IT Security Analyst
Core IT Pathway

An IT Security Analyst (or Security Operations Center Analyst) supports the detection, containment, and remediation of IT threats. They monitor networks/applications to identify a possible cyber-attack or intrusion and help coordinate and report on cyber incident responses. IT Security Analyst provides analysis and trending of security log data, Incident Response (IR) support, and threat and vulnerability analyses.

Because businesses are becoming more and more vulnerable to cyber security threats, this position has grown in importance and will continue to see increased opportunities.

4 Courses, 5 Certifications, 8 Credits	218 Hours
Foundations in Information Technology	**Cloud Services Administration Fundamentals**
IT Security Operations	**Business Skills Workshops**

5 Certifications*	CompTIA | Microsoft
CompTIA Tech+ CompTIA Network+ Microsoft Azure Fundamentals	Microsoft Security, Compliance, and Identity Fundamentals CompTIA Security+

Project

Students will build and maintain a virtual security operations center (SOC) through which they will analyze IT security events, respond to vulnerabilities, take incident response actions and generate incident response reports. Standard operating procedures will be created for the ongoing review and maintenance of the virtual SOC.

Certificate of Completion	College Credits
Students who pass all the courses and pass at least 50% of the certification exams receive a **Certificate of Completion** that represents successful completion of the IT Security Analyst program.	Whether or not you plan to continue your formal education immediately after completing a NuPaths' program, you'll earn college credits that you can apply toward a college degree. Students have the potential to earn up to **8 college credits** in the IT Security Analyst program.

Course Descriptions

Foundations in Information Technology

The course focuses on the basics of computer hardware, software, mobile computing, networking, troubleshooting, and emerging technologies. Students learn about configuring operating systems, networks and network configuration, and the role of the OSI model in networking and troubleshooting. A fundamental understanding of computer hardware, operating systems, computer software, networking technology, web browsers, security risks, troubleshooting, and system maintenance is gained. The course also explores cutting-edge technologies such as cloud computing and virtualization.

Cloud Services Administration Fundamentals

Students learn to design, implement, and analyze networks by configuring, managing, securing, and maintaining essential network devices. The course also explores cloud computing for sharing services with multiple users and providing administrative control of data storage and applications, and how those services are provided with Microsoft Azure.

IT Security Operations

The course addresses the vital fundamentals of security to support the principles of confidentiality, integrity, and availability. Security layers, authentication, authorization, and accounting are explored, along with network security to protect the Server and Client. Students also learn to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations.

Business Skills Workshops

This course focuses on the business or "soft" skills that allow people to interact effectively and productively; skills like collaboration, communication, emotional intelligence, and time management.

Technology Experience Gained

Azure . Cloud . Network management . DNS . TCP/IP . Network protocols and topologies . Active Directory . System recovery . Anti-malware products . Firewalls . Wireless router/switch . External storage . Mobile devices . Network ports . Malware detection . Social engineering . Application/service attacks . Wireless attacks . Cryptographic attacks . Penetration testing . Vulnerability scanning Security architecture . Identity and access management . Risk management . Cryptography and PKI.

*Third party certification providers give certification exams that must be successfully completed as per their requirements.