CYBER
INTELLIGENCE 4U

Cyber Intelligence 4U

2019 Course Catalog

About Cyber Intelligence 4U

Our mission is U as the student- whether you are an organization, university or individual. Our programs are designed for the challenges faced by organizations to increase cyber resilience, universities that understand that they need boots on the ground innovative programs and individuals who are looking to elevate their cyber education or move into cybersecurity from IT or another profession.

We understand cyber. This company was founded by a former CISO and entrepreneur with the goal of solving cybersecurity problems.

Cyber is a business issue and we are the first company to address it from this point of view educationally. Our Executive Course covers topics that bring all stakeholders together holistically to understand how cyber needs to be measured and managed as the # 1 business risk. Our Executive Course is offered as a certificate or as individual modules to address your most urgent needs.

We are short 2 million skilled resources in cybersecurity in the U.S. alone. That figure will rise to 3.5 million by 2021. Organizations are in need of more individuals and those they have are in need of higher skill levels. Our gamified approach to skills training eclipses typical courses aimed at a lecture format only.

Cyber is evolving with more sophisticated attacks at the most misunderstood levels: cloud, vendor and mobile. We offer strategic and tactical courses that address these gaps.

Our role-based training program is perfect for each cybersecurity professional that must always be learning and upping their cybersecurity stills. Regardless or your perceived role you don't want to miss this type of experience.

One of our most popular programs is for companies that sell cybersecurity solutions. Our Cybersecurity Selling Program uses a maturity-based approach that aligns to your cybersecurity products. Students learn how to have meaningful cybersecurity conversations that allow them to become trusted advisors to your clients and increase sales dramatically.

Lastly, our Offensive Cyber Security Program (OCSP) provides training using technologies created by former National Security Agency (NSA) elite.

Delivery of Courses

We offer multiple options and platforms based upon your needs.

1. **Customized**
   Most courses are customized for specific security educational or training needs. As an example, you may need to elevate the conversations of your sales force in terms of cybersecurity. We offer a unique maturity selling approach. We film, edit, translate and render course content based on your requirements.

2. **In-Person Delivery**
   We provide in-person delivery for all courses if required. Dedicated faculty with real-life industry knowledge are utilized, in order to provide a high-quality stimulating learning experience, as well as providing the most up-date techniques and information to your organization or university.

3. **Online: Our LMS or Yours**
   a. We work with the Canvas LMS. We can work with your LMS and integrate the courses to your prerequisites. Talk to us about integration prerequisites.
   b. Language support: We utilize captioning or dubbing for support of all languages. Talk to us about language prerequisites.
   c. All our courses are available online.

4. **Gamified Cybersecurity Training**
   We utilize the Escalate Platform for over 98 gamified cybersecurity training challenges. These challenges range in the number of participants and offer in-person and online opportunities in order to provide your organization various options for training.
      - Courses that use the Escalate Platform:
        - SecDevOps
        - IDS Tuning
        - NIST-NICE Role Based Training
        - All-For-All (A^3)
        - Capture the Flag (CTF)
        - OCSP Program

Course Offerings

Key:
F= Foundation Level Course
A= Advanced Level Course

BM= Board Member
CISO= Chief Information Security Officer
CIO= Chief Innovation Officer
CRO: Chief Risk Officer
CM= Compliance Manager

DPO= Data Privacy Officer
R= Remediator
V= Vendor
A=Auditor

Course	Days	Hrs	Delivery Method	Level	Roles	Pg.
Enterprise Cybersecurity Course Modules						
ENT501: The Evolution of Cyber Security		4	In-person or Online	F	BM, CEO, CISO, CM, DPO, R, V, A	10
ENT502: Why Cyber Risk		4	In-person or Online	F	BM, CEO, CISO, CRO, CM, DPO, R, V, A	11
ENT503: Cybersecurity Basics		4	In-person or Online	F	BM, CEO, CISO, CRO, CM, DPO, R, V, A	12
ENT504: Cybersecurity Roles		4	In-person or Online	F	BM, CEO, CISO, CRO, CM, DPO, R, V, A	13
ENT505: Cybersecurity Regulation		4	In-person or Online	F	BM, CEO, CISO, CRO, CM, DPO, R, V, A	14
ENT506: Cybersecurity Risk Management		8	In-person or Online	A	BM, CEO, CISO, CRO, CM, DPO, R, V, A	15
ENT507: Cyber Risk Management Use Cases		8	In-person or Online	A	BM, CEO, CISO, CRO, CM, DPO, R, V, A	16
ENT508: Cybersecurity Frameworks		8	In-person or Online	A	CEO, CISO, CM, DPO, R, V, A	17
EXEC509: Cybersecurity Strategy		8	In-person or Online	A	BM, CEO, CISO, CRO, CM, DPO, R, V, A	18
ENT510: Cyber Vendor Risk Management		8	In-person or Online	A	CISO, Vendor Managers, Senior Executives responsible for vendor risk	19
ENT511: Cyber Insurance		4	In-person or Online	A	BM, CEO, CISO, CM, DPO, R, V, A	20
ENT512: Breach Response and Table Top		8	In-person or Online	F	BM, CEO, CISO, CM, DPO, R, V, A	21

Course	Days	Hrs	Delivery Method	Level	Roles	Pg.
Enterprise Cybersecurity Course Modules						
ENT513: Cyber Forensics		4	In-person or Online	F	BM, CEO, CISO, CM, DPO, R, V, A	22
ENT514: Innovative Cyber Risk		4	In-person or Online	A	CIO, CISO, Senior Executive involved in budgeting and architecture decisions	23
ENT515: Cloud Security	1		In-person or Online	F	Cloud Technology Purchasing Decision Makers	24
ENT516: Mobile Security	1		In-person or Online	F	Mobile Technology Decision Makers	25
ENT517: Cyber M&A		4	In-person or Online	A	BM, CEO, CISO, CFO, A, Legal Team	26
ENT518: Cyber Audit		4	In-person or Online	F	BM, CEO, CISO, CM, DPO, R, V, A	27
ENT519: GDPR		8	In-person or Online	A	Everyone in organization that has a role in GDPR	28
ENT520: NYSDFS Part 500		4	In-person or Online	A	BM, CEO, CISO, CRO, CM, DPO, R, V, A	29
ENT521: Privacy Regulations (Coming September 2019)		4	In-person or Online	A	BM, CEO, CISO, CRO, CM, DPO, R, V, A	30
Intensive Executive Course Modules						
EXEC400: Cyber Insurance Quantification		1	In-person	A	C-Level Executives	32
EXEC401: Vendor Insurance Quantification		1	In-person	A		33
EXEC402: Mergers & Acquisition		1	In-person	A		34
MBL403: Tool ROI		1	In-person	A		35
ARC404: Cyber Budgeting		1	In-person	A		36
ARC405: Resource Management		1	In-person	A		37

Course	Days	Hrs	Delivery Method	Level	Roles	Pg.
Role Based 1-2 Day Training Modules						
CLD401: Cloud Security	1		In-person or Online	F	CISO and security personnel	39
CLD402: Cloud Security-02	1		In-person or Online	A	CISO and security personnel	40
MBL401: Mobile Security	1		In-person or Online	F	CISO and security personnel	42
MBL402: Mobile Security-02	1		In-person or Online	A	CISO and security personnel	43
VCR401: Vendor Cyber Risk	1		In-person or Online	F	Enterprise and Security Architects	45
VCR402: Vendor Cyber Risk-02	1		In-person or Online	A	Enterprise and Security Architects	46
Escalate Platform Offering Modules						
SecDevOpsE01: Capture The Flag	3	30	In-Person	A	Developers, Quality Assurance Team, SecDevOps, Security Architects	48
SecDevOpsE02: All Against All	1-30		Online	A		49
SecDevOpsE03: IDS Tuning		8	In-person or Online	A		51
SecDevOpsE04: Remote Files & Vulnerabilities		8	In-person or Online	A		52
SecDevOpsE05: NIST-NICE Role Cyber Challenges	30		Online and Mentoring	A		54
SecDevOpsE06: Challenge Based Learning-100+ gamified offerings	100		Online	A		55

Course	Days	Hrs	Delivery Method	Level		Pg.
6 Month Offensive Cybersecurity Professional Program Modules						
OCSPE01: Introduction to Reverse Engineering	30		In-person or Online	F	Anyone who has critical thinking skills and a clean criminal background check	57
OCSPE02: Linux Exploitation	30		In-person or Online	F		58
OCSPE03: Implant Development	30		In-person or Online	F		59
OCSPE04: Disk Forensics	30		In-person or Online	A		60
OCSPE05: Defensive Hunting	30		In-person or Online	A		61
OCSPE06: OSCP Study & Exam	30		In-person or Online	A		62
Cybersecurity Selling Program Modules						
CSP01: Evolution of Cyber	1		In-person or Online	F	Core Sales Teams, CS Solution Teams, CS Sales Teams, Sales Managers, Sales Executives, Anyone who wants to sell cyber	64
CSP02: Cybersecurity Basics	1		In-person or Online	F		65
CSP03: Cybersecurity Tools	1		In-person or Online	A		66
CSP04: Security Selling	1		In-person or Online	A		67
CSP05: Role Playing	1		In-person	A		68

Enterprise Cybersecurity Course Overview

This course was created based upon three years of research with the Fortune 1000 and cyber insurance companies. This course is about thought leadership and critical thinking. Build on concepts from the cyber insurance industry and standard risk management methodologies – primarily ROLF (reputational, operational, legal and financial) analysis.

This is a course about business impacts. The best cyber risk managers have a good technical understanding, and need to have a well-rounded solid skill set of core business acumen in terms of analytic, critical thinking focused on cyber risk and are excellent communicators and writers.

This course operates on an assumption of breach model and not on statistics from taxonomies or other non-dynamic methods. It is based on the inside-inside digital asset relationships, values and the interplay of cyber security controls that make cyber risk such a fascinating topic. It is delivered in a practical manner and uses solid business impact analysis and cyber tool information to derive data.

Most of today's cyber risk models like Factor Analysis of Information Risk (FAIR) use only control maturities, which provide very limited and superficial metrics. Cyber loss is multi-faceted, digitally based and is amplified by multiple factors including reputation, operational and legal impacts. Like all methodologies it must be tweaked and fine-tuned to each organization, their goals, and limitations.

Many of the methodologies today are too high level and overly complex. There is too much governance, risk and compliance (GRC) thinking and not enough digital asset thinking. Most are qualitative, and few are quantitative. These produce less meaningful metrics that don't allow for pivoting and a deep dive into cyber resilience.

Quantitative and qualitative cyber risk analytics must be balanced to allow critical thinking to emerge. Cyber can act one way from a compliance perspective, one way from a risk perspective and another from a governance perspective. The three must be balanced in context to organizational goals. Are you going to IPO, grow organically or through acquisition? Each goal (perspective) would have to look at cyber in a different light.

This course focuses on cyber risk management at the digital asset level which allows organizations to answer the top 10 questions that the board should be asking about their cybersecurity resiliency.

Our risk modeling can provide companies with the following thought leadership including:

- What are our most valuable digital assets?
- Where do these digital assets reside, who owns them, how are they categorized and compare to each other in terms of cyber risk?
- What relationships do we have with vendors associated to these assets?
- How well are we protected against a cyberattack?
- What is our cyber resiliency and how do we increase it?
- Do we have enough cyber budget?
- Do we have enough resources and how do we prioritize them?
- How effective are our cyber controls?
- Do we have enough cyber insurance?
- We are planning to sell the company, how does our cyber resiliency impact our acquisition price?

* This course requires the book 'Managing Cyber Risk' by Ariel Evans, CEO of Cyber Innovative Technologies – a premiere cyber risk software company.

https://www.amazon.com/Managing-Cyber-Risk-Ariel-Evans-dp-0367177749/dp/0367177749/ref=mt_paperback?_encoding=UTF8&me=&qid=1554022141

ENT501: The Evolution of Cyber Security

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	None	Foundation

Who Should Attend?

This course is for everyone in an organization – from the board member and CEO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor. Each has a role and must understand why cyber is a business risk and how to address it from a budgeting and resiliency level.

Course Outcomes

The course provides students perspective on why cybersecurity is a business issue and what that means to your organization. Students will be able to differentiate risk vs. vulnerabilities and other cyber jargon essential to the business. Students will be able to understand and discuss why cyber evolved out of IT and how the tone at the top is essential to an effective cybersecurity program.

Course Description

This course discusses the evolution of cyber from an IT issue to a business issue. It introduces the concept of cyber risk and provides a firm understanding of the history of cybersecurity, cybersecurity strategies, key trends in cybersecurity and spending, and cyber risk.

ENT502: Why Cyber Risk

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	Exec501	Foundation

Who Should Attend?

This course is for everyone in an organization – from the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor. Most organizations focus on vulnerabilities and misunderstand risk. Cyber risk is the #1 business risk and must be correctly understood.

Course Outcomes

Students will have the ability to understand cybersecurity from the business perspective. Students will differentiate the different types of cyber risk methodologies (outside-in vs. inside-out and inside-inside) and the digital asset approach and its use in cyber risk quantification and risk scoring and risk amplifiers using the concept of ROLF (reputational, operational, legal and financial).

Course Description

This course provides a clear understanding of what cyber risk is and how it is measured and scored using a digital asset (Internal) approach. Provides students the ability to understand cybersecurity from the business perspective. Introduces the concept of the digital asset approach and its use in cyber risk quantification and risk scoring and risk amplifiers using the concept of ROLF (reputational, operational, legal and financial).

ENT503: Cybersecurity Basics

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	None	Foundation

Who Should Attend?

This course is for everyone in an organization – from the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor. Using proper terminology and understanding the foundation of a cybersecurity program is the key to effective communication about cybersecurity.

Course Outcomes

Students will be able to communicate about cyber with everyone since they will be speaking the same language. Students will be able to discuss data breaches, enterprise risks and program components.

Course Description

This course focuses on terminology, cyber statistical data, breach statistics, an understanding of typical enterprise cyber risks, regulatory risks and the components of a cybersecurity program (people, process and tools).

ENT504: Cybersecurity Roles

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	None	Foundation

Who Should Attend?

This course is for everyone in an organization – from the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Security Team, Vendor and Auditor.

Course Outcomes

Students will understand the responsibilities associated to each role that is part of an organizations cybersecurity program and how to interact with each one.

Course Description

There are many stakeholders in cybersecurity. We outline roles and responsibilities in terms of how each role impacts cyber resiliency. These include the board, CEO, CRO, CISO, DPO, Compliance Manager, IT Auditors, Vendors, Regulators, Security Team and Legal Teams. This course provides a firm understanding of the roles and how they work together in the organization to support the cybersecurity program.

ENT505: Cybersecurity Regulation

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	None	Foundation

Who Should Attend?

This course is for those that must measure, analyze and enforce cybersecurity regulation. This includes the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor.

Course Outcomes

Provides students a firm understanding of regulation in terms of industry, data processed and the control tests across each framework. This course provides an understanding into each regulation requirements can be mapped across frameworks.

Course Description

All organizations start their cyber journey with compliance regulation. The course provides a holistic perspective into regulation and guidelines used across industries, data types and geography with case studies and prerequisites. Covers GDPR, PCI, ISO, NIST and most U.S. regulations. Can be customized to include any regulation or series of regulations.

ENT506: Cybersecurity Risk Management

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	8 Hours	None	Advanced

Who Should Attend?

This course is for those that have to utilize risk metrics for communication and reporting. This includes the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor - all that have a risk role and must understand how cyber risk is calculated.

Course Outcomes

This course uses the inside-inside view that focuses on the digital assets. 85% of businesses are in digital form. Students will understand how to risk model from a quantitative, amplification and qualitative approach based on the digital asset approach.

Course Description

85% of an organization's value is a digital asset. Therefore, 85% of business value is in digital form. This track is the basis of the Executive Program that provides the quantitative and qualitive metrics needed to measure risk exposures, impact and likelihood at the digital asset level.

ENT507: Cybersecurity Risk Use Cases

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	8 Hours	EXEC506	Advanced

Who Should Attend?

This course is for those that have to utilize risk metrics for communication and reporting. This includes the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor. All have a role and must understand the use of cyber risk in their specific context.

Course Outcomes

Students will be able to utilize the metrics from the cyber risk management course and create use cases aligning to measuring cyber resiliency. These include quantifying cyber insurance needs, target analysis for cyber M&A, prioritization of resources based on impacts, vendor risk analysis and cyber budgeting.

Course Description

The course provides the use cases for cyber insurance quantification, cyber resource prioritization, cyber budgeting needs, and M&A cyber risk quantification all based on a digital asset approach. It uses digital asset classifications to understand when to accept risk and if and when to remediate cybersecurity issues.

ENT508: Cybersecurity Frameworks

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	8 Hours	EXEC506	Advanced

Who Should Attend?

This course is for anyone who works with the security team on compliance and regulatory initiatives including the CEO, CISO, Compliance Manager, Data Privacy Officer, Remediators, Vendor and Auditor. Everyone has a role and must understand cyber risk in their specific context.

Course Outcomes

Most organizations start with compliance-based initiatives that align to regulatory frameworks. This course provides the means to understand the security controls that are associated to each framework with an emphasis on control test categories and the controls themselves with a mapping to a unified compliance framework.

Course Description

Students are provided a holistic perspective into control frameworks used across industries, data types and geographies with case studies, key regulatory actors and requirements.

ENT509: Cybersecurity Strategy

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	8 Hours	EXEC506 and EXEC507	Advanced

Who Should Attend?

This course is for the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor. Everyone has a role and must implement effective cybersecurity risk strategies.

Course Outcomes

Enables organizations to benchmark and measure an effective cybersecurity strategy.

Course Description

Takes cyber risk management and its use cases and translates its use into an effective cyber security strategy for organizations and to measure cyber security resiliency. Deep dives into measuring resiliency and the people, process and tools needed for accurate cyber budgeting, insurance Prerequisites, prioritization of remediation based on risk and M&A.

ENT510: Cyber Vendor Risk Management

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	8 Hours	EXEC506 and EXEC507	Advanced

Who Should Attend?

This course is for the vendor managers, the CISO and senior executives who are responsible for vendor cybersecurity risk.

Course Outcomes

Students learn how to analyze third party risk in terms of financial exposure and cyber risk scoring with an emphasis on how to reduce vendor risk.

Course Description

Vendors are the cause of 63% of reported data breaches. Reduction of vendor risk is one of the most pressing needs for organizations since the majority of both infrastructure and services are outsourced. This course teaches now to measure the impact vendors (both service and product) have on cyber risk and how to mitigate their risk down to acceptable levels.

ENT511: Cyber Insurance

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	EXEC506 and EXEC507	Advanced

Who Should Attend?

This course is for everyone in an organization – from the board member and CEO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor. Everyone has a role and must understand cyber risk in their specific context.

Course Outcomes

Provides the student with an understanding of 1st vs. 3rd party risk, gaps in current D&O policies and how claims are aligned to the digital asset cyber risk approach. Students will be able to advise on insurance coverage needs and exclusions.

Course Description

The course focuses on the types of cyber insurance trends and statistics, cyber risk management in the insurance industry, traditional cyber coverage, coverage gaps and risk quantification used in cyber insurance.

ENT512: Breach Response with Table Top

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	8 Hours	None	Foundation

Who Should Attend?

This course is for everyone in an organization – from the board member and CEO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor, Legal Team, Security Specialist and Auditor. Everyone has a role and must understand cyber risk in their specific context.

Course Outcomes

Students will be able to craft a cyber response plan and table top exercise.

Course Description

The course discusses cyber response planning, data collection and processing with acceptable law enforcement standards with real world application for forensic investigations. It provides students with the opportunity for table top exercises.

ENT513: Cyber Forensics

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	EXEC512	Foundation

Who Should Attend?

It is for everyone in an organization – from the board member and CEO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor. Everyone has a role and must understand cyber risk in their specific context.

Course Outcomes

Prepares the student to engage in a cyber investigation.

Course Description

Provides a deep dive into cyber enabled investigation goals, evidence collection techniques and investigative planning.

ENT514: Innovative Cyber Risk

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	None	Advanced

Who Should Attend?

This course is for those involved in innovation: Chief Innovation Officers, and their teams. It is also for the CISO and senior executives and those who make budgeting and architecture decisions regarding innovative technologies.

Course Outcomes

The course provides students with a firm understanding of innovative technologies including blockchain, AI, machine learning and quantum computing, their use, advantages for cybersecurity programs, and their cyber risks.

Course Description

Innovation will change how businesses productize their solutions. Some innovation will increase the effectiveness of a cybersecurity program and some will not. It is important when making strategic decisions about product development or use of these technologies to understand the impacts on cybersecurity.

ENT515: Cloud Security

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	1 Day	None	Advanced

Who Should Attend?

The course is designed for those making buying decisions on cloud technologies to guide them in exploring best practices in cloud security.

Course Outcomes

Students will understand the basics of cloud security and frameworks. Student will understand terminology, layers, and the shared responsibility model. Students will demonstrate a knowledge of critical security milestones for the success of Cloud strategy and digital transformation. Students will be able to choose the best cloud service provider for their needs.

Course Description

60% of an organization's infrastructure will be in the Cloud by 2021. Cloud Computing provides on-demand work access to a shared pool of computing capabilities or resources that can be provisioned rapidly with minimal management effort. Benefits to cloud are well documented.

This course provides focused learnings on cloud infrastructure, best practices for security architects and decision makers with inclusion of common cloud security issues encountered.

ENT516: Mobile Security

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	1 Day	None	Advanced

Who Should Attend?

The course is designed for those making buying decisions on mobile technologies to guide them in exploring best practices in mobile security.

Course Outcomes

Students will understand the basics of mobile security and controls. Students will understand terminology, layers, and the shared responsibility model. Students will demonstrate a knowledge of critical security milestones for the success of mobile strategy and digital transformation. Students will be able to choose the best mobile security solutions for their needs.

Course Description

Mobile security is overlooked due to a number of factors. However, it is not differentiated from the enterprise security risks faced by an organization.

This course provides focused learnings on mobile security best practices for security architects and decision makers with inclusion of common mobile security issues encountered.

ENT517: Cyber M&A

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	EXEC506	Advanced

Who Should Attend?

This course focuses on businesses with acquisition strategies. It is for everyone in an organization associated with M&A due diligence including the board member and CEO, CISO, CFO, Legal Team and Auditor.

Course Outcomes

Students will understand the digital asset approach to target cyber risk quantification for M&A. Students will be able to introduce these metrics into the target pricing discussions.

Course Description

Provides a perspective into quantification of cyber risk in an M&A scenario with use case studies from a leading NYC Cyber Attorney.

ENT518: Cyber Audit

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	None	Foundation

Who Should Attend?

This is for everyone in an organization. The board member and CEO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor has a role in cyber or IT audits.

Course Outcomes

Provides students the ability to interact with IT and cyber auditors.

Course Description

This course provides a deep dive into the world of cyber auditing - the examination of the management controls within an information technology infrastructure that determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives.

ENT519: GDPR

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	8 Hours	EXEC505 and EXEC506	Advanced

Who Should Attend?

This course is for everyone in an organization that has a role in GDPR – from the board member and CEO, CRO, CISO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor.

Course Outcomes

Students will put together a GDPR program based on the use and collection requirements of the GDPR. Students will be able to perform a risk assessment to measure privacy metrics and understand how to obtain GDPR compliance.

Course Description

This course provides a deep dive into the who, what, why and how regarding the General Data Protection Regulation. We focus on the requirements for the use and collection of privacy data and how to generate the privacy metrics (integrity and confidentiality) for each system that processes privacy data.

ENT520: NYSDFS Part 500

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	EXEC505 and EXEC506	Advanced

Who Should Attend?

This course is for everyone in a financial services organization that is responsible for cyber risk including the board member and CEO, CISO, CRO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor.

Course Outcomes

Students will be able to create a New York State Department of Financial Services Part 500 compliance program and cybersecurity risk assessment.

Course Description

This course is focused on the new cybersecurity regulation for financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (NYSDFS). It provides the means to pass a NYSDFS Part 500 audit.

ENT521: Privacy Regulation (Coming Sept. 2019)

Enterprise Cybersecurity Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	4 Hours	EXEC505 and EXEC506	Advanced

Who Should Attend?

This course is for everyone in a financial services organization that is responsible for cyber risk including the board member and CEO, CISO, CRO, Compliance Manager, Data Privacy Officer, Remediator, Vendor and Auditor.

Course Outcomes

Students will be able to create multiple compliance programs and cybersecurity risk assessment based on specific state wide regulations.

Course Description

This course is focused on new cybersecurity regulations for companies that are licensed or authorized to do business in various states.

Intensive Executive Course

Our 3-hour Intensive Executive Course is intended for C-Level executives to gain deeper knowledge on a variety of cyber topics in a short amount of time.

Clients will choose to focus the 3-hour course on 2-3 specific areas that most applies to their current cybersecurity concerns. We find that many of our clients choose to focus on Cyber Insurance in order to learn more about how much to buy, exceptions, and the different types of policies available.

Other organizations are more interested in Mergers and Acquisitions and the financial exposures, from the cyber perspective, related to acquisitions. Additionally, we offer programs on Tool ROI, Vendor Risk, Cyber Budgeting, and Resource Prioritization from a cyber perspective.

We deliver the course in-person in order to respond to specific focused questions from participants regarding the way their organization currently is operating vs. best practices.

EXEC400: Cyber Insurance Quantification

Executive Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
In-person	1 Hour		Advanced

Who Should Attend?

C-Level e

Course Outcomes

Students will be able to create a New York State Department of Financial Services Part 500 compliance program and cybersecurity risk assessment.

Course Description

Undersand types of policies to purchase, exceptions, and how much to buy.

EXEC401: Vendor Insurance Quantification

Executive Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
In-person	1 Hour		Advanced

Who Should Attend?

C-Level Executives in charge of setting and fulfilling company's strategy and ensuring the day-to-day operations align with the company's strategic goals.

Course Outcomes

Students will be able to create a New York State Department of Financial Services Part 500 compliance program and cybersecurity risk assessment.

Course Description

This course is focused on the new cybersecurity regulation for financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (NYSDFS). It provides the means to pass a NYSDFS Part 500 audit.

EXEC402: Mergers & Acquisitions

Executive Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
In-person	1 Hour		Advanced

Who Should Attend?

C-Level Executives in charge of setting and fulfilling company's strategy and ensuring the day-to-day operations align with the company's strategic goals.

Course Outcomes

Students will be able to create a New York State Department of Financial Services Part 500 compliance program and cybersecurity risk assessment.

Course Description

This course is focused on the new cybersecurity regulation for financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (NYSDFS). It provides the means to pass a NYSDFS Part 500 audit.

EXEC403: Tool ROI

Executive Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
In-person	1 Hour		Advanced

Who Should Attend?

C-Level Executives in charge of setting and fulfilling company's strategy and ensuring the day-to-day operations align with the company's strategic goals.

Course Outcomes

Students will be able to create a New York State Department of Financial Services Part 500 compliance program and cybersecurity risk assessment.

Course Description

This course is focused on the new cybersecurity regulation for financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (NYSDFS). It provides the means to pass a NYSDFS Part 500 audit.

EXEC404: Cyber Budgeting

Executive Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
In-person	1 Hour		Advanced

Who Should Attend?

C-Level Executives in charge of setting and fulfilling company's strategy and ensuring the day-to-day operations align with the company's strategic goals.

Course Outcomes

Students will be able to create a New York State Department of Financial Services Part 500 compliance program and cybersecurity risk assessment.

Course Description

This course is focused on the new cybersecurity regulation for financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (NYSDFS). It provides the means to pass a NYSDFS Part 500 audit.

EXEC405: Resource Management

Executive Course

General Information

Delivery Method	Days/Hours	Prerequisites	Level
In-person	1 Hour		Advanced

Who Should Attend?

C-Level Executives in charge of setting and fulfilling company's strategy and ensuring the day-to-day operations align with the company's strategic goals.

Course Outcomes

Students will be able to create a New York State Department of Financial Services Part 500 compliance program and cybersecurity risk assessment.

Course Description

This course is focused on the new cybersecurity regulation for financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (NYSDFS). It provides the means to pass a NYSDFS Part 500 audit.

Cloud Security Best Practices

In 2021, 60% of an organization's infrastructure will be in the Cloud. Cloud Computing provides on-demand work access to a shared pool of computing capabilities or resources that can be provisioned rapidly with minimal management effort. Benefits to cloud are well documented.

This course provides focused learnings on cloud infrastructure, best practices for security architects, security issues encountered, cloud security controls to mitigate risk, and frameworks used with a focus on the Cloud Security Alliance matrix.

The course is designed for SecDevOps, Security Architects, and Developers to guide them in exploring best practices in secure software development and design principles, pitfalls of design, industry standards, regulatory compliance Prerequisites for the cloud that must be baked into the design process, implementation, delivery, and risk management of secure cloud services.

This course reviews security characteristics of the leading cloud service providers, and the deep technology aspects of secure cloud architecture, development and support.

CLD401: Cloud Security

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	1 Day	None	Foundation

Who Should Attend?

CISO and security personnel

Course Outcomes

Students will understand cloud security issues and how to work with the CSA framework.

Course Description

This course provides the foundation for understanding and implementing cloud cybersecurity best practices.

Topics include:

- Introduction to the Cloud
- Terminology, layers and the shared responsibility model
- Critical security milestones for the success of Cloud strategy and digital transformation
- Analysis of Cloud CVEs, attack vectors and what may go wrong
- Cloud controls, frameworks and Prerequisites (e.g. CSA matrix)

CLD402: Cloud Security-02

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	1 Day	CLD401	Advanced

Who Should Attend?

CISO and security personnel

Course Outcomes

Students will be prepared to align controls and architectures to cloud security best practices.

Course Description

This course provides an advanced understanding for implementing cloud cybersecurity best practices.

Topics include:

- Vulnerabilities, compliance and configuration assessment
- Controls implementation automation, tools effectiveness and scorecards
- Application security – SSDLC for applications and Containers
- Infrastructure as code, DevOps and DevSecOps
- Cloud-native security – Products, guardrails and legacy vs cloud-native

Mobile Security Best Practices

Cybersecurity is the #1 business issue, eclipsing M&A and environment issues in 2018. There were many high-profile data breaches affecting retailers, banking and credit rating companies. Largely absent from the headlines were compromises directly attributed to the vulnerability of a mobile device—such as a smartphone, tablet, laptop or connected device. According to the Verizon Mobile Security Report, they found that the number of companies admitting that they'd suffered a compromise in which a mobile device played a role went up—from 27% in the 2018 report to 33% in 2019.

Attackers are adapting to the millennial mobile-centric world and expanding their arsenals. Couple that with the fact that most mobile devices have access to the same crown jewel data as those using fixed connections. This means that the compromise of a mobile device can now be just as great a risk to your customer data, intellectual property and core systems.

This course provides focused learnings on mobile infrastructure, best practices for security architects, security issues encountered, mobile security controls to mitigate risk and frameworks.

The course is designed for SecDevOps, Security Architects and Developers to guide them in exploring best practices in secure software development and design principles, pitfalls of design, industry standards, regulatory compliance prerequisites for the mobile that must be baked into the design process, implementation, delivery, and risk management of secure mobile services. This course reviews security characteristics of the leading mobile service providers, and the deep technology aspects of secure mobile architecture, development and support.

MBL401: Mobile Security

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	1 Day	None	Foundation

Who Should Attend?

CISO and security personnel

Course Outcomes

Students will understand mobile security issues and how to work with the security framework.

Course Description

This course provides the foundation for understanding and implementing mobile cybersecurity best practices.

Topics include:

- Course Intro
- Terminology, layers and the shared responsibility model
- Critical security milestones for the success of Mobile strategy and digital transformation
- Analysis of Mobile CVEs, attack vectors and what may go wrong
- Mobile controls, frameworks and Prerequisites

MBL402: Mobile Security-02

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	1 Day	MBL401	Advanced

Who Should Attend?

CISO and security personnel

Course Outcomes

Students will be prepared to align controls and architectures to cloud security best practices.

Course Description

This course provides an advanced understanding for implementing mobile cybersecurity best practices.

Topics include:

- Vulnerabilities, compliance and configuration assessment
- Controls implementation automation, tools effectiveness and scorecards
- Application security - SSDLC
- Infrastructure as code, DevOps and DevSecOps
- Mobile-native security – Products, legacy vs mobile-native

Security Architecture Risk Best Practices

Cybersecurity is the #1 business issue, eclipsing M&A and environment issues in 2018. Cybersecurity starts with the concept of baking security in.

This course provides focused learnings on best practices for security architects, security issues encountered, security controls to mitigate risk and frameworks.

The course is designed for Security Architects to guide them in exploring best practices in secure software development and design principles, pitfalls of design, industry standards, regulatory compliance prerequisites for the mobile that must be baked into the design process, implementation, delivery, and risk management.

VCR401: Vendor Cyber Risk

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	1 Day	None	Foundation

Who Should Attend?

CISO and Vendor Managers

Course Outcomes

Students will learn how to incorporate risk modeling into vendor risk management, best practices and governance.

Course Description

This course provides the foundation for understanding and implementing best practices for cybersecurity vendor risk management with an emphasis on benchmarking and scoring.

Topics include:

- Vendor Cyber Risk Modeling
- Critical security milestones for the success of cybersecurity strategy
- Vendor Risk Quantification
- Vendor Cyber Scoring
- Security controls, frameworks and requirements (e.g. NIST)

VCR402: Vendor Cyber Risk-02

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	1 Day	ARC01	Advanced

Who Should Attend?

Enterprise and Security Architects

Course Outcomes

Students will align compliance frameworks to vendors to manage residual cyber risk with an emphasis on risk reduction.

Course Description

This course provides an advanced understanding for implementing best practices for cybersecurity architectures.

Topics include:

- Vulnerabilities, compliance and configuration assessment
- Controls implementation automation, tools effectiveness and scorecards
- Contracts
- Cyber Insurance

Gamified Training with the ESCALATE® Platform

Escalate®'s cyber skills training platform is designed specifically for cybersecurity workforce-enhancing training. Escalate® provides metric based reporting to monitor cybersecurity training programs. Designed by former NSA cyber-threat specialists, Escalate® provides gamified training that cultivates cybersecurity talent in a series of applied and increasingly complex challenges.

Outcomes

Students will be in a continuous learning mode. Managers will be able to assess staff weaknesses, identify hiring needs, and find hidden cybersecurity talent in their organization.

Features

Escalate® provides best of breed training for cybersecurity teams. Escalate® is proven immersive ecosystem that delivers gamified cyber skills modules with an online community of mentors.

Product features include:

- 98 challenges (and growing) broken into 6 main topics (foundations, networks, reverse engineering, exploitation, malware development and malware) and 17 associated sub-modules. IOT & Scada Modules In Development.

- Live mentor coaching
- Community chat rooms
- Detailed reporting
- 24-7 access
- Secure cloud based
- Customized competitions
- No experience necessary

Use Cases

- Provides a continuous cybersecurity learnings environment
- Identification of skills gaps and hiring needs
- Assess and remediate cybersecurity staff weaknesses
- Uncover hidden cybersecurity talent in their organization
- Run inter and intra-company cybersecurity competitions
- Provides pre-hire screening assessments

SecDevOpsE01: Capture The Flag (CTF)

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online	Up to 4 Weeks	None	Advanced

Who Should Attend?

Developers, QA team, SecDevOps, Security Architects

Course Outcomes

A Capture the Flag contest is a special kind of cybersecurity competition designed to challenge its participants to solve computer security problems and/or capture and defend computer systems.

Course Description

The ESCALATE framework is an excellent platform to use in Capture the Flag (CTF) events due to its built-in scoring capability and its wide range of challenges across more than 12 security disciplines. The Escalate CTF platform can support up to 1000 contestants. The customer can run the CTF competition for a certain number of days (up to 4 weeks).

Event Support Add On

The Event Support Add-on includes full 24/7 support for 2 days (the typically CTF event period) and for standard event activities. The client's support prerequisites will be confirmed with the client prior to order confirmation, with any non-standard prerequisites being priced separately. We will aid in the initial setup process, facilitate account creation, conduct contestant & technical support, and all event completion tasks.

SecDevOpsE02: All Against All- A3

General Information

Delivery Method	Days/Hours	Prerequisites	Level
In-Person	3 Days/30hrs	None	Advanced

Who Should Attend?

Developers, QA team, SecDevOps, Security Architects

Course Outcomes

Not only does the exercise motivate individuals and encourage team work and real-time skill development, but it also reveals competency levels across the organization, and opportunities for skill and communication improvement.

Course Description

The “All Against All” or CyberA3, is a live-fire exercise. Each team is provided the same set of mission critical services. The goal is for each team to ensure their services have maximum uptime. However, each of these services may have one of more flaws that could enable a sophisticated attack to shut off each service. Teams must ensure their services have optimal uptime, while also researching vulnerabilities, developing exploits for those vulnerabilities and then patching their own vulnerable services.

There are several skill sets required if one wants to win: system and network administration, packet capture and network monitoring, vulnerability research, exploit development, reverse engineering and host and network forensics. Teams lose points for service downtime or if their flags are stolen. Teams gain points for stealing flags from their competitors. At the conclusion the team with the most points is crowned champion.

Example location, duration and timing

The CyberA3 event can be conducted across distributed teams or in a co-located environment to encourage engagement. The event is typically conducted over a 3 day period and adapted to client needs. The following is an example schedule (to be finalized with the client):

Day 1:
Setup by event staff

Day 2:
Setup by event staff

Day 3: PARTICIPATION DAY 1

0900-0930	Opening remarks & rules
0930-1100	Team setups
1100-1600	5 hours, team exercise

Day 4: PARTICIPATION DAY 2

1000-2400	14 hours, team exercise

Day 5: PARTICIPATION DAY 3

0000-1100	11 hours, team exercise
1300-1400	Awards ceremony
1400+	Teardown by event staff

Event Specifics

We will assist with identifying participant teams. Each team will be provided its own private space to engage in the exercise. Teams are typically comprised of 3-8 participants (although can be larger at client discretion). Our technology stack currently supports up to 12 competing teams, although more CyberA3 teams can be accommodated at additional charge.

Participants must bring their own hardware, software, and personnel. The vendor will provide exercise network infrastructure to include leader board, scoring server, networking cabling and switching, and participant servers, which may be virtualized. Participants will be provided meals and snacks. The intent is to keep teams focused, engaged, and on keyboard for three straight days to include a 24-hour continuous period. The event will be staffed appropriately to include setup and teardown, and day and night shift staffing. The event will include AV equipment where applicable and awards for the winning team.

SecDevOpE03: IDS Tuning

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	8 hours	None	Advanced

Who Should Attend?

Developers, QA team, SecDevOps, Security Architects

Course Outcomes

In the IDS tuning trainer, the presenter demonstrates a modern exfiltration technique and how to build countermeasures. By the end of the training, participants will:

- Observe attacker exfiltration
- Identify malicious traffic
- Discover how the attacker is obfuscating this action
- Build a mechanism to detect and report on the attack.

Course Description

We can develop customized training programs to meet client prerequisites. Our training includes practical, challenge-based problem solving, within the Escalate™ platform.

15 minutes	Explanation of the scenario	Presenter will provide an introductory context for the audience
45 minutes	Dissection of the defender's situation	Presenter will show the defender's perspective from the network. This will include packet capture and analysis of that traffic.
15 minutes	Break	
15 minutes	Hands-On Lab - Traffic Analysis	Participants will be presented with traffic collection and be able to view and manipulate such capture from their own laptops. During the lab the concentration will focus on removing extraneous information from the data set.
30 minutes:	Threat Modeling	During this block the presenter will attempt to identify what may be happening, by confirming if the suspected traffic is malicious and if so how was this conclusion reached, and what information is being communicated
45 minutes	Hands-On Lab - Scripting	During this block participants can build out programs to test their theories on what the alleged attacker is doing.
15 minutes	Obfuscation	Presenter will iterate through a set of common APT data-protection techniques in an attempt to identify what information is being leaked.
30 minutes	Hands-On Lab - Scripting	Students will have time to author programs to iterate and confirm what the presenter has uncovered.
30 minutes	(Optional lab) - IDS	Students will build IDS rules to identify and de-obfuscate attacker traffic
15 minutes	Conclusion	Presenter will recap the scenario. Students will be presented with similar challenges and be able to continue learning in a hands-on manner after the seminar is concluded.

SecDevOpsE04: Remote Files & Vulnerabilities

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	8 hours	SecDevOpsE03	Advanced

Who Should Attend?

Developers, QA team, SecDevOps, Security Architects

Course Outcomes

In this training, the presenter demonstrates a common mis-configuration in web app-based software. By the end of the training, participants will:

- Learn about server-side code and how this differs from client-side code
- Be introduced to web shells
- Observe an attack against a modern web application framework
- Perform the attack

Course Description

We can develop customized training programs to meet client prerequisites. Our training includes practical, challenge-based problem solving, within the Escalate™ platform.

15 minutes	Explanation of the scenario	Presenter will provide an introductory context for the audience
45 minutes	Uncovering the bug from the position of the attacker	Presenter will interact with the vulnerable application. This will include manual and automated probing using common tools which will be introduced to the audience.
15 minutes	Break	
30 minutes	Hands-On Lab - Reconnaissance and Enumeration	Students will interact with the same vulnerable application probing the attack surface.
15 minutes:	Tutorial on server-side code	Presenter will explain how a web server operates before and during a response to a web client request.
15 minutes	Break	
30 minutes	Code Execution	Explanation of how an attacker can compel the application into loading code. Presenter will also cover the concept and implementation of web shells, which is how an attacker can maliciously interact with the computer hosting the web application.
30 minutes	Hands-On Lab - Web Shells and prepping the battle space	Students build their own web shell and position it for a future attack
15 minutes	Break	
15 minutes	Gaining Execution	Presenter will show how the vulnerable app can be manipulated into calling the attacker's code

30 minutes	HandsOn Lab – Adversary Operations Simulation	Students will compel the victim application into calling their web shells
15 minutes	Break	
15 minutes	Access Escalation	Presenter will show how to gain a stronger foothold on the target
30 minutes	Hands-On Lab – Access Escalation	Students will model their Tactics, Techniques, and Procedures (TTPs) after the Presenter's
15 minutes	Source Code Review	Presenter will now show the web application from the server's perspective. Presenter will highlight where the weaknesses are and how one could perform automated checking to catch this before a release to production
30 minutes	Hands-On Lab – SecDevOps / QA / QC	Students will draft scripts to perform code sanity checking
15 minutes:	Conclusion	Presenter will recap the scenario. Students will be presented with similar challenges and be able to continue learning in a hands-on manner after the seminar is concluded.

SecDevOpsE05: NIST-NICE Cybersecurity Workforce Challenges

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online	Up to 4 Weeks	None	Advanced

Who Should Attend?

Developers, QA team, SecDevOps, Security Architects

Course Outcomes

Improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education. Identify gaps in cyber skills and provide hands on learning to address the gaps.

Course Description

This is a course that is customized to the customers' requirements in terms of its cybersecurity maturity. The NICE framework will be used to map work roles to the customer's cybersecurity maturity and the Escalate system challenges will be mapped to the roles. There will be up to 20 challenges for a specific mapped role.

We will map the NIST-NICE framework to your organization's current cyber maturity and create a custom program aligned to your needs. Once roles are established, we will offer on the Escalate cyber challenge platform up to 20 challenges for a specific mapped role. 98 challenges (and growing) broken into main topics:

- Foundations
- Networks
- Reverse engineering
- Exploitation
- Malware development
- Malware
- 17 associated sub-modules
- IOT & Scada modules in development

SecDevOpsE06: Challenge Based Learning-98 gamified offerings

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online	Up to 6 months	None	Advanced

Who Should Attend?

Developers, QA team, SecDevOps, Security Architects

Course Outcomes

Improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education. Identify gaps in cyber skills and provides hands on learning to address the gaps.

Course Description

This course uses 99 gamified challenges (and growing) broken into these main topics:

- Foundations
- Networks
- Reverse engineering
- Exploitation
- Malware development
- Malware
- 17 associated sub-modules
- IOT & Scada modules in development

Offensive Cybersecurity Professional Program (OSCP)

Our technical program provides cyber security training and workforce enhancement training for individuals to be certified as an Offensive Security Certified Professional (OCSP) or to significantly augment their current cyber security skill level.

We teach a gamified program that has been designed by premier security experts formerly with the National Security Agency (NSA). We provide hands-on learning with live machines in a safe lab environment. The offering cultivates an unparalleled level of student readiness and allows you to be associated with the gold standard in cyber talent. Our shift program allows you to identify internal resources that have aptitude in cyber and analytics and allows them to shift into cybersecurity seamlessly.

OCSPE01: Introduction to Reverse Engineering

Offensive Cybersecurity Professional Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	30 days	None	Foundation

Who Should Attend?

Anyone who has critical thinking skills and a clean criminal background check.

Course Outcomes

Students will reverse engineer a binary to get a flag. Challenges get progressively more difficult and introduce the need to use both a disassembler and debugger. Later challenges involve bypassing anti-debugging measures.

Soft Skills - The Evolution of Cyber and Cyber Roles

Students will be able to understand the evolution of cyber from an IT issue to a business issue and the concept of cyber risk and cybersecurity roles.

Course Description

This course provides a series of challenges focused on reverse engineering. In this 4-week module, students will learn the basic of reverse engineering. Through a series of practical challenges, students will learn the fundamentals of how software works, how to use disassemblers and debuggers, and how to read code that is not in plain text. As challenges get progressively more difficult, students will learn how to decode a running program, and how to bypass anti-debugging techniques often deployed by malicious actors.

OCSPE02: Linux Exploitation

Offensive Cybersecurity Professional Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	30 Days	OCSPE01	Foundation

Who Should Attend?

Anyone who has critical thinking skills and a clean criminal background check.

Course Outcomes

Students are given a binary that is running on a remote host. The student must reverse engineer the binary, discover a vulnerability, write an exploit, and then use the exploit on the remote host.

Students understand the foundations of a cybersecurity program.

Course Description

Students will utilize Kali Linux, the operating system for ethical hackers, digital forensics experts, and penetration (pen) testers. Students will learn how to use and install Kali Linux and its toolsets for vulnerability assessment, password cracking, and how to use Kali Linux for advanced pen testing, including stealthy testing, privilege escalation, tunneling and exfiltration, and pivoting.

Cybersecurity basics teaches terminology, cyber statistical data, breach statistics, digital asset cyber risk approach and other fundamental cyber concepts including the categories of a cybersecurity program.

OCSPE03: Implant Development

Offensive Cybersecurity Professional Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	30 Days	OCSPE02	Foundation

Who Should Attend?

Anyone who has critical thinking skills and a clean criminal background check.

Course Outcomes

Students will be able to write malware to perform tasks like keylogging and screen capture without getting caught by anti-virus. Students have to write a listening post to communicate with an implant that is already installed on a Windows target.

Students will understand how to create a breach response plan and do a forensics examination.

Course Description

This course focuses on challenges based on the student's ability to write malware to perform tasks like keylogging and screen capture without getting caught by anti-virus. Students will master how to write a listening post to communicate with an implant that is already installed on a Windows target.

OCSPE04: Disk Forensics

Offensive Cybersecurity Professional Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	30 Days	OCSPE03	Advanced

Who Should Attend?

Anyone who has critical thinking skills and a clean criminal background check.

Course Outcomes

Students will be able to figure out how a computer was infected with Malware. Students will perform able to hack-back operations against simulated APTs. Students will be able to gain access to multiple targets and moving laterally through an APT's network. Students will be able to analyze PCAPs that simulate malware communicating covertly over a network.

Course Description

This course is designed for experienced security professionals and deals with the theory and practice of digital forensics. It covers a wide range of topics all the way from basic disk forensics to smartphone and mobile forensics. This course will equip cyber investigators with the right skills and tools to perform a complete digital forensic analysis and investigation.

OCSPE05: Defensive Hunting

Offensive Cybersecurity Professional Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	30 Days	OCSPE04	Advanced

Who Should Attend?

Anyone who has critical thinking skills and a clean criminal background check.

Course Outcomes

Students are given RDP access to a Windows box that is infected with ransomware. Students will be able to find the ransomware, reverse engineer it, find the flaw in its encryption algorithm, write code to take advantage of the flaw, and then decrypt the files on target to get the flag. Students will be able to make use of an adversary's tools to prosecute a target network.

Course Description

Traditional security has focused on preventive defenses, but data breaches continue to occur despite the many security tools deployed. Defensive hunting turns this model on its head and provides challenges for unknown threats.

OCSPE06: Study & Exam

Offensive Cybersecurity Professional Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-Person	30 Days	OCSPE05	Advanced

Who Should Attend?

Anyone who has critical thinking skills and a clean criminal background check.

Course Outcomes

Students will be able to pass the OCSP Exam.

Course Description

Students study for and take OCSP exam before graduating the course.

Cybersecurity Selling Program

We offer a 4-Day intensive in-person OR a 4-month online Cybersecurity Selling program to ensure employees can confidently assess customer needs, present their cybersecurity solutions in context to customer needs, and sell products to potential clients.

Cybersecurity is complex topic. Organizations vary in terms of their cybersecurity maturity. Selling to each organization requires a clear understanding of this maturity. You cannot teach a new algebra student calculus.

We have done three years of research to map cybersecurity needs to organizational maturities. This course is based on that research.

Our approach is to gain trusted advisor status with your clients. The ability to elevate the conversation is critical to establishing trust with the client. We start with building the foundational knowledge to have a cyber conversation and cover terminology, breaches, trends and other valuable client-based information.

Your cybersecurity sales teams are most effective when they can position a solution that meets the clients most urgent need. Our cybersecurity selling offering allows them the ability to “meet your client where they are” and not push a solution that has no real relevance at this point in time.

Through our customized product role play, students can practice and prepare a practical approach when dealing with clients that ensures sales opportunities.

The four modules in the program are designed to equip students with the ability to successfully and confidently advise clients on the best fitting cybersecurity offerings available, according to their maturity and needs.

Our five modules put your salespeople in a new position in terms of cybersecurity conversations with customers.
The modules include:

1. Evolution of cyber
2. Cyber security basics
3. Cybersecurity tools
4. Security selling = Maturity selling
5. Cybersecurity selling role play

CSP01: The Evolution of Cyber

Cybersecurity Selling Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	1-Day In-person 1 month online	None	Foundation

Who Should Attend?

Core sales teams, cybersecurity solution teams, cybersecurity sales teams, sales managers, sales executives and anyone who wants to sell cyber.

Course Outcomes

Students will develop a firm grasp on the context and history surrounding the current state of cyber threats and cybersecurity today. Students will be able to identify cybersecurity stakeholders and decision makers and their roles. Students will understand the basics of an effective cybersecurity program. Students will understand hot topics in cybersecurity for budgeting and resourcing purposes.

Course Description

This course provides an overview of the evolution of cyber threats and cyber protection. Topics include:

- Cyber is a Business Issue
- Cyber Consequences, Spending and Trends
- Cyber Risk
- Cybersecurity Programs
- Cybersecurity Roles

CSP02: Cybersecurity Basics

Cybersecurity Selling Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	1 Day In-person 1 month online	CSP01	Foundation

Who Should Attend?

Core sales teams, cybersecurity solution teams, cybersecurity sales teams, sales managers, sales executives and anyone who wants to sell cyber.

Course Outcomes

Students will develop a firm grasp on attack surfaces and data breaches. Students will know the most interesting data breaches, how they happened and what could have been done to prevent them. Students will understand typical enterprise cyber risks, regulatory issues and how they present in conversation.

Course Description

This course provides an overview on the following topics:

- Attack Surfaces
- Data Breaches
- Typical Enterprise Risks of Today
- Regulatory Compliance Risks
- Case Studies

CSP03: Cybersecurity Tools

Cybersecurity Selling Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	1Day In-person 1 month online	CSO02	Foundation

Who Should Attend?

Core sales teams, cybersecurity solution teams, cybersecurity sales teams, sales managers, sales executives and anyone who wants to sell cyber.

Course Outcomes

Students will be able to understand what a cybersecurity tool is and identify various cyber tools based on an organization's maturity. Students will be able to recommend what is most appropriate to sell depending on the maturity of the organization.

Course Description

This course provides an overview of the evolution of cyber threats and cyber protection. Topics include:

- What is a cyber tool and how is it used?
- Immature Organization Tools
- Medium Maturity Organization Tools
- Mature Organization Tools

CSP04: Cybersecurity Selling

Cybersecurity Selling Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	1Day In-person 1 month online	CSP03	Foundation

Who Should Attend?

Core sales teams, cybersecurity solution teams, cybersecurity sales teams, sales managers, sales executives and anyone who wants to sell cyber.

Course Outcomes

Students will be able to map products based on the cybersecurity maturity model.
Students will be able to recommend products based on the customers' maturity.

Course Description

This course provides an overview of the evolution of cyber threats and cyber protection. Topics include:

- What is a cyber tool and how is it used?
- Immature Organization Tools
- Medium Maturity Organization Tools
- Mature Organization Tools

CSP05: Cybersecurity Role Playing

Cybersecurity Selling Program

General Information

Delivery Method	Days/Hours	Prerequisites	Level
Online/In-person	1 day In-person 1 month online	CSP04	Foundation

Who Should Attend?

Core sales teams, cybersecurity solution teams, cybersecurity sales teams, sales managers, sales executives and anyone who wants to sell cyber.

Course Outcomes

Students will be able to role play solution selling based on cybersecurity maturities.
Students will be able to garner upsell and cross-sell opportunities.

Course Description

This course is customized to your sales team and is recorded, edited and uploaded to our LMS. The scope is defined with your executives and your cybersecurity solutions are mapped to maturities. Role-playing is done with your teams in-person over a 1-day period.

CYBER INTELLIGENCE 4U

We look forward to hearing from you.

USA Headquarters
555 Madison Avenue
New York, New York
10022 USA

Telephone:
+1 917-472-0533 (US)

Email:
For general inquiries
info@cyberintelu.com

Ariel Evans
Managing Director
Ariel@cyberintelu.com

Julie Rothwell
VP Marketing
Julie@cyberintelu.com

Ami Pantz
Chief Operations Officer
Ami@cyberintelu.com