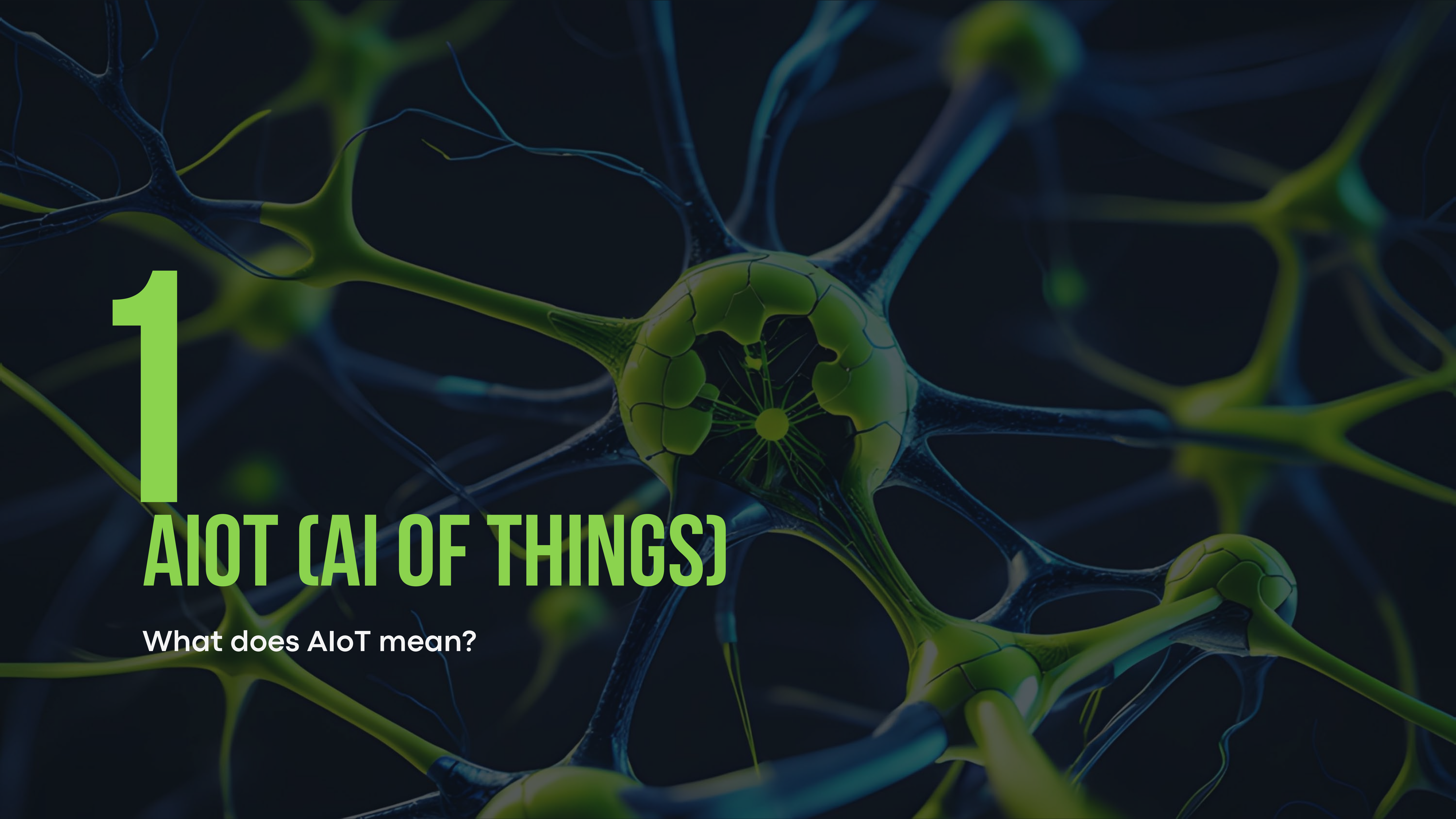
10 years Cloud Compute (AWS & Ali Cloud)

8 years Team Manager & Project Management

5 years IoT & Kubernetes/Docker & Prometheus & Spring Boot

4 years ISP & 3 years Overseas

* 3 years AI, ML, Deep Learning and Blockchain



1

AIOT (AI OF THINGS)

What does AIoT mean?

AIOT = AI + IOT

Automated Vehicles

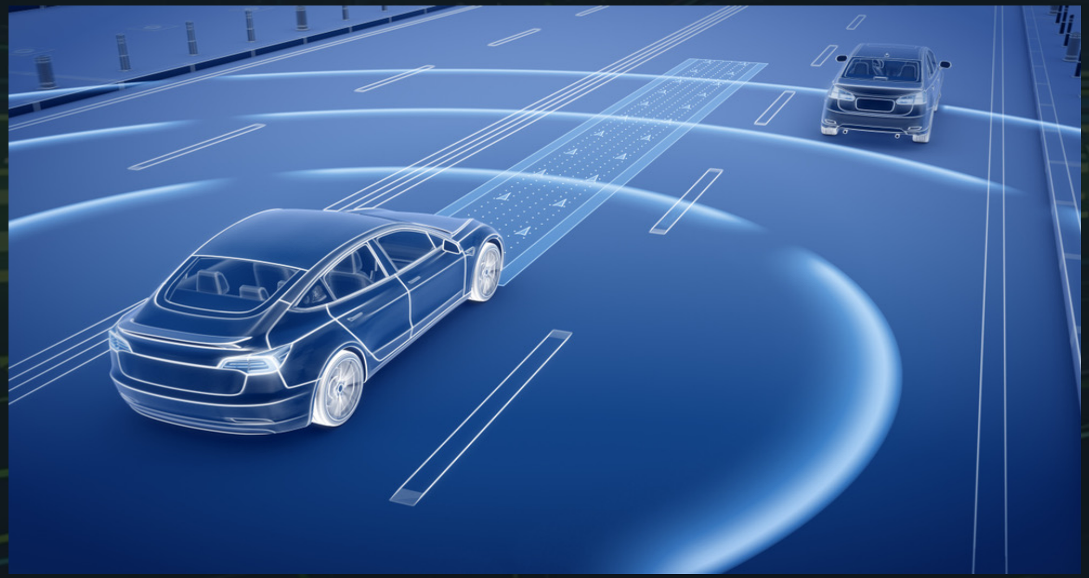
Tesla, Waymo, Mobileye, Cruise and Baidu

Smart City

Lighting, Video Surveillance, Monitoring traffic and smart buildings

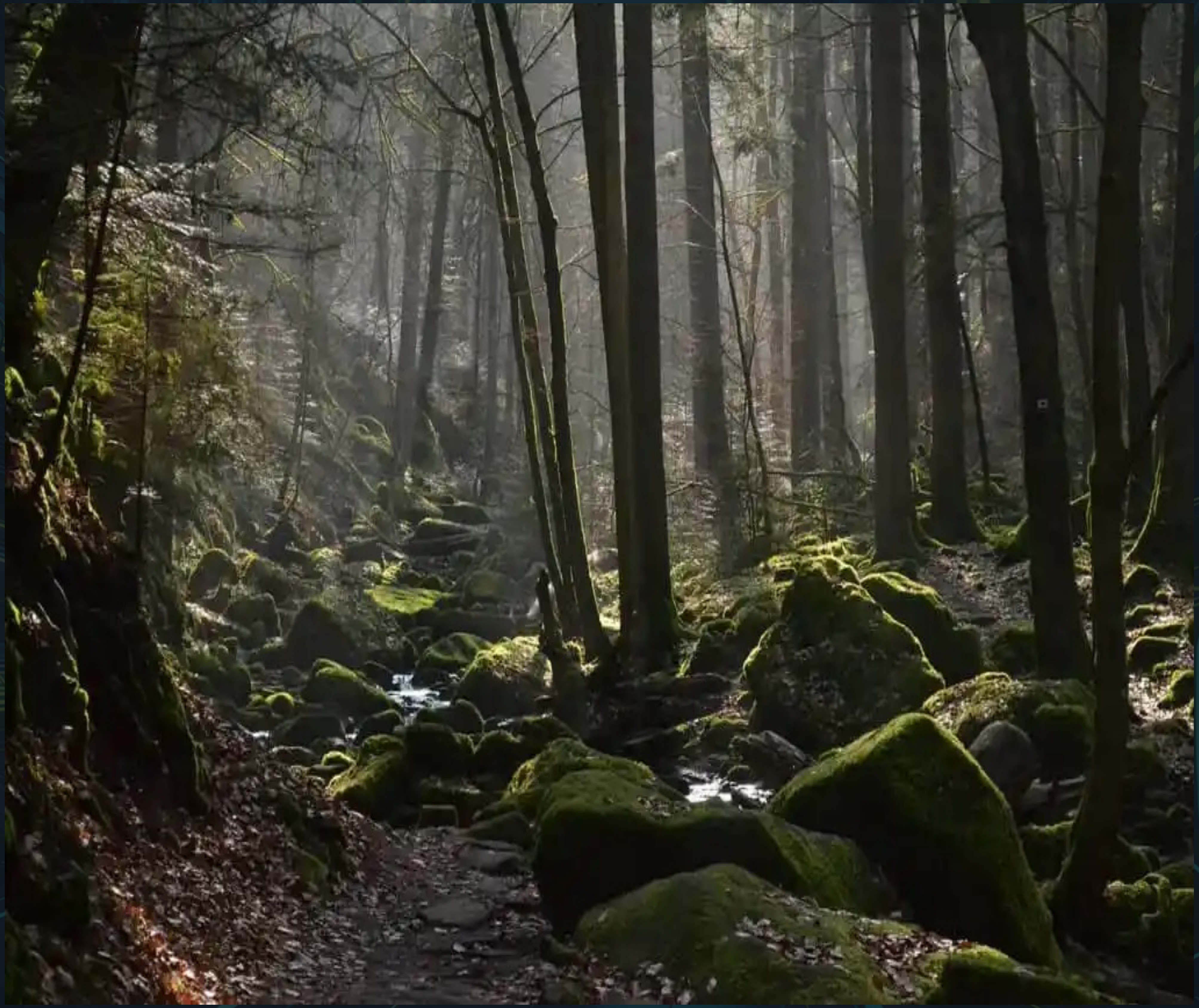
Manufacturing

Deep Learning and deep neural networks.



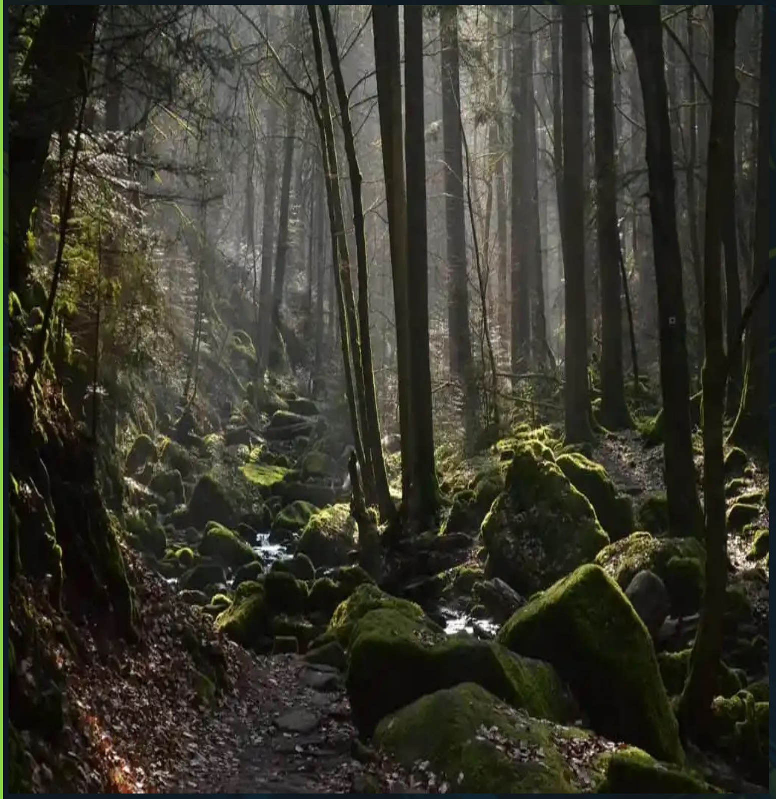
AIOT LIGHTING EXAMPLE

Let’s imagine I visited the Black Forest recently and captured a photo. Now, I'd like to recreate the same ambiance in my bedroom.



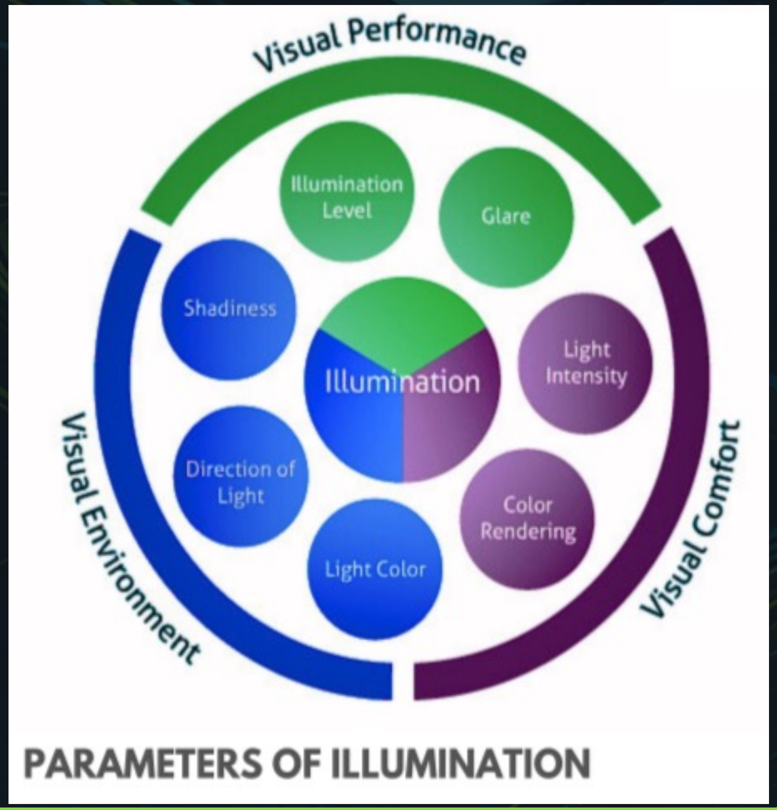
RECREATE ‘BLACK FOREST’ AMBIANCE IN MY BEDROOM

Black Forest Photo



covert

Lighting Parameters



command

Hardware Processing

Apply

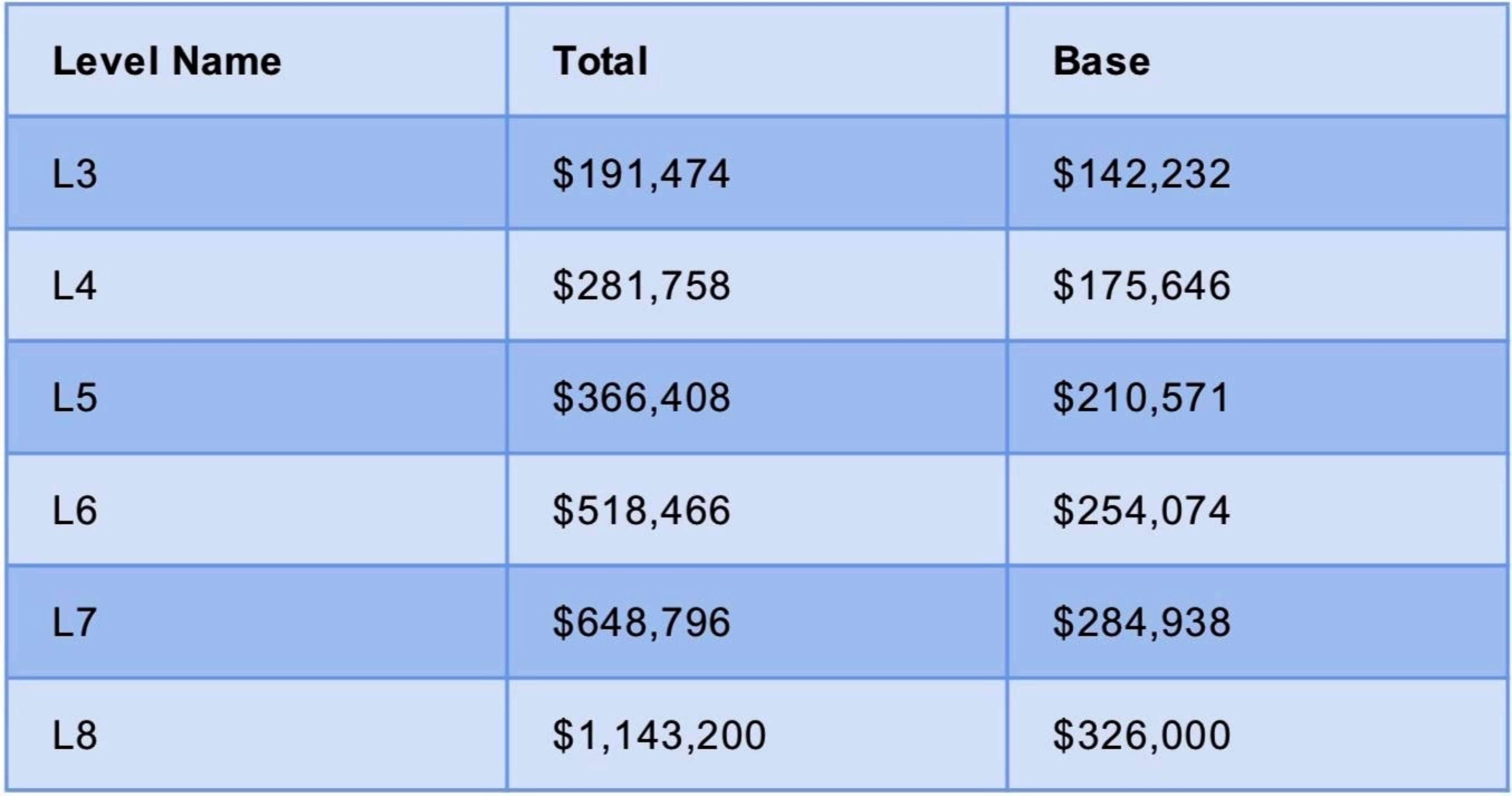
RECREATE ‘BLACK FOREST’ AMBIANCE IN MY BEDROOM

2

DEVOPS IN AIOT

How AI and AIoT Affect DevOps ?

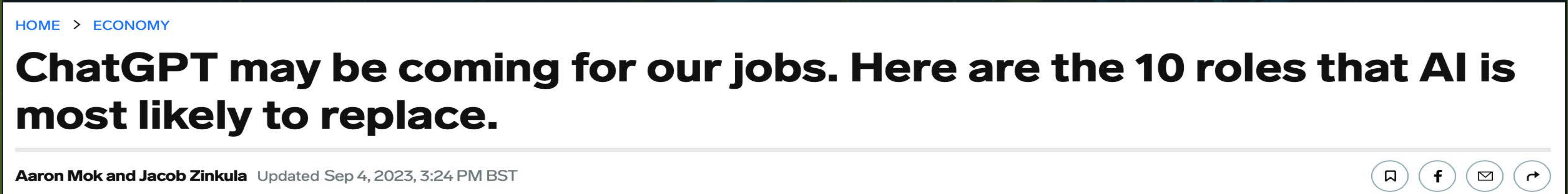
CURRENT AI CAPABILITY



Level Name	Total	Base
L3	$191,474	$142,232
L4	$281,758	$175,646
L5	$366,408	$210,571
L6	$518,466	$254,074
L7	$648,796	$284,938
L8	$1,143,200	$326,000

AI = Google Level 3 Software Engineer

AI = A Stanford Student in 16 units (majors)



HOME > ECONOMY

ChatGPT may be coming for our jobs. Here are the 10 roles that AI is most likely to replace.

Aaron Mok and Jacob Zinkula Updated Sep 4, 2023, 3:24 PM BST

10 years ago

- Telemarketers
- Bookkeeping Clerks
- Compensation and Benefits Managers
- Receptionists
- Couriers
- Proofreaders
- Computer Support Specialists
- Market Research Analysts
- Advertising Salespeople
- Retail Salespeople
- Content Marketers

Present

- Tech jobs (Coders, software engineers, data analysts)
- Media jobs (advertising, content creation, technical writer)
- Legal industry jobs (paralegals, legal assistants)
- Market research analysts
- Teachers
- Finance jobs (Financial analysts, financial advisors)
- Traders
- Graphic designers
- Accountants
- Customer service agents

WHAT AI CANNOT DO?

➢ AI is incapable of handling intricate problems.

For instance, Developers consistently encounter real-world open-ended questions and challenges.

➢ AI lacks the depth of thought exhibited by professional engineers.

➢ AI is deficient in critical thinking capabilities.

➢ AI struggles to engage in real-world collaboration and communication across various departments and teams. Soft skills, like communication and interpersonal skills, leadership, problem solving, forging and maintaining work ethic, time management, teamwork.

WHAT AI CANNOT DO?

- AI is incapable of handling intricate problems.

For instance, Developers consistently encounter real-world open-ended questions and challenges.

- AI lacks the depth of thought exhibited by professional engineers.
- AI is deficient in critical thinking capabilities.
- AI struggles to engage in real-world collaboration and communication across various departments and teams. Soft skills, like communication and interpersonal skills, leadership, problem solving, forging and maintaining work ethic, time management, teamwork.

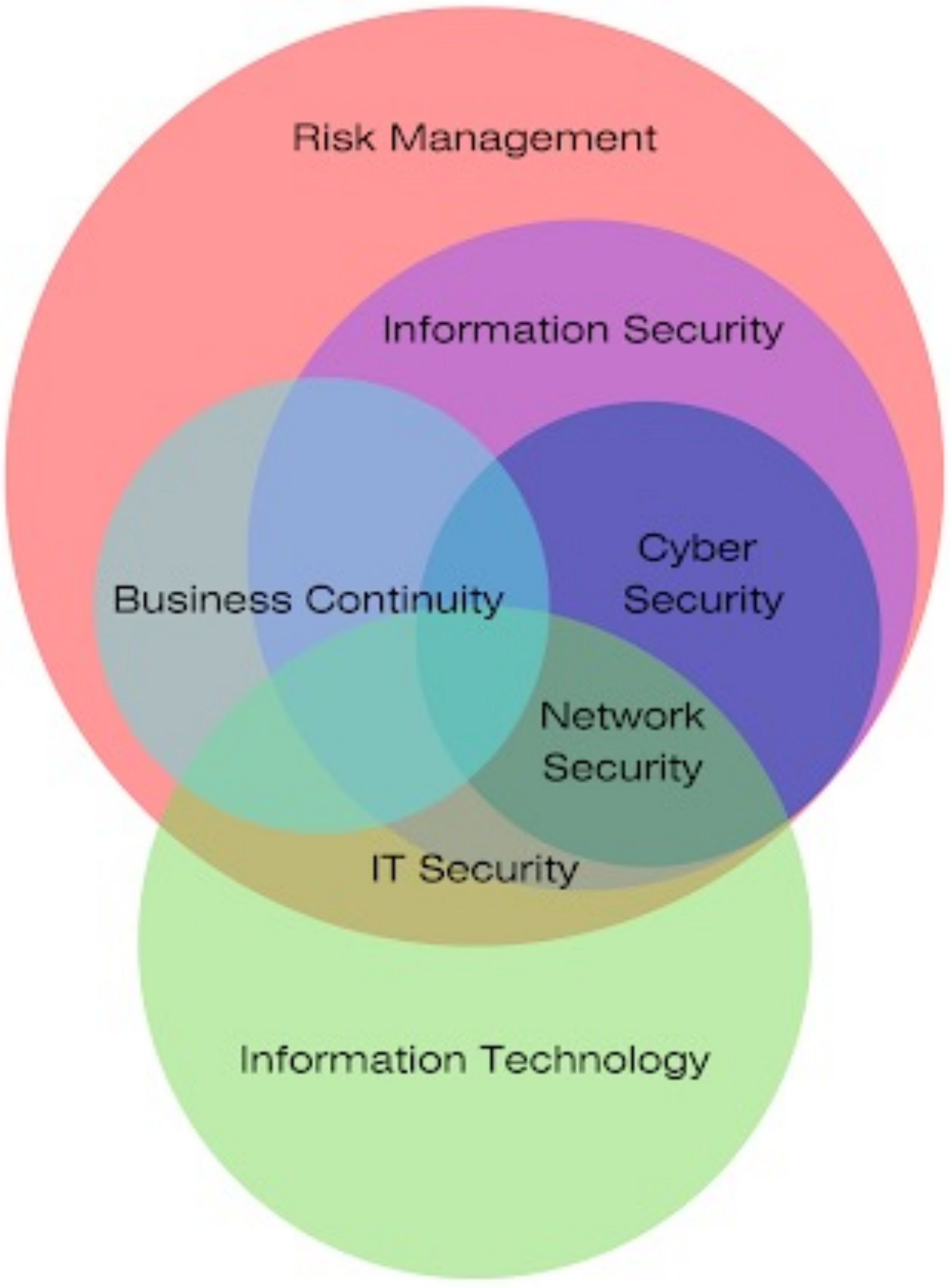
3

AI SECURITY

InfoSec, IoT Security in AI

INFOSEC

- Application Security
- Cloud Security
- Infrastructure Security
- Incident Response
- Cryptography
- Disaster Recovery
- Vulnerability Management

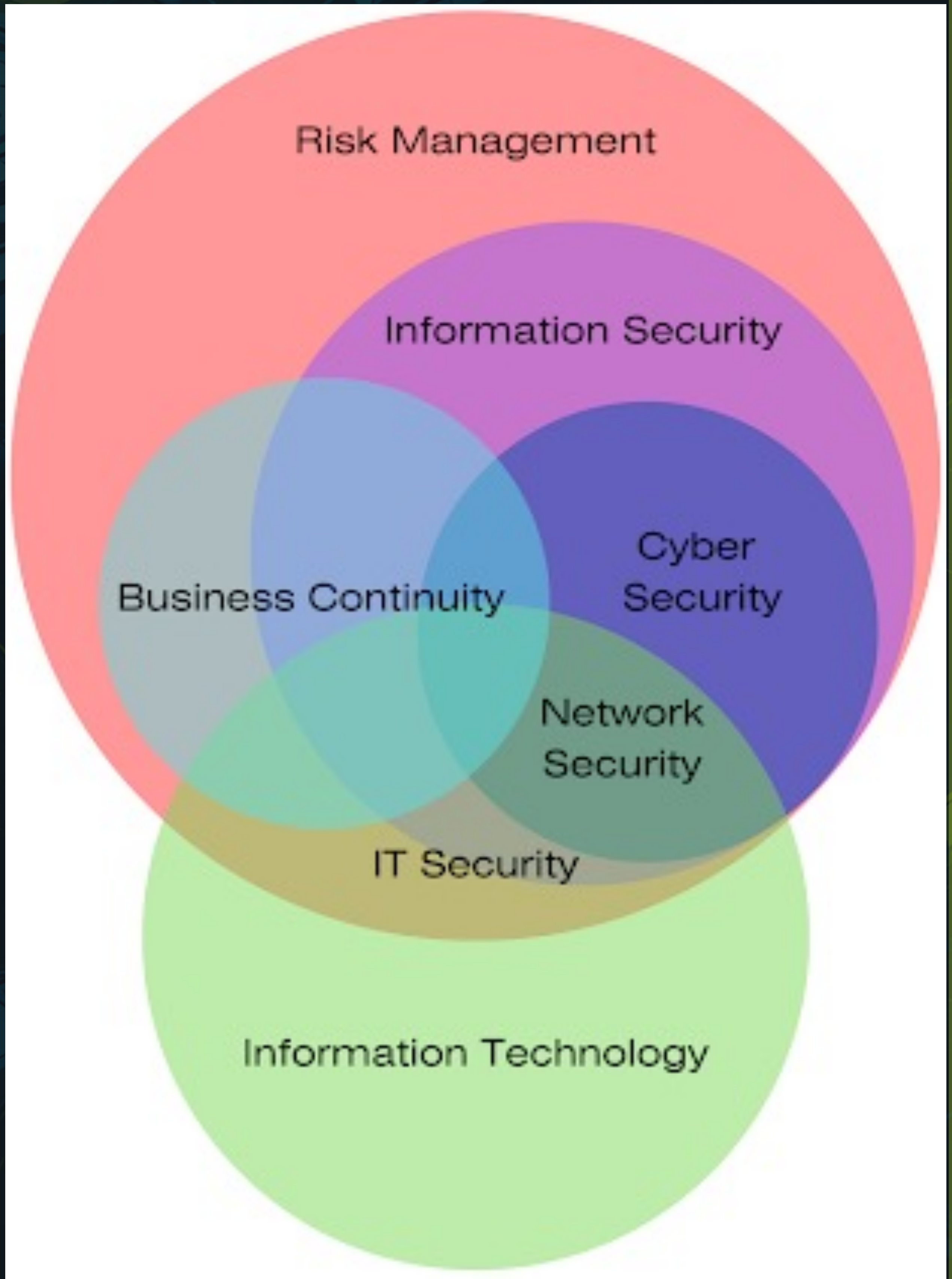


CYBERSECURITY

- Network Security
- Cloud Security
- Endpoint Security
- Application Security
- IoT Security

- 5G Networks
- IoV (Internet of Vehicles)
- IIoT (Industrial IoT)

. . .



IOT SECURITY

AIoT Security

- 5G Networks
- IoV (Internet of Vehicles)
- IIoT
  - ICS (Industrial Control System)

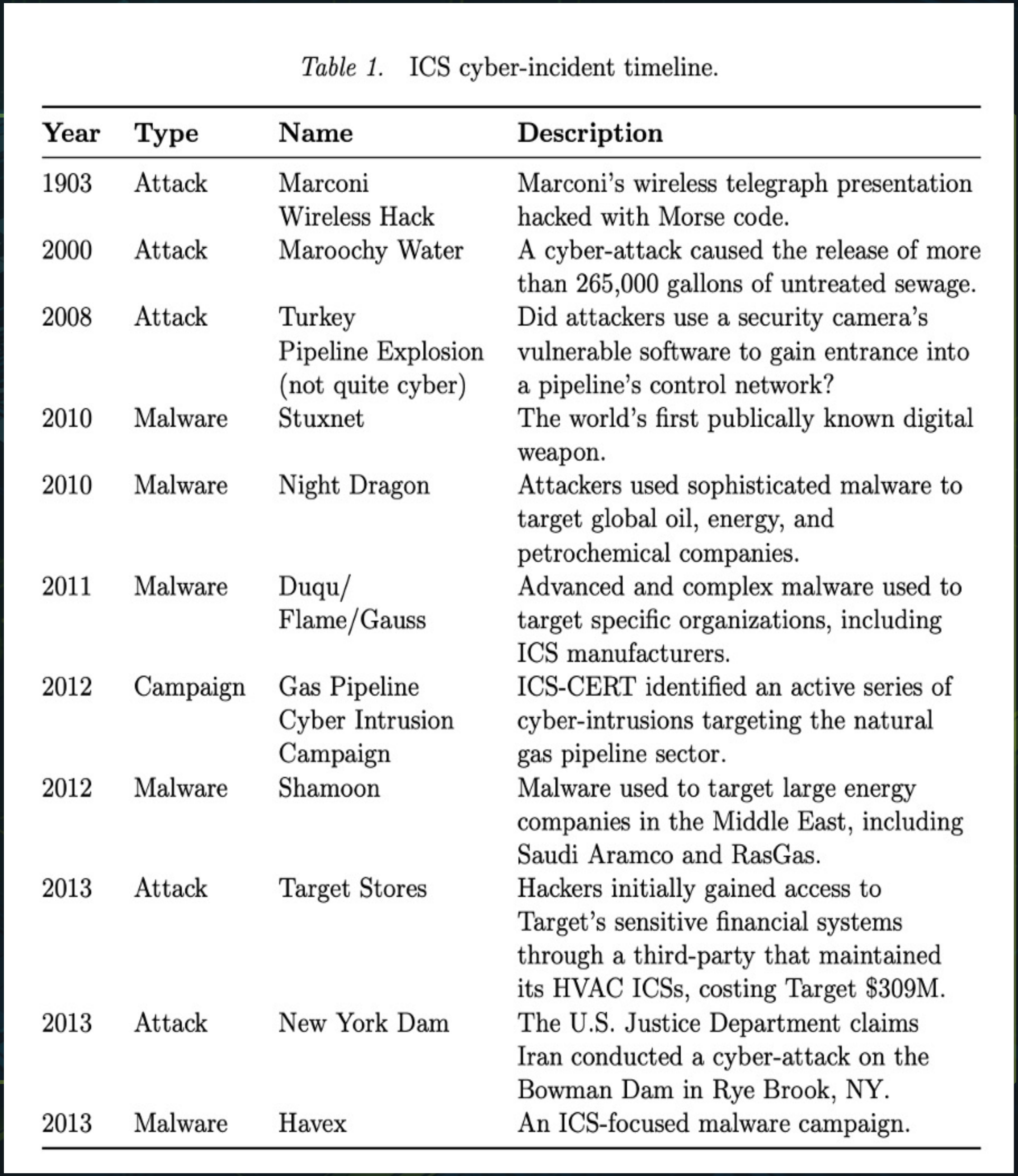


Table 1. ICS cyber-incident timeline.

Year	Type	Name	Description
1903	Attack	Marconi Wireless Hack	Marconi's wireless telegraph presentation hacked with Morse code.
2000	Attack	Maroochy Water	A cyber-attack caused the release of more than 265,000 gallons of untreated sewage.
2008	Attack	Turkey Pipeline Explosion (not quite cyber)	Did attackers use a security camera's vulnerable software to gain entrance into a pipeline's control network?
2010	Malware	Stuxnet	The world's first publically known digital weapon.
2010	Malware	Night Dragon	Attackers used sophisticated malware to target global oil, energy, and petrochemical companies.
2011	Malware	Duqu/ Flame/Gauss	Advanced and complex malware used to target specific organizations, including ICS manufacturers.
2012	Campaign	Gas Pipeline Cyber Intrusion Campaign	ICS-CERT identified an active series of cyber-intrusions targeting the natural gas pipeline sector.
2012	Malware	Shamoon	Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas.
2013	Attack	Target Stores	Hackers initially gained access to Target's sensitive financial systems through a third-party that maintained its HVAC ICSs, costing Target $309M.
2013	Attack	New York Dam	The U.S. Justice Department claims Iran conducted a cyber-attack on the Bowman Dam in Rye Brook, NY.
2013	Malware	Havex	An ICS-focused malware campaign.

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- Protects AI data confidentiality, integrity, and availability.
- Uses encryption and access controls.
- Secures data storage.
- Anonymizes data to prevent leaks.

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- Differential Privacy encompasses methods that introduce managed disturbances into data to safeguard individual privacy without compromising the general usefulness of the data.
- Federated Learning allows for spreading the training procedure over various devices to prevent the disclosure of raw data.

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- Application Security
- Cloud Security
- Infrastructure Security
- Incident Response
- Cryptography
- Disaster Recovery
- Vulnerability Management

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- It is crucial for identifying vulnerabilities and understanding how decisions are made.
- Transparent models are easier to audit and debug.

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- 5G Networks
- IoV (Internet of Vehicles)
- IIoT (Industrial IoT)

…

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- Protecting user data, preventing impersonation attacks
- Ensuring that AI-generated outputs are not exploited for malicious purposes

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- Adversarial Perturbations: Malicious inputs crafted to deceive AI models into making incorrect predictions.
- Transfer Attacks: Adversarial attacks that work across different AI models.
- White-Box and Black-Box Attacks, which depend on the attacker's knowledge of the target model's architecture.

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

- Bias Mitigation: techniques to identify and reduce biases in training data
- Fairness-aware Learning: created to design models that make fair predictions across different demographic groups.

a

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

a

- Coding practices
- Regular updates
- Proper disposal of systems.

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

- AI systems must comply with relevant regulations
- data protection laws (e.g., GDPR)
- industry-specific regulations
- ethical guidelines

a

AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

  - Human-in-the-Loop (Human Review)
  - Human expertise with AI analysis for threat detection
  - Overall Human Oversight

a

SUMMARY

- AIoT Definition and Applications in Reality.
- How AI and AIoT affect DevOps
- InfoSec and IoT Security in AI and AI Security Definition

THANK YOU !