

# Research Methodology - Let's Explore!

- A **systematic approach** to conducting research, involving methods, techniques, and tools to collect and analyze data to **solve a specific problem**.
- Influenced by **philosophical assumptions** like **epistemology** (how we know) and **ontology** (what exists).

“Which researcher are you most like?”

- The Philosopher (Loves theory!)
- The Detective (Data first!)
- The Engineer (Solves real-world problems!)
- The Artist (Creative and intuitive!)

# Epistemology — The Study of Knowledge

## How do we know what we know?

What is knowledge?

**Knowledge** is generally understood as the awareness, understanding, belief or familiarity gained through experience, education, reasoning, or discovery. It refers to the information, facts, skills, and insights that a person or group acquires and can apply.

Can knowledge be objective (true for everyone) or is it subjective

# Epistemology — The Study of Knowledge

## How do we know what we know?

What is knowledge?

“A forensic analyst **knows** that a file was accessed at 2:03 AM based on **system log evidence.**”

# Epistemology — The Study of Knowledge

## How do we know what we know?

What is knowledge?

“A forensic analyst **knows** that a file was accessed at 2:03 AM based on **system log evidence.**”

Knowledge here is a **justified belief based on evidence**  
it's not just guessing but supported by verifiable data.

# Epistemology — The Study of Knowledge

## How do we know what we know?

How Do We Acquire Knowledge?

Knowledge is acquired through **experience, observation, training, and communication** — a mix of theory and practice.

As a cyber security students, where will you acquire knowledge about malware detection?

# Epistemology — The Study of Knowledge

## How do we know what we know?

How Do We Acquire Knowledge?

Knowledge is acquired through **experience, observation, training, and communication** — a mix of theory and practice.

As a cyber security students, where will you acquire knowledge about malware detection?

- Lectures & tutorials
- Reading research papers
- Analysing real malware code
- Interviewing industry experts

# Epistemology — The Study of Knowledge

## How do we know what we know?

How Do We Justify Beliefs or Claims to Know Something?

“You claim a system was compromised by a specific threat actor. “

To justify it, you present:

- IP logs matching known attacker patterns
- Timestamped malware payloads
- Indicators of compromise (IoCs) from threat intelligence reports

follow a positivist epistemology (often used in quantitative research)

# Epistemology — The Study of Knowledge

## How do we know what we know?

Is Knowledge Objective or Subjective?

“SHA-256 hash values for files are consistent and verifiable by anyone.”

“An employee *feels* that the security policy is too strict, which makes them bypass protocols.”

follow an interpretivist epistemology (often used in qualitative research)

# Epistemology — The Study of Knowledge

## How do we know what we know?

- Ontology (The Study of Existence or Reality)
- Ontology is concerned with the nature of reality and existence: what is out there in the world and how we understand it.
- It explores questions like: • What is the nature of reality? • What kinds of things exist in the world?
- Are there objective realities that exist independently of us (external reality), or is reality shaped by our perceptions (subjective reality)?
- How do we categorize and classify things in the world?
- Epistemology and ontology are closely linked because they both help researchers decide how to approach their research and what to study

# Epistemology — The Study of Knowledge

## How do we know what we know?

### **What *is* a cybercrime?**

**Context:** A digital forensics investigator is trying to determine whether a phishing email should be considered a form of social engineering or a standalone cybercrime.

**Question:** What philosophical concern is being addressed?

- A. Epistemology
- B. Ontology
- C. Methodology
- D. Logic

# Epistemology — The Study of Knowledge

## How do we know what we know?

### Trusting the Evidence

**Context:** A forensic analyst is validating whether digital timestamps can reliably prove the time a file was accessed.

**Question:** Which concept is being explored?

- A. Ontology
- B. Epistemology
- C. Ethics
- D. Cryptography

# Epistemology — The Study of Knowledge

## How do we know what we know?

### Real or Virtual?

**Context:** A researcher questions whether digital identities (like avatars or social media profiles) are “real” identities in legal or philosophical terms.

**Question:** This reflects which philosophical perspective?

- A. Methodology
- B. Ontology
- C. Epistemology
- D. Digital Forensics

# Epistemology — The Study of Knowledge

## How do we know what we know?

### Can Logs Be Trusted?

**Context:** A security analyst relies on system logs to reconstruct an attack. They question if logs are tampered with or forged.

**Question:** What philosophical concern does this raise?

- A. Ontology
- B. Epistemology
- C. Logic
- D. Programming

# Epistemology — The Study of Knowledge

## How do we know what we know?

### Putting It All Together

**Context:** A digital forensics team believes that cyber incidents are socially constructed (e.g., insider threats motivated by culture), and thus uses interviews alongside log analysis.

**Question:** How do their **ontology** and **epistemology** align?

- A. Ontology: Objective reality; Epistemology: Use only technical logs
- B. Ontology: Reality is constructed; Epistemology: Use both social & technical data
- C. Ontology: Systems only exist when online; Epistemology: Use simulations
- D. Ontology & Epistemology: Always fixed

# Epistemology — The Study of Knowledge

## How do we know what we know?

### **Positivist Approach in Action**

**Context:** A forensic analyst insists on using only technical data (e.g., log files, network traffic, hashes) to determine the cause of a breach. They avoid interviews or subjective reports.

**Question:** What epistemological stance are they following?

- A. Interpretivist
- B. Positivist
- C. Constructivist
- D. Ethical Realism

# Epistemology — The Study of Knowledge

## How do we know what we know?

### Q7: Interpretivist Perspective

**Context:** An insider threat investigation includes interviews with employees to understand their motivations and experiences in the workplace. The goal is to understand how employees perceive security protocols.

**Question:** What epistemological stance is this?

- A. Positivist
- B. Interpretivist
- C. Objectivist
- D. Reductionist

# Epistemology — The Study of Knowledge

## How do we know what we know?

### Combining the Two

- **Context:** A digital forensics team collects technical data to identify breach origins but also interviews employees to explore how poor communication may have contributed.

**Question:** What approach does this reflect?

- A. Pure positivism
- B. Pure interpretivism
- C. Mixed-method epistemology
- D. None of the above

# Epistemology — The Study of Knowledge

## How do we know what we know?

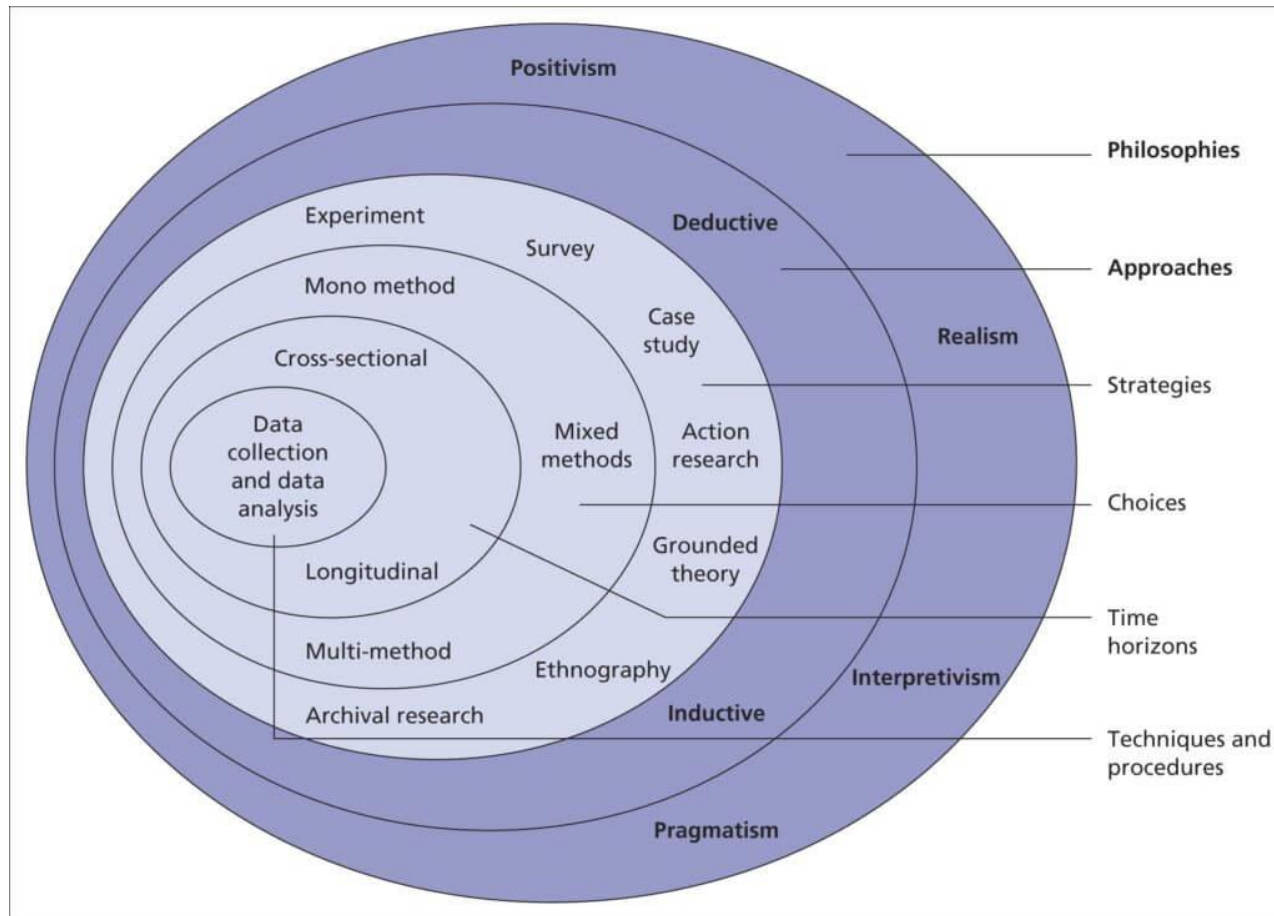
### Choose the Epistemology!

**Scenario:** A researcher studies how users *feel* about two-factor authentication by conducting focus groups and analyzing opinions.

**Question:** Which epistemological stance is most appropriate?

- A. Positivist
- B. Interpretivist
- C. Ontological
- D. Deductive

# Selecting Research Methodology Based on *Saunders et al.'s Research Onion Model*



# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Research Philosophy (Epistemology/Ontology)

**Question:** *What is the nature of reality and knowledge in your research?*

### Example:

A researcher believes that cyber incidents have objective causes that can be measured via logs and data.

→ **Philosophy: Positivism** (Objective reality exists, knowledge from observation)

### Alternative Example:

A researcher studies how employees *perceive* insider threat policies.

→ **Philosophy: Interpretivism** (Reality is socially constructed)

# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Positivism

### Description:

- Assumes reality is **objective** and can be measured.
- Knowledge is gained through **observable, quantifiable data**.
- Research is typically **deductive**, testing hypotheses.
- Often used in **quantitative studies**.

### Cybersecurity Example:

A researcher analyzes 200 system logs to determine if failed login attempts increase during specific hours, using statistical models.

- **Tools/Methods:** Log analysis, SPSS, automated data collection, experiments.

### Why Positivist?

The study is based on **measurable facts** and aims to discover generalizable patterns.

# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Interpretivism

### Description:

- Assumes reality is **socially constructed** and **subjective**.
- Knowledge comes from understanding **human experiences**
- **and meanings**.
- Research is often **inductive**, building theories from data.
- Common in **qualitative research**.

### Digital Forensics Example:

A researcher interviews forensic investigators to understand how they make judgment calls under pressure during live incident response.

- **Tools/Methods:** Interviews, observations, thematic analysis.

### Why Interpretivist?

The focus is on **individual perceptions** and **context**, not general laws.

# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Pragmatism

### Description:

- Believes that **the research question** should drive the philosophy and methods.
- Combines both **objective and subjective** views of knowledge.
- Often uses **mixed methods** (quantitative + qualitative).
- Focuses on **practical outcomes** and real-world solutions.

### Cybersecurity Example:

A researcher first analyzes phishing data trends (quantitative), then interviews users about why they clicked phishing links (qualitative), to improve future awareness training.

- **Tools/Methods:** Surveys + Interviews, Data + Contextual analysis.

### Why Pragmatist?

Solves a real-world problem by using **whatever methods best answer the question.**

# Selecting Research Methodology

## Based on *Saunders et al.'s Research Onion Model*

| Philosophy     | View of Reality         | Methods       | Example Context                                          |
|----------------|-------------------------|---------------|----------------------------------------------------------|
| Positivism     | Objective & measurable  | Quantitative  | Log file analysis for breach pattern detection           |
| Interpretivism | Subjective & contextual | Qualitative   | Interviews with forensic analysts                        |
| Pragmatism     | Mixed — practical focus | Mixed methods | Combine log analysis + user interviews to study phishing |

# Research Strategies

- Experiment
- Software Development
- Survey
- Case Study
- Action Research
- Ethnography

# Research Strategies

- **Experiment**
- Software Development
- Survey
- Case Study
- Action Research
- Ethnography

A **controlled and structured method** to test hypotheses by manipulating variables and observing the effect.

Testing whether one antivirus tool detects more malware than another by running both tools on the same infected system under lab conditions. Purpose: To measure cause and effect in a controlled setting.

# Research Strategies

- Experiment
- **Software Development**
- Survey
- Case Study
- Action Research
- Ethnography

The process of **designing, building, and testing a tool, system, or application** as part of solving a research problem.

Developing a custom tool that automates the detection of ransomware signatures in memory dumps.

Purpose: To create a functional solution and evaluate its effectiveness.

# Research Strategies

- Experiment
- Software Development
- **Survey**
- Case Study
- Action Research
- Ethnography

A method of collecting standardized data from a group of participants — usually via questionnaires or online forms.

Example in Cybersecurity: Distributing a questionnaire to 100 IT employees to understand their attitudes toward two-factor authentication.

Purpose: To gather data about opinions, behaviors, or demographics from a larger sample.

# Research Strategies

- Experiment
- Software Development
- Survey
- **Case Study**
- Action Research
- Ethnography

An in-depth exploration of a single case (or small number of cases), such as an event, organization, or individual.

Example in Digital Forensics: A detailed investigation of how a financial institution handled a major data breach, including interviews and document analysis.

Purpose: To gain rich, contextual insights into complex situations.

# Research Strategies

- Experiment
- Software Development
- Survey
- Case Study
- **Action Research**
- Ethnography

A collaborative approach where the researcher works with participants to identify a problem, implement changes, and evaluate the impact in real time.

Example in Cybersecurity Training: A researcher partners with an organization to develop a new employee cybersecurity training program, monitors its implementation, and adjusts it based on feedback.

Purpose: To improve practice through participatory change.

# Research Strategies

- Experiment
- Software Development
- Survey
- Case Study
- Action Research
- **Ethnography**

A long-term, immersive method where the researcher observes and interacts with participants in their real-world setting to understand cultural and behavioral patterns. Example in Digital Forensics: A researcher embeds within a SOC (Security Operations Center) team for 3 months to observe how analysts respond to real-time threats. Purpose: To deeply understand human behavior in its natural context.

# Research Strategies

| Strategy                    | Description                                     | Example in Cybersecurity / Forensics          |
|-----------------------------|-------------------------------------------------|-----------------------------------------------|
| <b>Experiment</b>           | Test cause-effect relationships under control   | Compare malware detection rates of tools      |
| <b>Software Development</b> | Build and test new systems/tools                | Develop a ransomware detection script         |
| <b>Survey</b>               | Collect standardized data from many respondents | Measure user awareness of phishing            |
| <b>Case Study</b>           | In-depth study of one case/event                | Analyze a company's breach response           |
| <b>Action Research</b>      | Research + real-time change with participants   | Co-developing a security policy with IT staff |
| <b>Ethnography</b>          | Long-term observation in natural settings       | Observe SOC team handling incidents           |

# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Research Approach

**Question:** *How will you use theory — build it up or test it?*

- **Deductive (Testing Theory):**

You start with a theory (e.g., phishing increases with poor training) and test it with data from multiple companies.

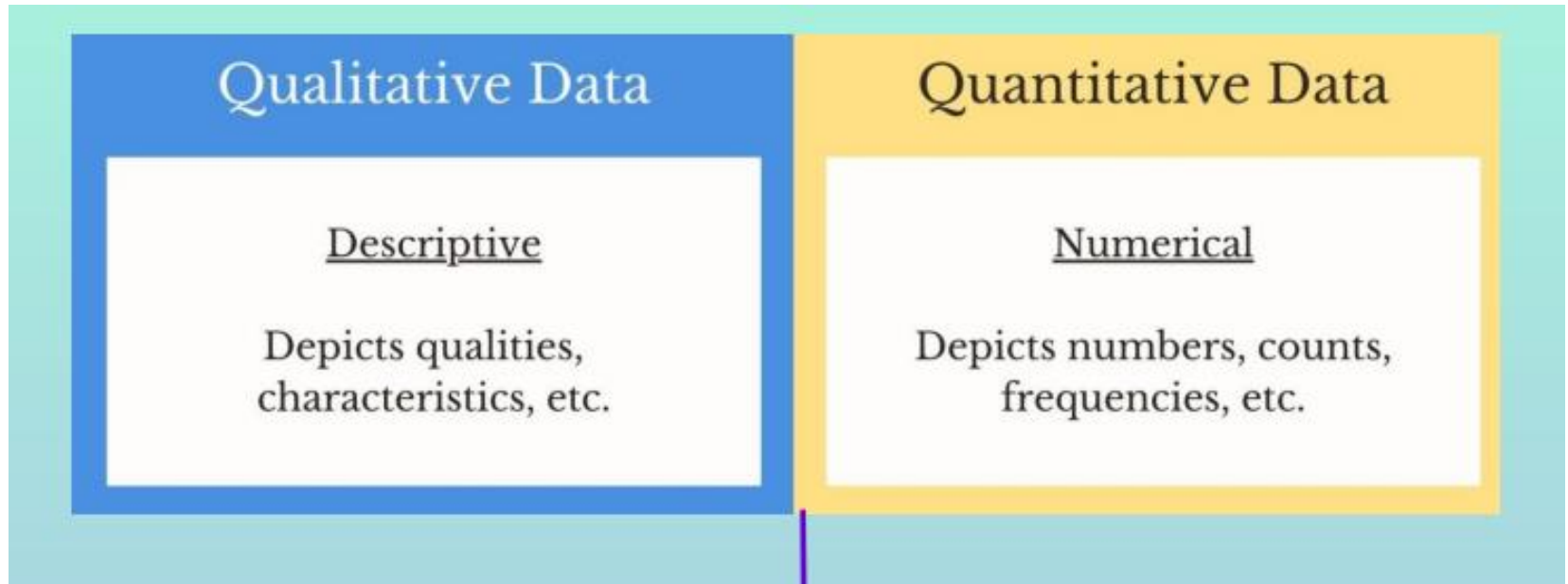
→ **Approach: Deductive**

- **Inductive (Building Theory):**

You collect interviews from employees about how they respond to phishing emails, and generate themes.

→ **Approach: Inductive**

# Research method - Qualitative Vs Quantitative



# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Methodological Choice

Question: What type of data will you collect?

Quantitative: Analyzing 100 incident reports for patterns in breach timing.

→ Choice: Quantitative (positivist aligned)

Qualitative: Conducting interviews with forensic investigators on investigation challenges.

→ Choice: Qualitative (interpretivist aligned)

Mixed Methods:

Combining both: data analysis and interviews. → Choice: Mixed Methods

# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

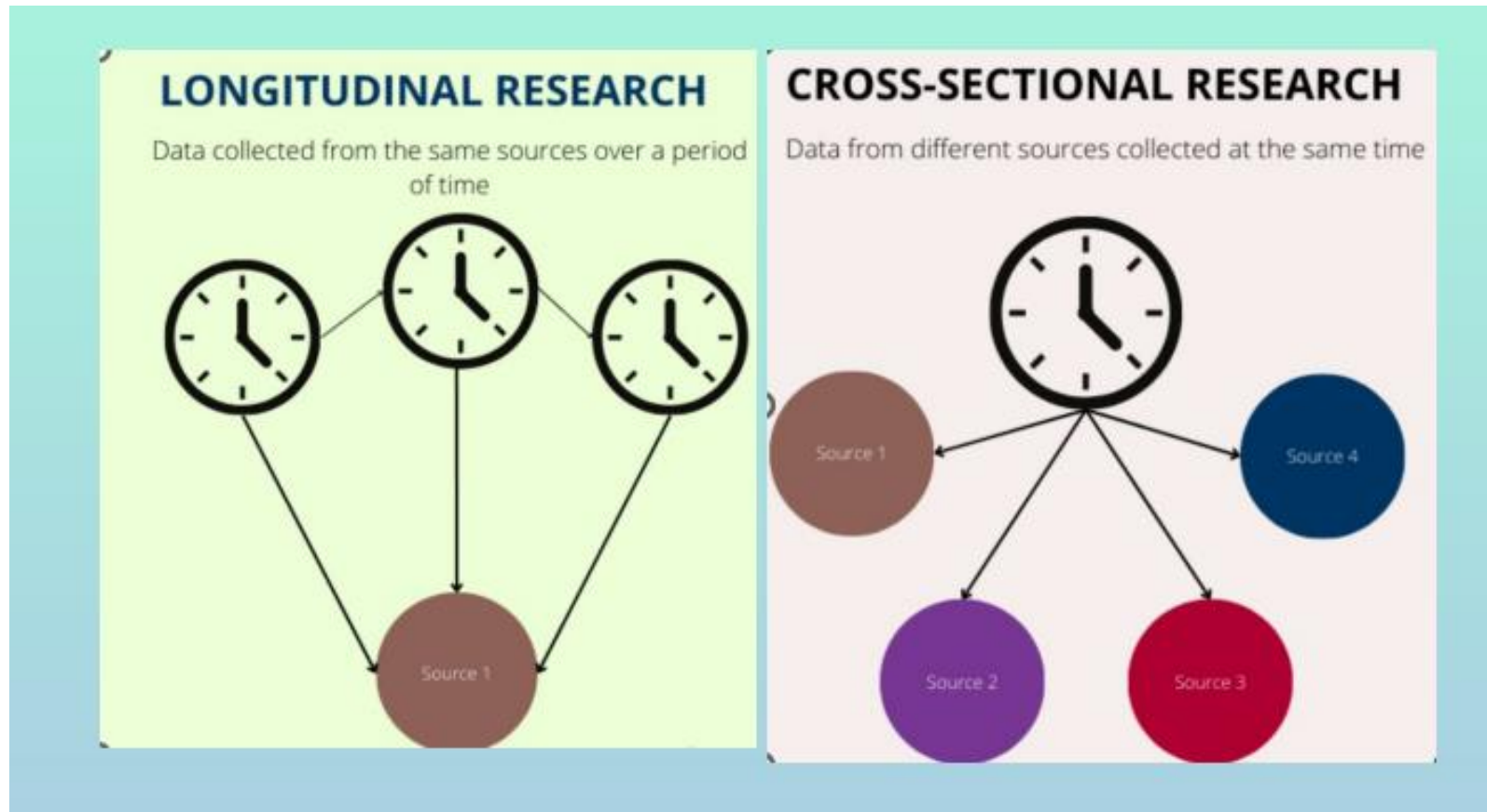
## Research Strategy

**Question:** *What method will you use to collect data?*

**•Example:**

- Case Study:** In-depth forensic analysis of a single ransomware attack
- Experiment:** Testing detection rates of two malware scanners
- Survey:** Asking analysts about tool effectiveness
- Ethnography:** Observing incident response team behavior

# Time Horizons – Longitudinal and Cross sectional



# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Time Horizon

**Question:** *Over what time period is your data collected?*

- **Cross-sectional:** One-time survey on incident response effectiveness

- **Longitudinal:** Tracking phishing resilience training outcomes over 6 months

# Selecting Research Methodology

Based on Saunders et al.'s Research Onion Model

## Data Collection & Analysis Techniques

**Question:** *How will you gather and analyze your data?*

- **Quantitative Tools:** Python scripts for log analysis, statistical tests
- **Qualitative Tools:** Thematic coding from interviews, NVivo

# Selecting Research Methodology

Based on *Saunders et al.'s Research Onion Model*

## Example Final Methodology Choice (Student Project)

**Title:** *“The Impact of User Training on Phishing Resilience”*

- **Philosophy:** Positivism
- **Approach:** Deductive
- **Methodology:** Quantitative
- **Strategy:** Survey
- **Time Horizon:** Cross-sectional
- **Tools:** SPSS, Excel

# Design Science Research (DSR)

- Design Science Research is a methodology used to **create and evaluate innovative artifacts** (tools, models, methods, or systems) that solve **real-world problems**.  
It's **common in computing, cybersecurity, and software engineering** research.

# Design Science Research (DSR)

## Key Steps in Design Science Research

- (Adapted from Hevner et al., 2004)

### Problem Identification & Motivation

Define the real-world problem and justify why it is important.

#### Example:

Many forensic tools fail to detect fileless malware attacks during memory analysis.

# Design Science Research (DSR)

## Key Steps in Design Science Research

- (Adapted from Hevner et al., 2004)

### Define Objectives for a Solution

Set clear goals the artifact must achieve (functionality, usability, efficiency).

#### Example Objective:

Create a lightweight tool that scans RAM snapshots for fileless attack patterns using custom heuristics.

# Design Science Research (DSR)

## Key Steps in Design Science Research

- (Adapted from Hevner et al., 2004)

## Design & Development

Build the actual artifact (tool, model, method).

### Example:

Develop a Python-based memory scanner that flags suspicious PowerShell commands executed in memory.

# Design Science Research (DSR)

## Key Steps in Design Science Research

- (Adapted from Hevner et al., 2004)

### Demonstration

Show how the artifact solves the problem using scenarios, simulations, or case studies.

Example:

Use a real-world memory dump infected by fileless malware to test the scanner and demonstrate detection.

# Design Science Research (DSR)

## Key Steps in Design Science Research

- (Adapted from Hevner et al., 2004)

## Evaluation

Measure the artifact's performance using metrics, expert review, or comparisons.

### Example:

Compare detection accuracy, speed, and false positives with existing forensic tools like Volatility.

# Design Science Research (DSR)

## Key Steps in Design Science Research

- (Adapted from Hevner et al., 2004)

## Communication

Share the results with practitioners and academics through reports, papers, or presentations.

### Example:

Publish a research paper or present the tool at a digital forensics conference.

# Design Science Research (DSR)

## Key Steps in Design Science Research

- (Adapted from Hevner et al., 2004)

| Step                   | Description                 | Cyber/Forensics Example                      |
|------------------------|-----------------------------|----------------------------------------------|
| Problem Identification | Recognize a gap or issue    | Fileless malware hard to detect in RAM       |
| Define Objectives      | Set solution goals          | Build a tool that detects stealth techniques |
| Design & Development   | Build the artifact          | Create a Python RAM scanner                  |
| Demonstration          | Use the artifact in context | Test on infected memory dump                 |
| Evaluation             | Assess the effectiveness    | Compare detection accuracy                   |
| Communication          | Share the results           | Present findings in thesis/conference        |

# Reference

- [1]. M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, 5th ed. Harlow, U.K.: Pearson Education, 2009.
- [2] S. Mardiana, "Modifying Research Onion for Information Systems Research," *Solid State Technology*, vol. 63, no. 4, pp. 5304-5313, 2020.
- [3] W. Kuechler and V. Vaishnavi, "The emergence of design research in information systems in North America," *Journal of Design Research*, vol. 7, no. 1, pp. 1–16, 2008.
- [4] T. Faste and H. Faste, "Demystifying 'design research': Design is not research, research is design," in *Proceedings of IDSA Education Symposium 15*, 2012.
- [5] T. J. Ellis and Y. Levy, "A guide for novice researchers: Design and development research methods," in *Proceedings of the Informing Science & IT Education Conference (InSITE)*, Citeseer, pp. 107–118, 2010.
- [6] A. Hevner and S. Chatterjee, "Design science research in information systems," in *Design Research in Information Systems*, Springer, pp. 9–22, 2010.
- [7] A. Hevner, S. T. March, J. Park, and S. Ram, "Design science research in information systems," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.
- [8]. K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.
- [9] H. A. Simon, *The Sciences of the Artificial*, MIT Press, 1996.

# Activity- Research Methodology (Week 5)



<https://forms.office.com/e/ca1W271MwE>