# Internship Experience

## IT Security

**Will Kittredge | 8/4/2025**

# Goal & Outline

***What does a security analyst do?***

1. Foundational concepts
2. What we're up against
3. My internship

The goal of this presentation is to answer the question: ***"What does a security analyst do?"***

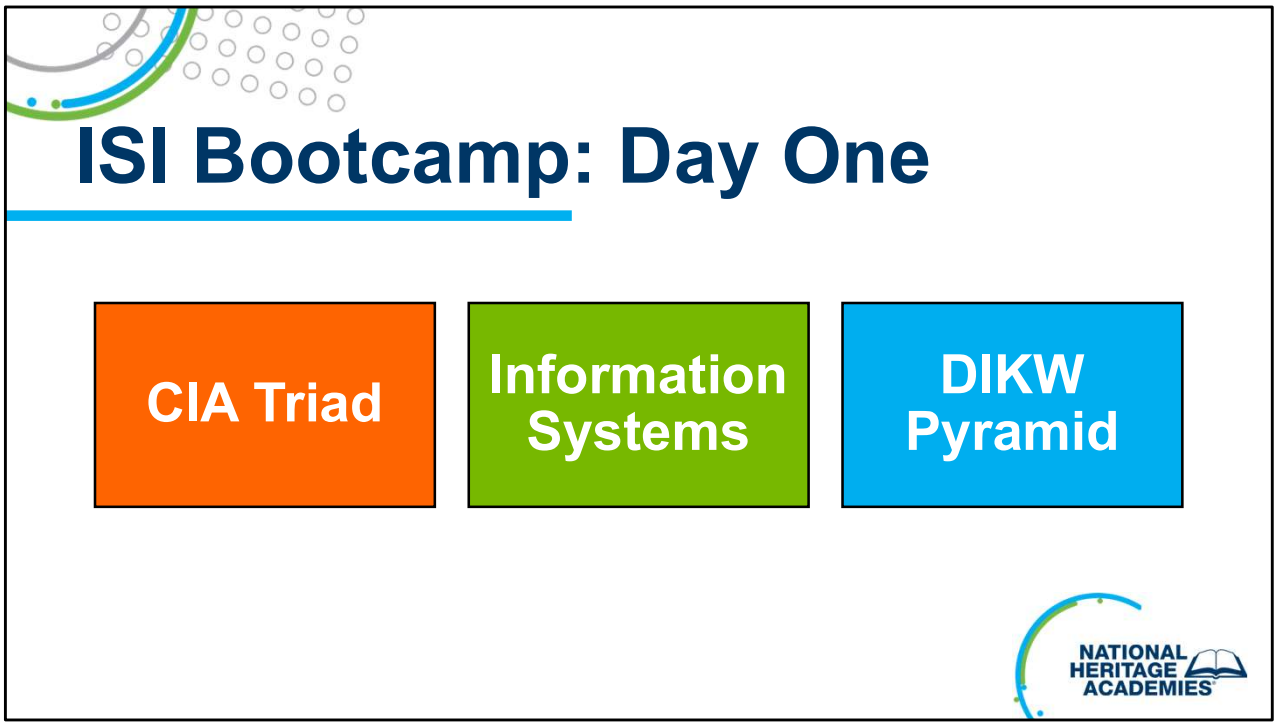
We're going to cover three main topics:
1. Foundational information security concepts
2. What we're up against ("we" refers to analysts at NHA)
3. My internship experience (what we did)

# What does a security analyst do?

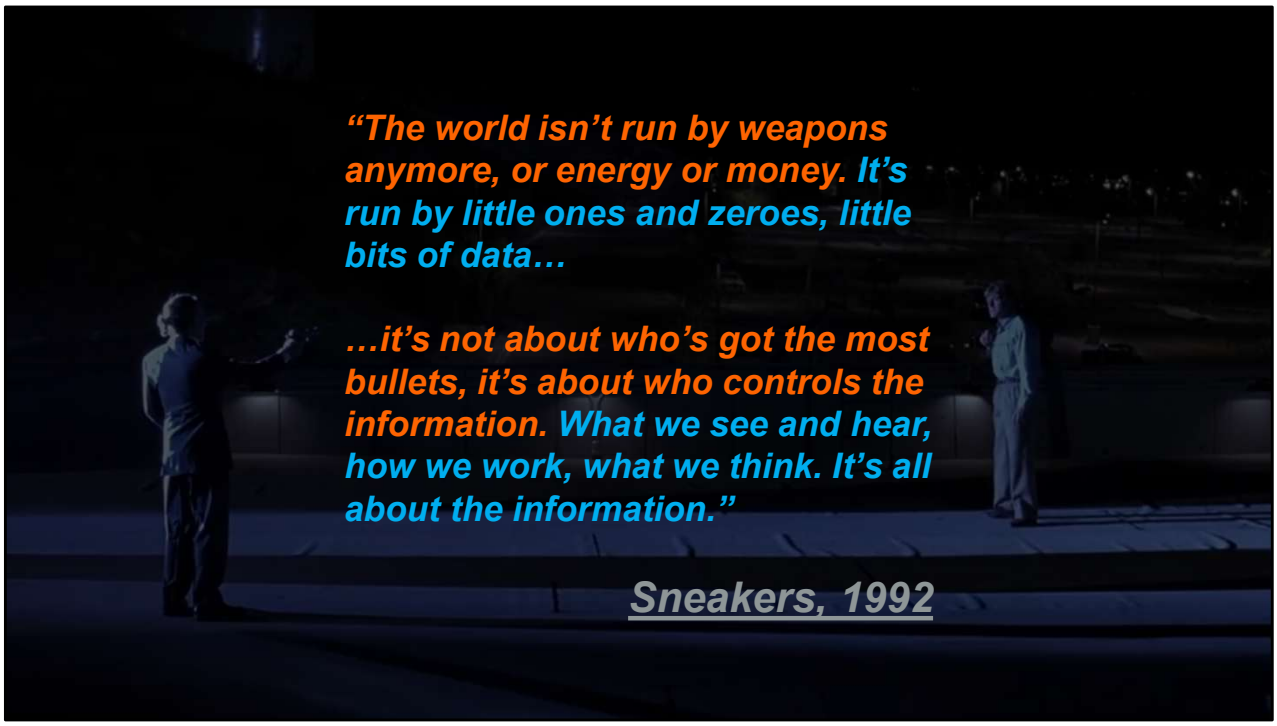
So, what does a cybersecurity analyst do? This is the #1 question that people ask me. I won't call on anyone, but I want you to think about your answer for a second.

My professor asked us the same question on our first day in class. To be honest, the answer that he gave us wasn't anything like what I was expecting or had come up with.

**I'm going to tell you what they taught me in day one of ISI** (Information Security and Intelligence, our cybersecurity program at Ferris) **bootcamp.**




1. **The CIA Triad** – How we protect information (not the three-letter agency).
2. **Information Systems** – The environment that we work in.
3. **The DIKW Pyramid** – What we're doing.




Before we continue, I wanted to share this quote that I think about often. The most important parts are in bold. This quote comes from the movie *Sneakers*:

*“**The world isn’t run by weapons anymore, or energy or money**. It’s run by little ones and zeroes, little bits of data… **it’s not about who’s got the most bullets, it’s about who controls the information**. What we see and hear, how we work, what we think. It’s all about the information.”*

Everything that we do traces back to information and controlling information.

By the way, I highly recommend that you watch *Sneakers*! You might even say it’s the real point of this presentation (kidding). It has a great cast and a fun story.

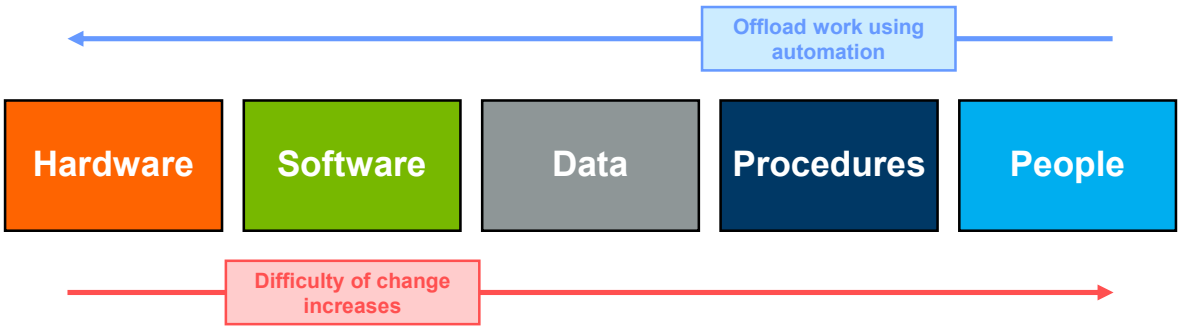
*Sneakers* is from 1992. The World Wide Web wasn’t open to the public until 1993. Most people didn’t have a glimpse of what the modern world would be like, but *Sneakers* hit the nail on the head.


This slide shows the **confidentiality, integrity, and availability (CIA) Triad.**

When I say that *"it's about who controls the information,"* I'm talking about controlling these three aspects:

- **Confidentiality:** The information can only be accessed by approved parties.
- **Integrity**: The information hasn't been changed in any unauthorized or unexpected way.
- **Availability:** The information can be accessed when we need it.

# INFORMATION SYSTEM



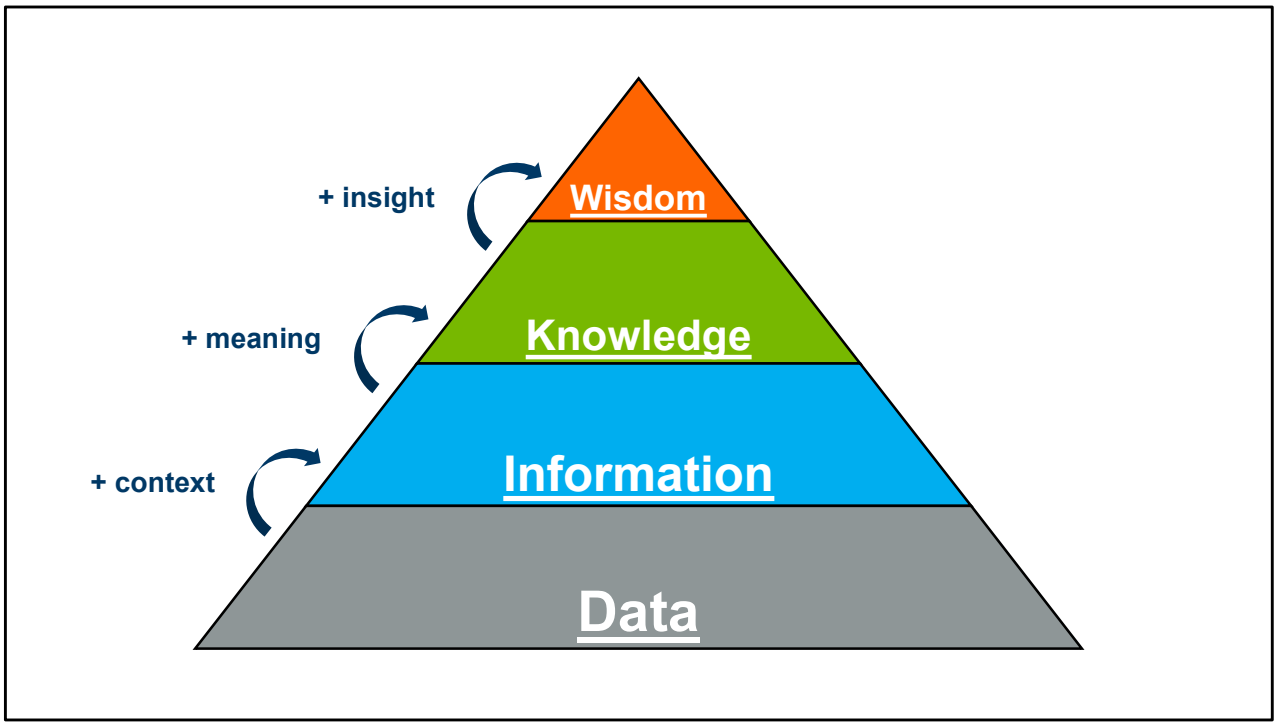

This slide shows an **information system.** Modern information systems operate with humans and computers.

Broadly speaking, we operate within information systems. Business rely on them to process information and make decisions.

**Data** is the *actual events* the system is reacting to and the *bridge* between humans and computers.
**Procedures and software** are the *instructions* for how to react to data.
**People and hardware** are the *actors* that enact the instructions.

We offload work to computers using automation because it is easier for them to enact changes, and it frees up time for us to spend on more important things.

We keep these information systems secure by ensuring that confidentiality, integrity, and availability is maintained.




This slide shows the **Data/Information/Knowledge/Wisdom (DIKW) Pyramid.**

- **Data** is raw signals and events. Given *context* it becomes…
- **Information** is useful, organized, and structured. Given *meaning* it becomes…
- **Knowledge** is contextual and synthesized learning. Given *insight* it becomes…
- **Wisdom** is understanding, integrated, and actionable.

Analysts transform data into wisdom. The **data** that our security systems collect is transformed into **information** for us to look at. Using this, we can determine what the information means to gain some **knowledge** of a situation. All of this is used, along with our education and experience, to add insight to what we've learned so that we can make a **wise** decision.

Example:
*"Based on **[x]** information that we validated from **[y]** source data, we learned that **[z]** has occurred and believe that it would be wise to do **[a]** in response."*

# 1,443,324,310

***One billion, four hundred and forty-three million, three hundred and twenty-four thousand, three hundred and ten***

*What is this number?*
**1,443,324,310** (One billion, four hundred and forty-three million, three hundred and twenty-four thousand, three hundred and ten)

This is the number of "**events processed**" inside Rapid7 InsightIDR, one of the main pieces of security software that we use, in just the **last week.**

- This means roughly 200 million events per day (24 hours).
- Do you ever feel like you have information overload?

Keep in mind, it's currently the middle of summer. **This is the slow season.** At the beginning of the internship when school networks were more active, there were roughly 800 million events per day (24 hours). This means about four times the number of events processed per week compared to now.


I've referred to events for the last three slides, but **what is an event?**

An event is essentially anything that happened in an information system that we have a record of. This could be:

- Somebody visiting a website
- Somebody using their ID badge to enter a room or building
- Somebody launching a program on their work laptop
- Etc.

It's important to understand that an event does not necessarily need to happen on a computer (although this usually is the case).

# Information Overload

- >1 billion events, ≈1 million emails ***per week***
- 100+ schools
- 7 team members
  - 1 director and 1 manager
  - 3 full time
  - 2 interns

NATIONAL HERITAGE ACADEMIES

1.4 billion events in a (slow) week sounds like a lot.

Remember the information overload I mentioned earlier?
- >1 billion events per week
- >1 million emails per week
- Thousands of students and employees
- Thousands of devices
- 100+ schools

All of this is handled by **7 team members**:
- 1 director
- 1 manager
- 3 full time analysts/architects
- 2 interns

**How do we do it?**

# Handling Information

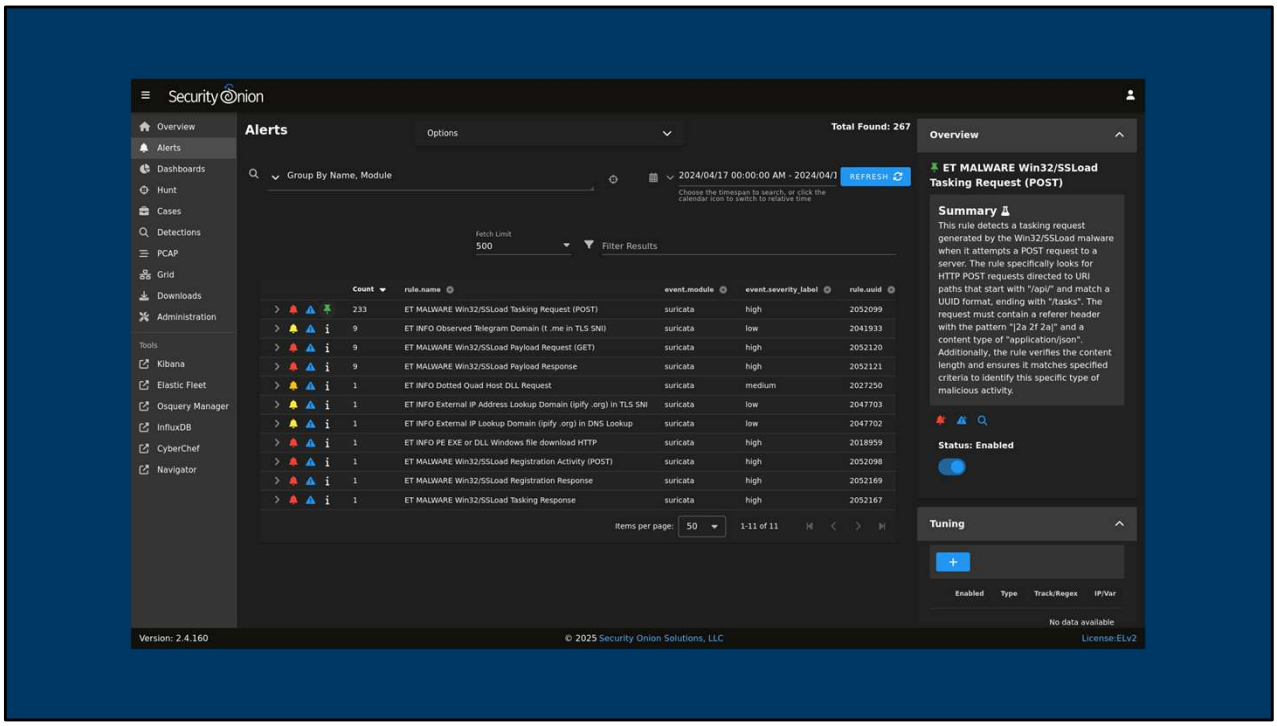
***We rely heavily on tools and automation to give analysts more time to spend on the things that matter.***

- InsightIDR SIEM
- InsightConnect automation
- Misc. tools (PhishER, VirusTotal, etc.)

**Tools and automation give analysts more time to spend on the things that matter.**

We rely heavily on multiple tools and tool automations that allow us to handle large volumes of information, enforce security controls, and investigate events. Here are a few:

- Rapid7 InsightIDR SIEM
- Rapid7 InsightConnect automation
- Microsoft Defender XDR SIEM
- Security Onion SIEM
- Cisco Umbrella
- KnowBe4 PhishER SOAR
- ANY.RUN malware sandbox
- VirusTotal threat intelligence




As part of the internship, Caydon and I worked on two projects that involved deploying tools/automation:

- Security Onion SIEM
- InsightConnect automation workflows

An example screenshot of the Security Onion alert dashboard is visible on the slide. This tool is like Rapid7 InsightIDR and will allow us to explore events on the Service Center network in more detail. Deployment involved creating and proposing a project plan, updating all of the old nodes, and testing the grid.

The screenshots that Caydon showed in his presentation come from the automation workflows project, where we used Rapid7 InsightConnect to streamline various everyday tasks and save valuable time. The main automation tool we created allows us to send tickets to the TeamDynamix system via Slack messages with an interactive builder. It has built in error detection, error handling, documentation, help messages, and ticket status reporting.

# Thank you!