XALTIUS
Towards Higher Excellence

Job Oriented Certification Program in

Cyber Security

Our live in-person or online program. Become a cybersecurity professional in as little as 24 weeks.

Includes 2 months of certified internship!

6 MONTHS

www.xaltiusacademy.com

FROM DIRECTOR'S DESK

Vertex,
33 Ubi Avenue 3,
#06-53,
Singapore, 408868

Greetings!

Every educational institute needs to implement valuable learning. Xaltius creates a positive attitude and inspire the students to achieve professional excellence in the most memorable way.

The need to modify and adapt is continuous and at Xaltius Academy we appreciate this opportunity as we believe it brings out the best in us, helping us strive further to provide valued learnings at all times.

We are motivated to remain an innovative with our best education level, surpassing our students in providing them a better experience.

We help our students by providing them transformational information solutions so that they can have the bright future to build innovative and intelligent ideas.

As we embark upon our journey to the exciting times ahead, we will continue to co-innovative with our education to ensure profitable growth and ever increasing value by creating an inspiring environment for our students.

Desmond Sek
Co-founder & Director

LETTER

Table of Contents

Why Cybersecurity?

You are living in unprecedented times in the course of technological development. The world has fully adopted the most transformational technology in its history before figuring how to deal with its inherent—and very real—risks. The Internet is revolutionizing the world. We are totally dependent on it. But, it wasn't designed with security in mind. We have traded our personal security for convenience.

That's where cybersecurity comes in. This relatively new, exploding industry is on a mission to secure a world that suddenly finds itself running on the Internet, and thereby enabling the future potential of technology itself. The world needs more cybersecurity professionals.

Whether you have zero cybersecurity knowledge, are self-taught, or are somewhere in between, our course is crafted for anyone. Graduates are prepared for a variety of career paths. Here are a few of the most common:

COMMON CYBERSECURITY CAREER PATHS

CYBERSECURITY ENGINEER | Average salaries: $109,749

Cybersecurity Engineers, sometimes called Information Security Engineers, identify threats and vulnerabilities in systems and software, then apply their skills to developing and implementing high-tech solutions to defend against hacking, malware and ransomware, insider threats and all types of cybercrime. (salary from ZipRecruiter, as of April 2022)

NETWORK ADMINISTRATOR | Average salaries: $66,751

A Network Administrator is responsible for keeping an organization's computer network up-to-date and operating as intended. Any company or organization that uses multiple computers or software platforms needs a network admin to coordinate and connect the different systems. (salary from ZipRecruiter, as of April 2022)

SECURITY ANALYST | Average salaries: $83,549

Security Analysts are ultimately responsible for ensuring that the company's digital assets are protected from unauthorized access. This includes securing both online and on-premise infrastructures, weeding through metrics and data to filter out suspicious activity, and finding and mitigating risks before breaches occur. (salary from ZipRecruiter, as of April 2022)

SECURITY CONSULTANT | Average salaries: $87,922

A Security Consultant works as an advisor and supervisor for all security measures necessary to effectively protect a company or client's assets. Security Consultants use their knowledge and expertise to assess possible security threats and breaches in order to prevent them and create contingency protocols and plans for when violations occur. (salary from ZipRecruiter, as of April 2022)

PENETRATION TESTER | Average salaries: $105,984

Penetration Testers help organizations identify and resolve security vulnerabilities affecting their digital assets and computer networks. (salary from ZipRecruiter, as of April 2022)

Program Overview

Network Security
This course will focus on the core ideas in network security - Ethernet, WIFI, attacks on TCP hijacking, and more.

Systems Security
This course will focus on System Architecture, Operating System Architecture, System Exploits (hardware, operating system and memory). Learn to utilize tools such as Metasploit and command line tools in Linux.

Threat Intelligence
The course teaches techniques organized around military principles of intelligence analysis and introduces larger concepts of how cyberspace has become a new warfighting space

Governance, Risk Management, and Compliance
This course covers how to engage all functional levels within the enterprise to deliver information system security. The course addresses a range of topics on securing the modern enterprise.

Logs & Detection
This course will focus on engineering solutions to allow analyzing the logs in various network devices, including workstations, servers, routers, firewalls and other network security devices.

Python
This course provides the fundamental structure and language for creating Python scripts and automation. The focus will be on learning basic coding, code analysis and secure coding practices.

Application Security and Penetration Testing
This course focuses on applications and their vulnerabilities running on both workstations and servers. You'll learn penetration testing for vulnerabilities either in applications or network resources.

Applied Cryptography
This course teaches the components of cryptography, provides hands-on experience on configuring a web server with SSL/TLS, and interfacing with Certificate Authorities, issuing certificates, configuring SSH securely, and sending/receiving encrypted and signed email.

Capstone
The group project will present a scenario and allow the students to work within their individual expertise to work through the particulars. The project will culminate in a professional level oral and written report, which can be used as part of a portfolio.

PROGRAM OUTLINE BY PHASE

		HOURS	DAYS
PHASE 1	**Cybersecurity Foundational Skills** Systems Security, Network Security, Applied Cryptography, GRC, & Python	24	8 (4 weeks)
PHASE 2	**Cybersecurity Intermediate Skills** Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, & Python	36	12 (6 weeks)
PHASE 3	**Cybersecurity Skills Development** Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, & Logs and Detection	24	8 (4 weeks)
PHASE 4	**Gray Hat Hacking** Systems Security, Network Security, Logs and Detection, Application Security and Penetration Testing, & GRC	30	10 (5 weeks)
PHASE 5	**Cybersecurity Skills Application** Systems Security, Network Security, Logs and Detection, Application Security and Penetration Testing, & Capstone	30	10 (5 weeks)
PROGRAM TOTAL		144	

Curriculum

Cybersecurity Engineering Prep

All students are required to complete what we call “Cybersecurity Engineering Prep” before the start of class. During the prep course, students will get accustomed to the platform, set up their virtual machines, and obtain a basic understanding of Python, Systems, and Networks to prepare them for day 1 of class.

The prep course generally takes between 10-20 hours to complete, and is bookended by a pre-test and post-test to assess understanding of the concepts covered.

Network Security

This course will focus on the core ideas in network security. The first portion of the class will continue review of basic network protocols: Ethernet, 802.11 (WiFi), IP, UDP, TCP, ARP, DHCP, DNS, ICMP, BGP, SMTP, POP/IMAP, FTP, HTTP, IGMP, and the attacks on these basic technologies: TCP hijacking, ARP cache poisoning and domain spoofing, as well as countermeasures. We then explain sniffing and port scanning, firewalls, IDSes and NIDSes and cover wireless protocols and their security. Then we segue into AppSec with a focus on web security. Finally, we look at denial of service and attack payloads.

At the completion of this course, a student will be able to:

- Utilize the layers of the TCP/IP and OSI models in analyzing network protocols.
- Analyze packet captures and draw conclusions about network activity.
- Create a web application and evaluate its security.
- Explain network security protocols as well as their vulnerabilities.
- Utilize attack tools to mount attacks against various types of 7 networks and use countermeasures to forestall these same attacks.
- Map ports on a given IP, fingerprint services, catalog vulnerabilities, bypass firewalls, and mount a large array of web-based exploits.
- Deliver a wide variety of payloads to attain and maintain backdoor access to a compromised machine.

TOOLS LEARNED

WIRESHARK
LAMP STACK
WEB SPIDERS
HONEYPOTS
MARAI BOTNET
IOT
TCP HIJACKING
ETHERNET SNIFFING
DNSSEC
SQL/INJECTION
IP FUNDAMENTALS
FIREWALLS, WAFS
NETCAT
PORT SCANNING
WPA/AIRCRACK-NG
ARP CACHE/POISONING
FILTERING AND REGEX
IDS/IPS
SOAP/REST
XSS

TOOLS LEARNED

WINDOWS
LINUX SYSTEM
BASH SHELLS
LINUX SEC MODEL
AUTHENTICATION
ACTIVE DIRECTORY
OWASP
BASIC C CODING
LINUX COMMAND
ASSEMBLY BASICS
BUFFER OVERFLOW
SHELLCODE INJECTION
METASPLOIT PAYLOADS
METERPRETER
ROOT KITS
CLOUD SECURITY
HYPERVISOR EXPLOITS
IOS SECURITY

Systems Security

This course will focus on System Architecture, Operating System Architecture, System Exploits (hardware, operating system and memory). We will also utilize tools, including Metasploit and command line tools in Linux (xxd, gdb, etc) for further analysis of exploits. We will explore exploits and their countermeasures, including buffer overflows, TOCTOU, shellcode injections, integer overflows and off-by-one errors. We will also cover basic Cloud security and migration considerations, Hypervisor Exploits and Android and iOS security.

At the completion of this course, a student will be able to:

- Understand the foundations of working in security culture as a
- security professional.
- Develop solid resumes showcasing skills attractive to hiring managers and partners and demonstrate the ability to interview for cybersecurity roles..

TOOLS LEARNED

OPERATIONAL DESIGN
OPEN SOURCE INTELLIGENCE (OSINT)
MALTEGO
SOCIAL ENGINEERING
CYBER THREAT INTELLIGENCE CYCLE
INTELLIGENCE PREPARATION OF THE ENVIRONMENT
CYBER KILL CHAIN
ACTIVE CYBER DEFENSE MODEL
CENTER OF GRAVITY ANALYSIS
CARVER MATRIX

Threat Intelligence

The course teaches techniques organized around military principles of intelligence analysis and introduces larger concepts of how cyberspace has become a new warfighting space that targets private and public critical infrastructure, and economic and national security targets across all sectors globally. Students must understand the overall threat environment, how to discern the "so what" of information, and critically think and analyze complex human influenced cyber problems and threats to public and private information enterprises. Threat Intelligence 200 introduces students to the various methodologies of intelligence analysis and planning. Students will learn about the Cyber Kill Chain, Center of Gravity (COG) Analysis and CTI Diamond Model and then learn how to apply them using Cyber Intelligence Preparation of the Environment (IPE). The class, Cyber Mission Analysis, will culminate with students presenting their Mission Analysis Brief to the instructor as if they are the CISO.

A high-level perspective of threat intelligence (its creation and consumption):

- Adversary monetization methods
- Intelligence analysis
- Intelligence gathering
- Planning with intelligence
- Intel sources

TOOLS LEARNED

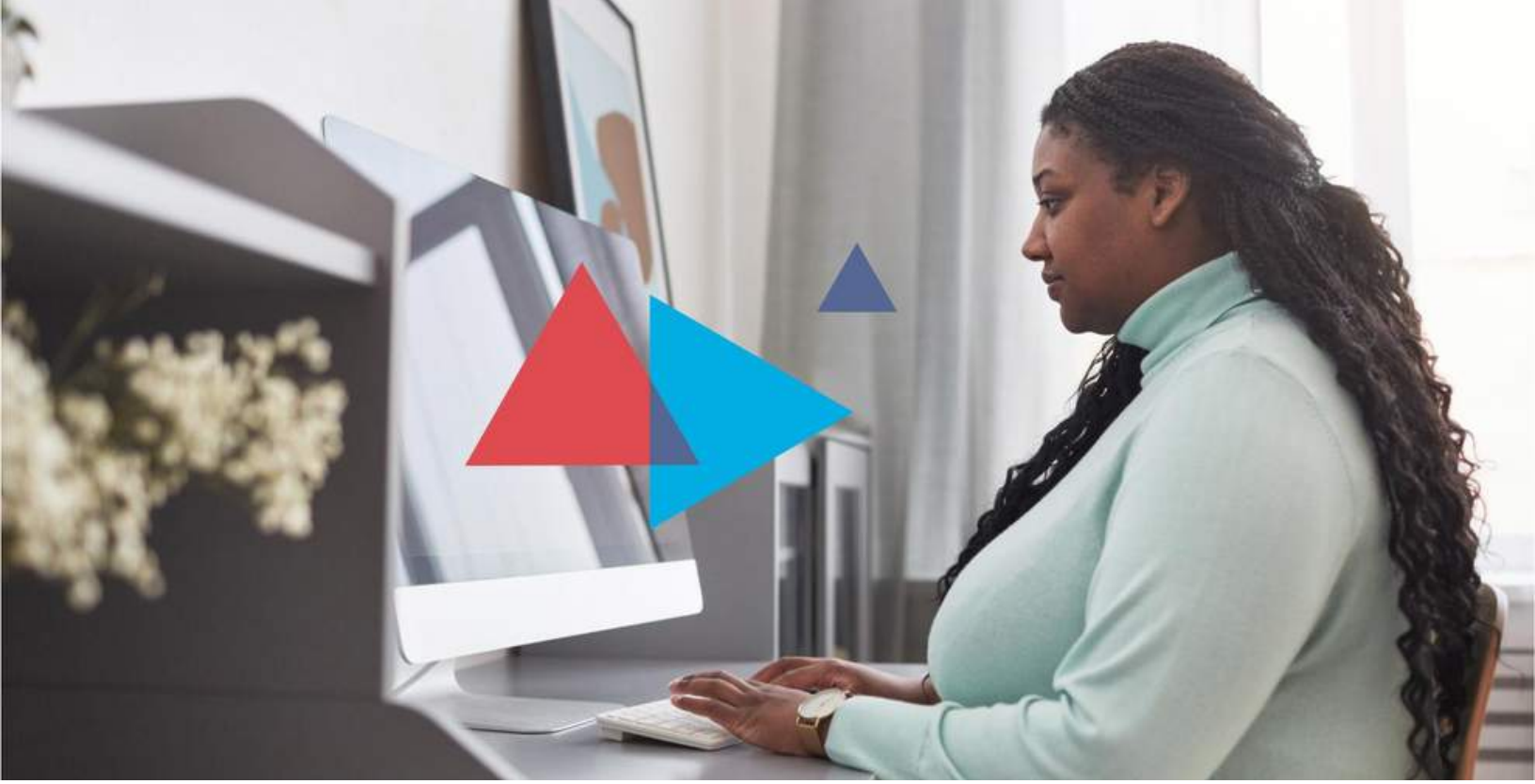
ISO/IEC 38500
COBIT 5
ISO/IEC 27001
OCTAVE
NIST
ITIL
RISK MANAGEMENT FRAMEWORK
CIA MODEL
BUSINESS IMPACT ANALYSIS
IDENTITY AND ACCESS MANAGEMENT

Governance, Risk Management and Compliance

This course will focus on Governance, Risk, and Compliance (GRC). Students will learn how to engage all functional levels within the enterprise to deliver information system security. These topics include plans and policies, enterprise roles, security metrics, risk management, standards and regulations, physical security, and business continuity. Each piece of the puzzle must be in place for the enterprise to achieve its security goals; adversaries will invariably find and exploit weak links. By the end of the course, students will be able to implement GRC programs at the maturity level that many organizations are not at currently and to establish efficient, effective, and elegant Information Security Programs.

A high-level perspective of threat intelligence (its creation and consumption):

- Plans and policies
- Risk management
- Physical security
- Enterprise roles
- Standards and
- Business continuity
- Security metricsregulations



TOOLS LEARNED

CYBER KILL CHAIN AND LOGGING
REGEX
LOGSTASH AND FILEBEAT CONFIGURATION
NETWORK MAPPING
NORMALIZATION
SIEM ARCHITECTURE & AUTOMATION
DATA VISUALIZATIONS
KIBANA
SPLUNK

Logs and Detection

This course will focus on engineering solutions to allow analyzing the logs in various network devices, including workstations, servers, routers, firewalls and other network security devices. We will explore the information stored in logs and how to capture this data for analyzing these logs with a Security Information and Event Manager (SIEM). We will learn the steps involved in Incident Response and Crisis Management.

At the completion of this course, a student will be able to:

- Identify log sources and the configurations necessary to achieve appropriate logging levels.
- Describe the different types of data contained in log files.
- Configure data sources and SIEMs to allow the analysis of log data, including the automation of those tasks.
- Identify steps in Incident Response and Crisis Management..

TOOLS LEARNED

PYTHON 2.X
PYTHON 3.X
PYTHON IDES
CONDITIONALS
LOOPS
DATA STRUCTURES

Python

Python programming is a fundamental skill used by Cybersecurity Engineers. This course provides the fundamental structure and language for creating Python scripts and automation. The focus will be on learning basic coding, code analysis and secure coding practices.

Python 100 will cover the differences between interpreted and compiled coding languages. The focus for the interpreted languages will be the basic code structure for Python, conditionals, loops and algorithm diagramming tools. Students will work on analyzing basic code, modify that code to add additional functionality and writing simple algorithms.

Python 200 will dive deeper into topics such as more advanced algorithms and Object Oriented Programming. Secure coding techniques and methodologies will also be covered, including standard frameworks.

Python code will be utilized in other courses, such as Networking, Systems and Cryptography.

At the completion of this course, a student will be able to:

- Analyze Python scripts to determine what functionality they provide.
- Write simple Python scripts using conditionals, loops, variables and other
- data structures.
- Import modules to increase the functionality of the Python script.
- Use coding frameworks to ensure secure coding techniques are utilized.

TOOLS LEARNED

PENETRATION TESTING EXECUTION STANDARD (PTES) FRAMEWORK
METASPLOIT
OPENVAS
NMAP
SHELLCODE GENERATION
FUZZING
ROOTKITS
BURP SUITE

Application Security & Penetration Testing

Application Security focuses on the applications and their vulnerabilities running on both workstations and servers. Penetration testing is using vulnerabilities either in applications or network resources that allows for exploitation. This can lead to server downtime, service interruptions or in the worst case, root level access for the malicious actor. This course focuses on methodologies utilized by penetration testers to analyze and assess risk to systems, networks, applications and other vulnerable areas of concern to a company. These are the same techniques used by malicious actors to compromise a company. The role of the penetration tester is critical in finding the vulnerabilities and risks before they can be exploited.

APP100 will focus on the basic techniques and tools employed by a penetration tester or hacker. The focus will be on the Penetration Testing Execution Standard (PTES) framework for determining where a company has exposure, testings the vulnerabilities, and basic approaches to exploiting the vulnerabilities. Additionally, network mapping will be revisited and specific techniques for reconnaissance will be discussed.

APP200 will look at specific exploits and how they can be utilized to more efficiently target and exploit systems and networks. The focus will be on crafting specific exploits based on the results of the reconnaissance techniques. Finally, post exploitation activities and reporting will be discussed.

At the completion of this course, a student will be able to:

- Describe the usage of Metasploit and other Kali Linux pentesting tools.
- Describe the Penetration Testing Execution Standard (PTES).
- Utilize attack tools to mount attacks against various types of networks and applications and use countermeasures to forestall these same attacks
- Deliver a wide variety of payloads to attain and maintain backdoor access to a compromised machine and actions to combat these attacks, as well.

TOOLS LEARNED

BASIC SYMMETRIC CIPHERS
DES/3DES
AES
MODES OF OPERATION
HASH FUNCTIONS
AUTHENTICATION (HMAC)
RSA
OPENSSL
BITCOIN
SSLSTRIP

Applied Cryptography

This course in Applied Cryptography teaches students the components of cryptography, provides hands-on experience on configuring a web server with SSL/TLS, and educates students in interfacing with Certificate Authorities, issuing certificates, configuring SSH securely, and sending/receiving encrypted and signed email.

In the 100 module students will be introduced to basic principles of encryption and authentication; additionally, students will understand and analyze historical approaches to cryptography. Students will practice symmetric cryptography, namely block ciphers, hash functions, and message authentication Codes.

The 200 module focuses on asymmetric cryptography (i.e. RSA and Diffie-Hellman Key Exchange). Combined with symmetric encryption, this makes a powerful combination for securing communications. Applications of these technologies will be explored by deploying SSL and SSH solutions. The 300 module covers anonymity and exploits using cryptography. Students explore weaknesses in WEP and SSL that lead vulnerabilities and discover how to counter them.

At the completion of this course, a student will be able to:

- Explain the fundamental goals of cryptography.
- Apply knowledge to use common crypto software.
- Analyze vulnerable applications with respect to cryptographic best practices.
- Create tools to attack and fix applications in a virtual
- lab environment.
- By the course's conclusion, students will have covered all relevant parts of the cryptography section of the industry-standard
- CISSP certification program.

Capstone

TOOLS LEARNED

All tools from any course may be taught and/or utilized.

The scenario-based capstone activity allows the student to demonstrate their knowledge and proficiency. The group project will present a scenario and allow the students to work within their individual expertise to work through the particulars. Very little guidance will be given, allowing the students to work along multiple paths to completion. The project will culminate in a professional level oral and written report, which can be used as part of a portfolio.

At the completion of this course, a student will be able to:

- Apply the knowledge from all previous courses to analyze a scenario, for example by performing risk assessments or other security analysis.
- Utilize the knowledge from all previous courses to recommend best practice approaches to improve security posture in the scenario.
- Utilize the knowledge and skills from all previous courses to implement appropriate security controls and countermeasures in the scenario.
- Demonstrate decision-making, compliance, strategy development and professional communications through oral and written reports designed to support and make recommendations to senior management.

Program Pace & Schedule

At Xaltius Academy, we know that how you choose to study is as integral to your success as what you're learning. Paired with our online learning platform, Canvas, and individualized support, all students have access to a personalized learning experience.

Learn online. But not alone.

The community at Xaltius Academy is unmatched - from study groups to peer projects and check-ins, our students often say their cohort supported them through the program.

You'll start the program with a cohort of students, all learning together in a live lecture format.

WEEKEND LIVE

Length	24 weeks
Time Commitment	18 hrs/week
Career Services Support	Yes
1:1 with Instructors	Yes
Live Lectures	Yes
Assigned Cohort	Yes

Why Xaltius Academy?

Practical hands-on learning | You'll learn in-demand market technologies and skills, work in labs, and create a real-world portfolio.

1:1 with Instructors | Schedule sessions with instructors with various industry experience to work on technical concepts, get feedback on submitted work, or set project goals. Students also have the opportunity to attend community events hosted by guest lecturers in the Data Science field.

Learn in community | You may be learning online, but you're not alone. Students have the opportunity to join student-led affinity groups that span the student base, such as Women in Tech, Parents in Tech and Black in Tech. You also have the opportunity to connect with alumni and other students at Xaltius Academy to build their network.

Individual Career Coaching Support | Work one-on-one with a career coach for 180 days after program completion.

Program Pedagogy built by Experts

OUR GLOBAL PRESENCE

Innovating in the field of Emerging Technologies, Xaltius has democratized education across location, age gender, experience and more in the last few years. Xalitus has global footprints with learners from all across the globe.

Countries

20+

Join a culture as committed to your success as you are with representation from over 50 nationalities.

Learners

1M+

Our alumni network continues to grow strong, and we encourage you to to be a part of it.

Hiring Partners

500+

Recruitment Drives to connect you with the best talent admirers in the Industry.

FORAGE
VIRTUAL LEARNING EXPERIENCE

Experience work with virtual programs from innovative global companies.

1.5 M+

students registered into Forage programs

70+

programs in diverse industries and roles

2-5X

more likely to land a job at a partner company by completing that company's virtual experience program

ACCESSIBLE EXPERIENCE FROM TOP COMPANIES

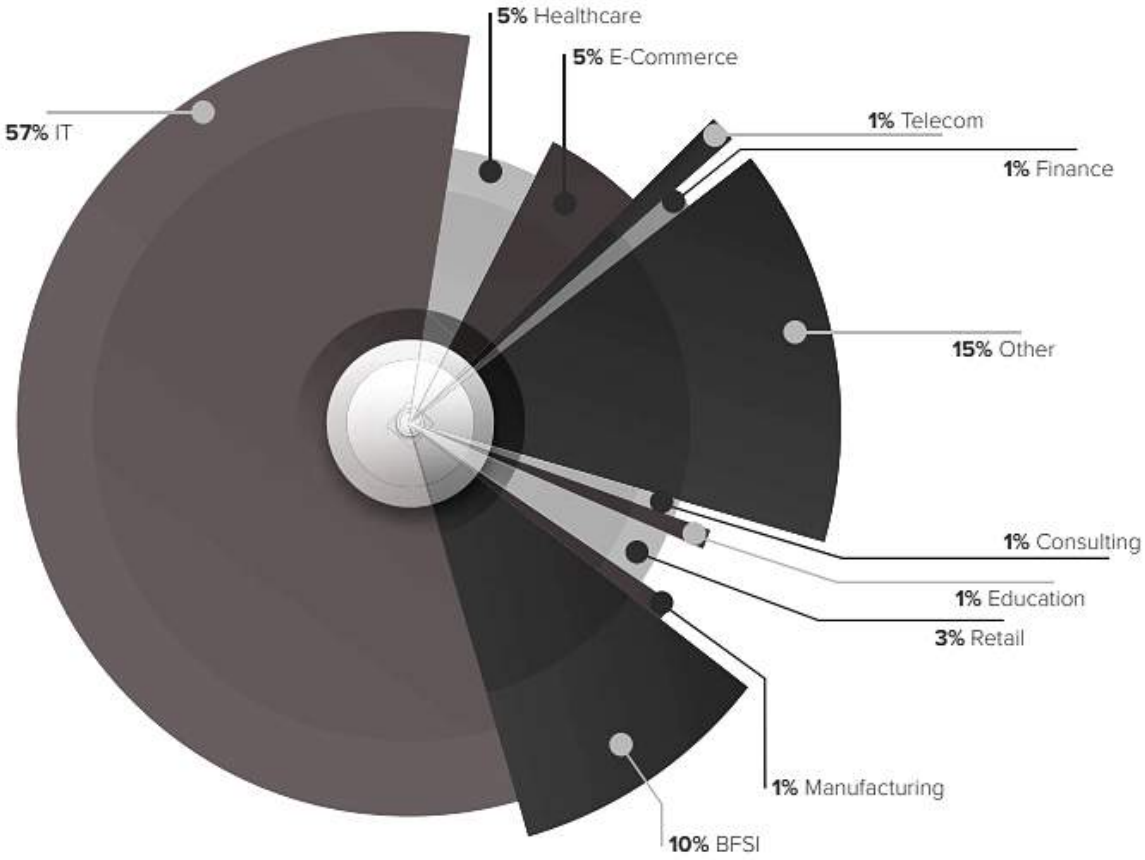
Learn highly relevant skills in your own time, at your own pace.

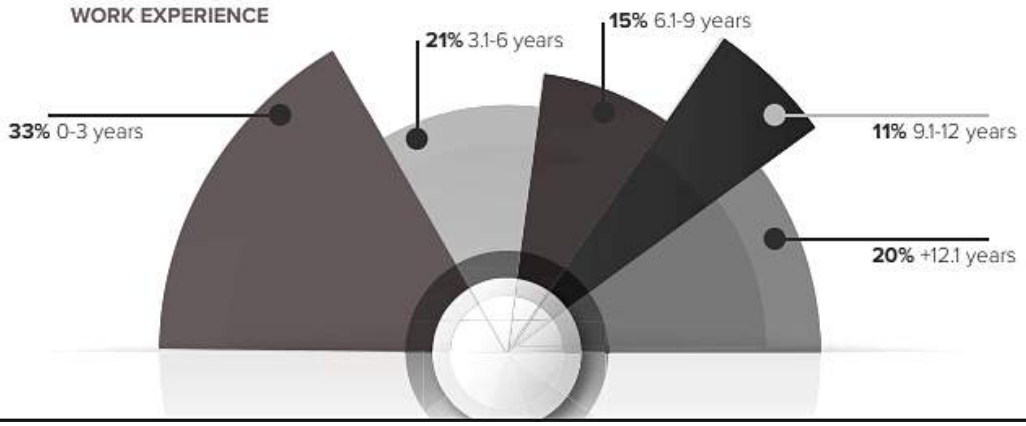
Experience what real work looks like and learn critical skills, all amongst some of the best students across the world.

Replicate work at top companies, and connect students to the companies themselves.

Get a genuine career advantage with Fortune 500 companies.

STUDENT
DEMOGRAPHICS





CLIENTS & PARTNERS

Our Students work at

MEET THE FOUNDERS

Let's meet our team members who are professional and have rich experiences.

Desmond Sek

Co-founder & Director

Desmond has numerous years of experience in the tech industry and has worked across various technologies including Java, Python, Machine Learning, Deep Learning and Computer Vision. Desmond loves coding and is passionate about languages.

A M Aditya

Co-founder & CTO

Aditya is a tech enthusiast with vast experience across various technologies in data science, machine learning, deep learning and computer vision. He has worked across various domains including automotive, banking, retail among others.

Pranjal Dubey

Co-founder & CEO

Pranjal is a strong business professional having experience in various domains including Retail, Products, Finance and Education. Truly committed to making things happen, he is spearheading tech-enabled educational initiatives globally.

”

“Education is the most powerful weapon that we can use to change the world.”

– Nelson Mandela

XALTIUS
Towards Higher Excellence

Vertex, 33 Ubi Avenue 3, #06-53, Singapore, 408868
Phone: +65 8303 9150, Email: info@xaltius.tech, Web: https://www.xaltiusacademy.com/