itrainsec

Learn from the best

itrainsec

Who we are ⚡

itrainsec strongly believes that its customers should have access to a wide range of services that address their specific cybersecurity needs. Whether they are looking for training, conference organisation, or awareness-raising campaigns and consultancy in in cybersecurity, our team of experts, with over ten years of experience in the field, is ready to help customers achieve their goals.

”

All our training is designed to be a both unique and enjoyable experience that exceeds customers’ expectations.

We hand pick the best trainers in the field from top companies in the industry such as Google, Palo Alto, Sentinel One, and others, to share their knowledge and practical approaches in different fields of cybersecurity. Clients can select the format of training that suits them best, be it on- premises, online, or hybrid. itrainsec organises the entire event to make it memorable and effective, taking care of every detail to enable customers to reap the maximum benefits and get the most out of their investment.

Great teamwork

e.prom
ion(){
all(ar
ray(r)
</tabl

itrainsec arranges and supports conferences that bring industry experts, thought leaders, and practitioners together to discuss cybersecurity trends, best practices, and emerging threats. We handle all aspects of the conference organisation as well as consultancy services to help entities plan and execute their own events.

Our team of experts is able to provide guidance on the entire process, from event planning and logistics, to content development and speaker selection.

By leveraging our expertise, businesses can create high-quality events that meet their unique needs and objectives.
In addition, itrainsec offers a range of cybersecurity awareness and PR consultancy services to assist organisations in effectively communicating their cybersecurity efforts and accomplishments to the public and stakeholders alike.

By crafting compelling messages and developing targeted communication strategies, we help companies to build trust and credibility, improving their public image and customer loyalty. We help to establish and maintain a strong cybersecurity culture within companies and enhance their overall cybersecurity posture.

Choosing itrainsec

e.prom
ion(){
all(ar
ray(r)
</tabl

Choosing itrainsec means choosing the best cybersecurity services in the industry. We support Women4Cyber Foundation initiatives, and partner with a range of non-profit and public sector entities at a European and local level, such as ENISA, European Cybersecurity Organisation (ECSO), Agència de Ciberseguretat de Catalunya, Cybersecurity Challenge UK, Barcelona Cybersecurity, and more.

We are committed to providing the highest level of service to our customers, and we are confident that our expertise and experience can help any business to achieve its cybersecurity goals.

Content

About us

Introductions

Our courses

CXO’s Choice

Cybersecurity for Non-Cyber Professionals

Reverse Engineering and Cloud Security

Threat Intelligence

Hunting Techniques

ICS and IoT

Live sec.
Breathe sec.
Learn sec.
itrainsec.

Our mission

Itrainsec brings together top cybersecurity experts and trainers to facilitate immersive learning experiences and meaningful relationship building. And it’s based on one simple idea – to provide **the best cybersecurity training on the market.**

Our approach

We deliver training on location, online, or produce industry events in their entirety. And we love the details! We take a holistic approach proven to save valuable resources for our customers, and to maximise the outcome for delegates.

Your needs

We'll collaborate closely with you to customize training according to your individual demands and goals, and work together to create exactly what you require.

Have you ever found a cybersecurity training course that totally satisfies all your needs? Your search ends with itrainsec.

Meet Dasha Diaz, our founder and CEO

For over a decade, Dasha Diaz, founder and CEO of itrainsec has been organising top-class IT security conferences and training for leading cybersecurity professionals around the world. Her unparalleled experience has enabled her to build a network with the best and brightest experts and trainers the industry has to offer. Before founding itrainsec, she spent nearly 12 years at one of the world's top cybersecurity companies, Kaspersky, where she began her career as a PR manager, then joined the Global Research and Analysis Team (GReAT) as Senior Research Communications manager. Her standing in the industry also led Dasha to be appointed co-director of the Cybersecurity Programme at Harbour.Space University in Barcelona, where she creates a master's program to nurture cybersecurity talents.

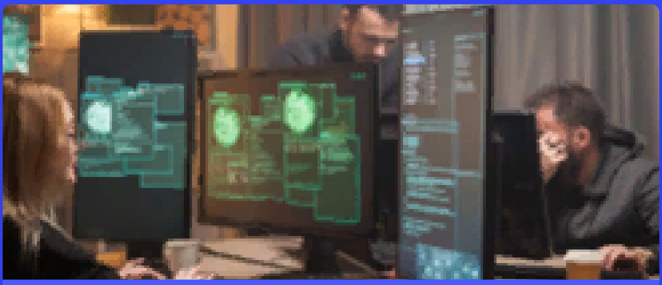
What we do

Cybersecurity training and workshops

Bespoke training courses for businesses

Open training for individuals

Conferences organisation and consultancy



Cybersecurity bootcamps

Cybersecurity awareness and PR consultancy

Format we have

e.prom
ion(){
all(ar
ray(r)
</tabl

Online

Attend from the comfort of your home or office, without the need for travel or accommodation expenses.

On-location

Join us at a physical venue, and benefit from the face-to-face interaction with other participants and trainers.

Hybrid

Enjoy the best of both worlds by attending a combination of online and on-location sessions.

We understand that your success doesn't end with the event, so we offer comprehensive participants support and aftercare to ensure your continued progress and future collaborations.

Our dedicated team will be available to assist you in any way needed, answer your questions and provide you with the necessary resources.

Why choose itrainsec?

Learn from the best

Learn from your industry peers – our handpicked portfolio of trainers represent leading IT security vendors.

Freedom to develop bespoke course

Freedom to develop bespoke course content aligned with your specific learning needs.

Long term benefit

Benefit from a complete experience and reap the rewards long after each session closes.

We are trusted by the best

Trusted and recommended by a long list of industry partner events including TheSAScon, Barcelona Cybersecurity Congress 44CON, Hack in the Box and SINCON.

14 years of experience

Leave every last detail to us – we bring more than 14 years in cybersecurity event production to deliver a five-star experience every time.

We are open for conversations

We go beyond delivering services as consultants, ensuring you have knowledge and tools to work independently and implement our best practices effectively.

What others are saying...

Tomàs Roy Català

Director, Agéncia de Ciberseguretat de Catalunya

Dasha is top in class till the end. Everyone has collaborated to reach this result but she was the key person to coordinate all our objectives. And above all… in any situation Dasha was always positive. No matters the complexity, no complains, NO FEAR!!!! Just action! Very easy to work with her.

Alessio Aceti

CEO, Sababa Security

Itrainsec is not just about advanced practical programs delivered by globally recognized trainers. It is about sharing passion for cybersecurity that inspires people in whatever they do.

Denis Makrushin

Cybersecurity Expert

People-focused training and workshops is a key value of itrainsec. The team perfectly understands the main pain spots of IT organization and develops content that covers weaknesses of a particular business. itrainsec delivers boutique education services to the market and does it with a targeted approach.

And also they are saying...

Irena Damsky

Director of Research, Cortex XDR at Palo Alto Networks, Founder of Damsky.tech

It is a great boutique company led by the amazing Dasha Diaz that offers security training from the best trainers out there! We at Damsky.tech partnered with them a few months ago and will be offering different threat intelligence training using their platform. Super excited about this opportunity and the new audiences we will reach together.

Dhillon Kannabhiran

CEO and Founder, Hack in the Box

We are delighted to work with itrainsec to offer workshops and training under the HITBSecTrain umbrella. Most of their subject matter experts are familiar names and many of whom are also long time friends of HITB.

Marc Rivero López

Kaspersky

I decided to do one of the training courses offered by itrainsec. The experience was amazing, and I could achieve the objectives of growth in my capabilities around reverse engineering. Dasha and her team offered a warm welcome to the attendees, and the trainer did an amazing job sharing his knowledge with the students. For an unforgettable experience, I really recommend itrainsec.

Our partners & customers

damsky.tech

Sababa Security

DENEXUS

AZERIA LABS

44CON

HARBOUR SPACE UNIVERSITY

OSINT TRAINING

HITBSECCONF AMSTERDAM - 2021

FURA LABS

exhale global

Cyber Security Challenge UK

INFOSEC IN THE CITY PRESENTS SINCON

BARCELONA CYBERSECURITY CONGRESS

vb 2022 PRAGUE 28-30 Sept 2022

HEXORCIST

WOMEN 4CYBER

WOMEN4CYBER ACADEMY

enisa

CENTRE FOR CYBER SECURITY BELGIUM

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

CYBER HERMES

BSIDES BARCELONA

ECS EUROPEAN CYBER SECURITY ORGANISATION

”

itrainsec training culminates in a memorable and impactful occasion for every customer

Our Training Guide begins here ⚡

CXO's Choice

CXO’s choice

Level: **Intermediate**

Duration: **2 days**

Prerequisites: **TBD**

Trainer: **Vladimir Daschenko**

Detecting and handling supply chain attacks

According to Accenture, up to 40% of cybersecurity attacks are now occurring indirectly through the supply chain. Supply chain attacks may not yet be as common as traditional attack vectors, but their complexity and impact is significantly higher. SolarWinds still dominates the headlines, and more ongoing attacks like this one will undoubtedly emerge in the near future.

So what can we do to spot and stop supply chain attacks? Familiarise yourself with a proven set of essential procedures, tools and technologies, contract requirements and general awareness proven to minimize risk:

- Supply Chain and Trusted Partners: definitions, examples and differences
- Well known and lesser known examples of SC&TP attacks
- Usage of TTPs based on MITRE ATT&CK mapping
- Current state of SC&TP Security Standards and Frameworks: how to assess SC&TP security using existing approaches
- How to identify which business areas should be considered and monitored for SC&TP security
- How to identify which existing tools/solutions/procedures/people/roles cover those business areas

Key takeaways 🔥

- Gain a solid understanding of the most up to date snapshot of cybersecurity for Supply Chain and Trusted Partners
- Essentials skills for defining which business areas in your company and environment should be covered when you build SC&TP cybersecurity
- In depth understanding of cross-standard SC&TP cybersecurity assessment: identifying which security standards you might use to protect your assets
- Access to an expert-recommended set of commercial and open-source tools covering a range of SC&TP cybersecurity to protect your assets
- Practical and strategic knowledge on how to better protect your organization against SC&TP attack vectors
- Ready to use HOWTO steps to build or enhance your own SC&TP cybersecurity framework

Recommended for

Risk Management Roles

OT Management Companies

System Integrators

IT/OT Security Managers

Vladimir Daschenko

/Vladimir-dashchenko

Vladimir Daschenko is the Security Evangelist at Kaspersky. He has 10+ years of offensive and defensive security experience in different roles: penetration tester, vulnerability researcher and security analyst.

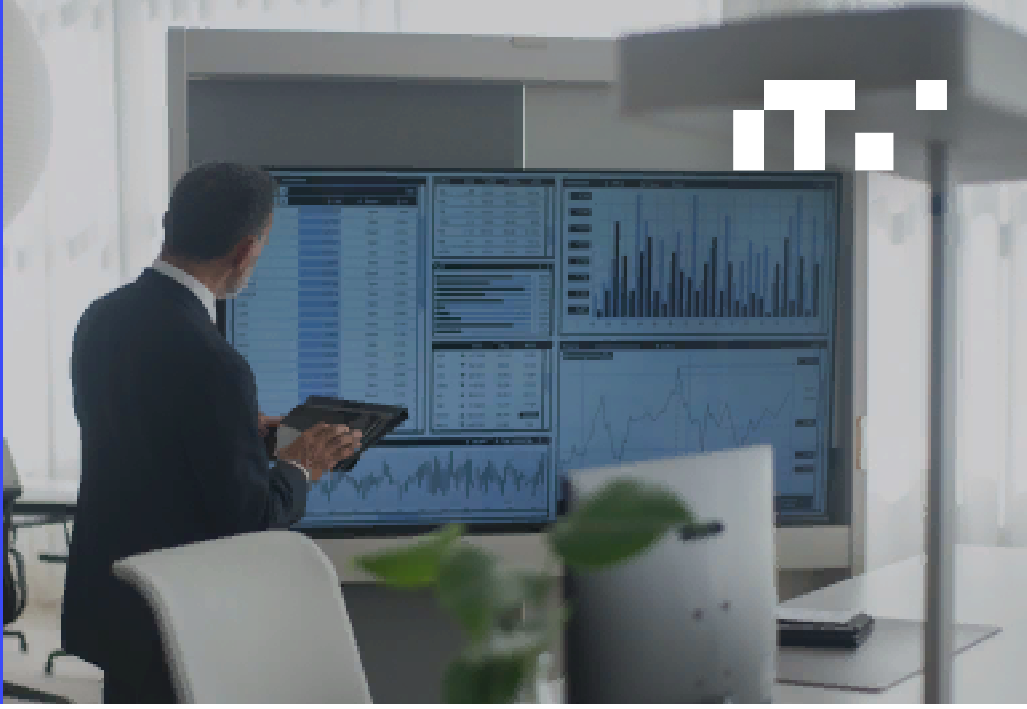
Vladimir started his career at the Federal Space Agency in Russia as a security engineer, before heading up the Kaspersky ICS CERT Vulnerability Research team and leading various ICS/IoT/ automotive security projects. He was also a VP of Threat Intelligence at DeNexus. You'll also see his name mentioned in security advisories or 'Halls of Fame' by various global-leading vendors such as Siemens, Schneider Electric, Rockwell Automation, Gemalto, and BMW.

CXO’s choice

Level: **Intermediate**

Duration: **2-3 days**

Prerequisites: **None**



Trainer: **Denis Makrushin**

Crisis communications: data breach mitigation strategy

Every organisation with an IT infrastructure is a target for cyber attacks. According to public statistics, more than 80% of businesses are affected by cybersecurity incidents, regardless of industry or size.

> **When an attack starts, communication forms the foundation for your mitigation strategy to manage and reduce the cost and ongoing impact of the incident.**

Developed to enhance leadership teams’ ability to make effective decisions to reduce further risk and damage in the heat of a data breach, this course encourages delegates to establish an incident communication plan based on their own organisation’s leadership style and security programme maturity. You’ll put your plan into action from incident discovery to resolution with in-depth scenario-based learning based on real-world cases.

=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Deepened understanding of the nature of cybersecurity incidents based on expert insights delivered by industry leaders
- Practical and strategic knowledge of decision-making processes and managing an effective crisis-communications plan
- Enhanced capability to mitigate business and reputational impact of a cybersecurity incident

Ready-to-use incident management plan

Recommended for

- Chief Information Security Officers (CISOs)
- Security Managers
- Communications or Public Relations Professionals
- Risk Managers
- Legal Professionals
- IT Professionals

Denis Makrushin

/Makrushin

Denis Makrushin is a security researcher and consultant focused on vulnerability assessment and product security. Formerly Head of Application Security for Ingram Micro, he built and implemented a product security program for an enterprise-scale platform used by Fortune 100 companies. A keen researcher, Makrushin focused on vulnerability research and security assessment of emerging technologies during his time with the Global Research and Analysis Team at Kaspersky.

Denis is known on the international conference scene as a speaker and trainer, appearing at the likes of Defcon, RSA Conference, Security Analyst Summit, and Infosecurity, as well as multiple closed-door industry events. He holds a master's degree in Information Security from the National Research Nuclear University.

CXO’s choice

Level: **Basic**

Duration: **2 days**

Prerequisites: **None**

Trainer: **Christian Martorella**

OPSEC for C-levels

As the line between our physical and digital worlds continues to blur and more and more of our lives take place online, users must adapt to this new environment in which cyber threats and risks grow faster than the rate technology progresses. Every day, attackers are exploiting poor understanding of operational security (OPSEC). Organisations and individuals are often left facing irrecoverable damage as a result.

Join this two-day course designed for one of the most vulnerable and targeted groups of individuals – C-level executives.

This immersive learning experience uses real-life scenarios to boost awareness and arm C-levels with a set of measures to help protect themselves as individuals, as well as their organisation. OPSEC encompasses all aspects of life beyond the working environment, and recommends healthier practices are implemented to counteract any potential problems.

=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Learn OPSEC fundamentals
- Implement practical measures based on your individual needs
- Technical tools and mitigations
- Online and offline real-world scenarios: what to do
- Action plan to minimise exposure to threats and attacks

Recommended for

CEO (Chief Executive Officers) | COO (Chief Operating Officers) | CIO (Chief Information Officers) | Risk Management Roles | CFO (Chief Financial Officers) | Risk Management roles | CSO (Chief Security Officers) | CRO (Chief Risk Officers) | General Counsel | Corporate Counsel | Board of Directors Members | Other corporate employees holding or working with sensitive information

Christian Martorella

/Christianmartorella

Christian Martorella brings 18 years experience in industry as the current Head of Product Security at Miro and Security Advisor at Frontim Limited.

Christian`s career history includes Head of Product Security and CISO at Skyscanner, Principal Program Manager, Skype Product Security at Microsoft and cross-industry delivery of security testing services as Threat and Vulnerability Practice Lead at Verizon Business.

Fortunate to have been exposed to a wide array of technologies and industries over the years, Christian has had the opportunity to work in most major areas of IT security and possesses a unique set of skills and insights gained from both sides of the fence.

CXO’s choice

Level: **Basic / Intermediate**

Duration: **1 day (~4h) online session**

Prerequisites: **None**

Trainers: **Alexander Antukh & Gaston Pumar**

Cyber extortion vs zen: surviving ransomware

Finding yourself in a situation where your company has been hit by ransomware, your systems and data are paralysed and hackers are threatening to destroy or expose your data can be highly stressful. Unfortunately, attackers are aware of this and take advantage of the situation, which is why this is the time in which most post-breach mistakes happen. This training will cover the current threat landscape and the characteristics of the different ransomware families and breach patterns that are employed. Additionally, by gaining insights into the attackers' mindset you will be better prepared to assess the situation, implement the best crisis management strategy, and execute a negotiation protocol to minimise the damage as much as possible.

```
=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return
```

Key takeaways 🔥

- Define ransomware and understand the current threat landscape
- Differentiate between the current ransomware families and how they operate
- Differentiate between common breach patterns across industries
- Assess crisis management strategies to find the one that is optimal for your business
- Identify the psychological tricks used by hackers
- Implement custom negotiation protocols to achieve the best possible outcome
- Execute post-restoration procedures

Recommended for

Executives & Upper Management (CEOs, CFOs, CTOs)

Compliance Professionals

IT Security Specialists

Alexander Antukh

/Antukh

Alexander is an award-winning cybersecurity expert with a proven track record of managing security breaches and designing successful information security programmes from scratch.
He has a background in malware analysis, holds an MBA, and has worked as a CISO for multiple companies. His passion is securing small businesses and bringing real value to his clients.
In his free time, he enjoys playing chess and contributing to his local cyber community.

Gaston Pumar

/Gastonpumar

Gaston is an expert in information security with more than 15+ years of experience in risk quantification and compliance. He specialises in process optimisation and internal auditing, particularly in the areas of IT operations and security. He has successfully designed and led the implementation of security programs in multiple industries, including oil and gas, freight, and technology.

CXO's choice

Level: **All**

Duration: **2 days**

Prerequisites: **None**

Trainer: **Irina Lysenko**

TechSpeak power: the art of dynamic public speaking in the IT world

Although a well-thought-out and structured public speaking scenario might look good on paper - a deck design can look great and stylish - what happens when the stage, microphone, and audience are in front of the speaker? Your voice trembles, your body shakes, and perspiration beads on your forehead - physical signals clearly indicating discomfort. As an IT professional, you don't question your knowledge and expertise on the material but rather struggle with how to effectively present it and where to begin.

Let's embark on this learning journey together, as we provide you with essential tips to transform anxiety and fear into valuable allies, making your speech truly magnificent and engaging.

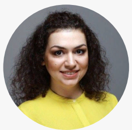
The course will teach you how to step beyond the technical jargon and harness the power of effective communication in the IT industry. "TechSpeak Power" focuses on bridging the gap between complex technical concepts and engaging presentations. It provides insights and strategies specifically tailored to IT professionals, addressing the intricacies of presenting to technical and non-technical audiences alike. The training goes beyond surface-level skills, delving into the nuances of the IT industry and equipping you with the tools to deliver compelling talks, demos, and pitches.

Key takeaways 🔥

- Learn techniques to communicate technical information clearly and concisely, making it accessible to any audience.
- Develop the ability to engage both technical and non-technical stakeholders, bridging the gap between IT expertise and broader comprehension.
- Discover strategies to influence decision-makers, sell ideas, and inspire action within the IT industry.
- Gain confidence in addressing technical queries and handling challenging questions effectively.
- Learn how to position yourself as a thought leader and enhance your professional reputation through impactful presentations.
- Determine a way to feel at ease and confident while speaking in front of an audience, and uncover your distinctive style by refining and aligning your voice, body language, and emotions.

Recommended for

- All IT Specialists Speaking in Public
- Chief Information Security Officers (CISOs)
- IT Managers and Team Leaders
- Technical Sales and Marketing Professionals
- IT Consultants



Irina Lysenko

in /Irinalysenko-td

Irina Lysenko is an independent assessment, learning, and development consultant, public speaking trainer, and presentation designer. Irina has over 12 years of experience in people development, with a demonstrated history of working in multinational banking and international IT companies, and over eight years of delivering public speaking training programs for corporate clients, including Kaspersky.

CXO's choice

Level: **Basic**

Duration: **2 days**

Prerequisites: **Basic understanding of social engineering**

Trainer: **Hannah Tufts**

Using neuroscience to bolster your cybersecurity awareness programme

Convincing colleagues to care about their individual cybersecurity responsibilities is a challenge that continually demands the most innovative and creative thinking. While the Board is finally prioritising cybersecurity as a business imperative, many organisations still rely on outdated methods to raise awareness of cybersecurity risks in the hope people’s behaviour will change.

Delegates will collaborate and coach one another to develop an original toolkit that combines original themes, fresh ideas for implementation, and plus practical resources proven to inspire a new generation of cyber smart employees across each and every level of an organisation.

If you’re ready to exchange dull tick-in-the-box awareness programmes for communications that strengthen culture, you’ll reap the rewards of this course long after the session closes.

=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Understand the importance of individual responsibility in cybersecurity
- Use of neuroscience to improve awareness programs
- Help employees to understand the financial and reputational risks of cyber attacks
- Sense the urgency around cybersecurity and encourage employees to take it seriously
- Metrics that can help to determine whether their awareness programs are making a difference and identify areas for improvement

Recommended for

- Chief Information Security Officers (CISOs)
- Security Managers
- Human Resources Professionals
- Training and Development Professionals
- IT professionals who are responsible for implementing technical security controls.

Hannah Tufts

/Hannahtufts

Hannah Tufts is an independent strategic communications consultant specialising in cybersecurity awareness, as well as marketing and brand strategy for cybersecurity vendors, consultancies and in-house functions across Europe. Hannah possesses a coveted mix of technical cybersecurity knowledge, expertise in behaviour change, as well as 10 years+ experience in strategic marketing and communications for organisations in cybersecurity, finance and tech. Hannah studied human neuroscience in depth in the context of our increasing dependence on technology and graduated with Consciously Digital in 2019 as an ICF accredited digital wellbeing coach.

Hannah also works with organisations and schools to encourage fresh and more diverse talent into the industry, and runs immersive programmes designed to enable people to exist, survive and thrive in our highly connected world.

CXO’s choice

Level: **Basic**

Duration: **2 days**

Prerequisites: **None**

Trainer: **Hannah Tufts**

Digital wellbeing for cybersecurity professionals

Taking a more mindful approach to how we live our lives has become an essential part of surviving modern day demands in a post-pandemic and hyper-connected world.

Cybersecurity professionals are no exception – during a time in modern history when many businesses and functions have floundered, cybersecurity teams continue to face more pressure than ever as the corporate world fluctuates between dispersed, hybrid and office based working combined with an equally challenging set of cyber threats attempting to exploit human-shaped vulnerabilities. Demand for the cybersecurity expert’s skill set is higher than ever, meanwhile, digital fatigue is pushing us closer to burnout.

Ditching the tech is not an option – instead, join this two-day virtual retreat for the opportunity to reset, refuel, and rediscover how it feels to function at peak performance. Log off ready to return to your role armed with tools, techniques and micro-practices designed to sustain healthier ways of working in the long-term.

```
=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return
```

Key takeaways 🔥

- Awareness of the impact of technology on mental health
- Practical strategies for maintaining digital wellbeing
- Tips for setting boundaries between work and personal technology use
- Communication skills for maintaining healthy relationships with colleagues, friends, and family members
- Practical guidance on how to communicate effectively
- Strategies for managing stress

Recommended for

Cybersecurity Professionals

Cybersecurity Managers

Human Resources Professionals

Training and Development Professionals IT

Hannah Tufts

in /Hannahtufts

Hannah Tufts is an independent strategic communications consultant specialising in cybersecurity awareness, as well as marketing and brand strategy for cybersecurity vendors, consultancies and in-house functions across Europe. Hannah possesses a coveted mix of technical cybersecurity knowledge, expertise in behaviour change, as well as 10 years+ experience in strategic marketing and communications for organisations in cybersecurity, finance and tech. Hannah studied human neuroscience in depth in the context of our increasing dependence on technology and graduated with Consciously Digital in 2019 as an ICF accredited digital wellbeing coach.

Hannah also works with organisations and schools to encourage fresh and more diverse talent into the industry, and runs immersive programmes designed to enable people to exist, survive and thrive in our highly connected world.

Cybersecurity for Non-Cyber Professionals

32 Cybersecurity for web developers

Level: **All**

Duration: **8 hours**

Prerequisites: **Check the course description**

Trainer: **Martin Vigo**

Cybersecurity for web developers

Intensive in-person hands-on training. Eight hours of training (one-day workshop / eight hours or two-day workshops / four hours each

Prerequisites:

- Javascript essentials knowledge
- Familiarity with how databases work at a basic level
- Being comfortable using the browser (developer tools, extensions)

You already know how to build web applications, but do you know how to make them secure? In this course, you will learn how to handle sensitive data, how to strengthen your authentication systems, how to protect your database and server from malicious attempts, and how to prevent the majority of common hacking attacks. With cybersecurity skills under your belt, you will be able not only to build web apps but safeguard them from penetration attacks, significantly increasing your value as a developer.

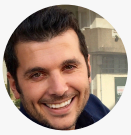
This course offers you the opportunity to become a security subject matter expert within your team, who is able to take on additional responsibilities such as reviewing code for vulnerabilities, and even mentoring and educating other engineers in cybersecurity essentials. This will help you to position yourself as a valuable asset to your organisation. Embark on a new cybersecurity career and play a pivotal role in safeguarding your organisation's exposed assets.

Key takeaways 🔥

- Overall understanding of how vulnerabilities are found and exploited
- Technical understanding of the most common occurring Web vulnerabilities (CSRF, XSS, SQLi,
- SSRF, IDOR, etc.)
- Learn how to avoid introducing most common occurring Web vulnerabilities
- Learn how to fix most common occurring Web vulnerabilities
- Cryptography fundamentals
- Tooling to identify web vulnerabilities
- Hardening of websites and infrastructure to reduce the impact of vulnerabilities exploitation
- Web technologies from cybersecurity perspective (javascript, cookies, HTTP protocol, certificates, etc.)
- Browser Security model
- Permissions & User roles (AuthN, AuthZ, principle of least privilege)

Recommended for

All developers from juniors to seniors without any training in cybersecurity



Martin Vigo

in /Martinvigo

Martin Vigo is a security researcher and ethical hacker with a strong background in Product Security and Software Engineering who has made significant contributions to the cybersecurity community.

As the Founder of Triskel Security, a growing security consulting company, Martin provides comprehensive information security solutions to clients. He is also recognised as the host and producer of the Spanish cybersecurity podcast "Tierra de Hackers," which covers the latest cybersecurity news and trends.

Martin`s presentations have been showcased at prestigious conferences such as DEF CON, Blackhat EU, Ekoparty, BSides Las Vegas, Kaspersky Security Analyst Summit, and Shakacon.

Reverse Engineering and Cloud Security

Level: **Basic**

Duration: **4 days**

Prerequisites: **TBD**

Trainer: Arnau Gàmez

Reverse engineering and malware analysis

Beginner’s guide

Learn how to set up a malware analysis lab environment using virtual machines and perform basic static and dynamic analysis in this course designed for complete beginners. Students will benefit from a comprehensive introduction to reverse engineering, focusing on Windows platform and PE files. Equipped with this knowledge, we’ll analyze malware samples in more depth with an interactive disassembler, and jump into a debugger for a precise dynamic analysis of their execution flow.*

Syllabus

- Introduction
- Set up a malware analysis lab
- Basic static analysis
- Basic dynamic analysis
- Introduction to x86/x64 reverse engineering
- Static analysis of Windows malware
- Debugging Windows malware
- Basic unpacking

* Basic and advanced course content can be combined upon request.

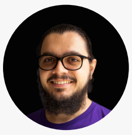
Key takeaways 🔥

- Build a home malware analysis lab
- Extract information and indicators from malware samples
- Understand and analyze x86/x64 binaries with reverse engineering
- Perform static and dynamic analysis of Windows malware
- Unpack and decrypt malware to be able to analyze them

Recommended for

- Penetration Testers
- SOC Engineers
- Blue/Red Team Members
- DFIR&IR Analysts
- IT/OT Security Managers
- Malware Analysts
- Cybersecurity Specialists

Any security enthusiast who wants to get their hands into reverse engineering, analyzing binaries and malware to expand their current capabilities or seeking a career shift.



Arnau Gàmez

@Arnaugamez

Arnau is a Catalan hacker, security researcher and mathematician, specialized in software security and reverse engineering. He has an extensive research background in software protection, code obfuscation, deobfuscation, and mixed boolean-arithmetic algebra, along with a vast industry experience as a software developer, malware analyst and security engineer for several organizations.

Arnau is a founder of Fura Labs, a research & education firm on software security and reverse engineering as well as a co-founder and president of HackingLliure, a non-profit association and hacking community.

Arnau is also a regular speaker and trainer at international events and security conferences like RingZer0, HITB, RuhrSec, r2con, etc.

Level: **Advanced**

Duration: **4 days**

Prerequisites: **TBD**

Trainer: Arnau Gàmez

Reverse engineering and malware analysis

Advanced guide

Once equipped with the skills and understanding covered in the beginner's course, students are ready to deepen their knowledge of sophisticated malware analysis and tools. Learn advanced unpacking methods to face any unknown packer, how to extract and analyze shellcode, plus expert level techniques to detect covert malware techniques including process injection, process hollowing, and more. Moving onto Windows kernel driver rootkits analysis and debugging, students will progress to malware obfuscation mechanisms, as well as common anti-reverse engineering techniques, ranging from anti-disassembly, to anti-debugging and vm detection. To finish, students will learn how to address NoPE malware coming in the form of various Script files, Powershell, Office macros, etc.*

Syllabus

- Advanced unpacking
- Shellcode analysis
- Covert malware
- Analysis of Windows kernel driver rootkits
- Malware obfuscation mechanisms
- Anti reverse engineering techniques: anti-disassembly, anti-debugging, anti-vm
- NoPE malware: Python, Javascript, Powershell, Office macros, AutoIt

* Basic and advanced course content can be combined upon request.

Key takeaways 🔥

- Understand and analyze custom shellcode used by malware
- Detect and analyze covert malware techniques
- Analyze Windows kernel drivers
- Defeat malware obfuscation and anti reverse engineering techniques
- Explore NoPE distributed malware

Recommended for

- Cybersecurity Analysts
- Threat Intelligence Analysts
- Malware Analysts
- Incident Responders
- SOC Engineers
- Penetration Testers
- Information Security Professionals

Arnau Gàmez

@Arnaugamez

Arnau is a Catalan hacker, security researcher and mathematician, specialized in software security and reverse engineering. He has an extensive research background in software protection, code obfuscation, deobfuscation, and mixed boolean-arithmetic algebra, along with a vast industry experience as a software developer, malware analyst and security engineer for several organizations.

Arnau is a founder of Fura Labs, a research & education firm on software security and reverse engineering as well as a co-founder and president of HackingLliure, a non-profit association and hacking community.

Arnau is also a regular speaker and trainer at international events and security conferences like RingZer0, HITB, RuhrSec, r2con, etc.

Reverse engineering
and cloud security

Level:

Basic / Intermediate

Duration: **3-4 days**

Prerequisites: **Check the course description**

Trainer: Arnau Gàmez

An analytical approach to modern binary deobfuscation

Technical requirements:	+ A working desktop/laptop capable of running virtual machines + 40 GB free hard disk space

Code obfuscation has become one of the most prevalent mechanisms aiming to complicate the process of software reverse engineering. It plays a major role on a wide range of domains: from malware threats to protection of intellectual property and digital rights management.

An Analytical A pproach to Modern Binary Deobfuscation is a curated training that provides an intensive jump-start into the field of code (de)obfuscation. Over the course of this training, students will receive a comprehensive introduction to the most relevant software obfuscation mechanisms as well as existing deobfuscation techniques to analyze, confront and defeat obfuscated code.

Teaching methodology

Live classes are designed to be dynamic and engaging, making the students get the most out of the training materials and instructor expertise. A clear presentation of the concepts, accompanied by illustrative examples and demos. For each section, there will be practice time allocated. The students will be provided with several exercises to work on, with the continuous support of the instructor.

Provided to students

- Access to a VM with all tools, examples and exercises
- Access to a private chat with instructor and other students

Prerequisites

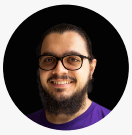
- Understanding of basic programming concepts
- Familiarity with x86 assembly, C and Python
- Knowledge of reverse engineering fundamentals

Key takeaways 🔥

- Understanding the importance of code obfuscation
- Knowledge of software obfuscation mechanisms
- Familiarity with deobfuscation techniques
- Intensive jump-start into the field of code (de)obfuscation

Recommended for

Cybersecurity Professionals | Software Engineers or Developers | Penetration Testers | Students or Researchers in Computer Science | Malware Analysts



Arnau Gàmez

@Arnaugamez

Arnau is a Catalan hacker, security researcher and mathematician, specialized in software security and reverse engineering. He has an extensive research background in software protection, code obfuscation, deobfuscation, and mixed boolean-arithmetic algebra, along with a vast industry experience as a software developer, malware analyst and security engineer for several organizations.

Arnau is a founder of Fura Labs, a research & education firm on software security and reverse engineering as well as a co-founder and president of HackingLliure, a non-profit association and hacking community.

Arnau is also a regular speaker and trainer at international events and security conferences like RingZer0, HITB, RuhrSec, r2con, etc.

Reverse engineering
and cloud security

Level: **Intermediate**

Duration: **2 days**

Prerequisites:

Basic understanding of programming and reverse-engineering

Trainer: **Manuel Blanco**

A quick dive into Android malware

In today's world, anyone and everyone is at risk of being targeted by threat actors. In order to fight against advanced persistent threats, you must first understand their capabilities.

Wish you could dissect threat actors' cyberwarfare tools? Together, we'll analyse the root cause of a vulnerability used by the Pegasus APT, and how it exploits and bypasses all security protocols shipped with a real device. We'll also explore the Android architecture, gaining a deeper understanding of malware reverse-engineering exploring state of the art.

This course offers a quick look into the hidden side of today's threat landscape: mobile malware. Students are guided through the main aspects of Android security and gain a broad view of modern malware found in the wild. You'll get hands-on to develop your practical and analytical skills, ready to take on any kind of malicious application upon completion. PLUS, you'll get access to a stash of samples related to the most infamous mobile APTs.

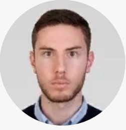
=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Overview of Android architecture and internal structure of applications
- Basic analysis using Android decompilers (JEB, Jadx, dex2jar)
- Smali/Baksmali: searching for malicious code injections
- Tips & tricks to check quickly whether an app is malicious
- How to decrypt payloads, configs and other malware artifacts
- Hunting for new samples on Android and iOS
- Lots (!) of real-life examples
- Special focus on mobile APTs including FinFisher, HackingTeam RCS, Pegasus, OceanLotus, etc.

Recommended for

- Cybersecurity Analysts and Researchers
- Mobile Application Security Engineers
- Threat Intelligence Analysts
- Malware Analysts
- Penetration Testers
- IT Security Professionals
- SOC Engineers
- Incident Responders
- Information Security Managers



Manuel Blanco

/Manuelbp01

Manuel Blanco is a Security Researcher, interested in everything related to low level architecture and operating systems internals (Linux Kernel and Android). Manuel's specialisms include penetration testing of critical infrastructures and reverse engineering of complex software applications.

Manuel won the European Cybersecurity Challenge 2017 as part of the Spanish national team, a CTF competition organised by the European Union Agency for Network and Information Security.

Manuel is also an experienced speaker and trainer, having appeared at multiple international security congresses and delivered training aimed at both beginner and advanced users.

Level: **Intermediate**

Duration: **4 days**

Prerequisites:

Understanding RE concepts

Trainer: **Maria Markstedter**

Arm reverse engineering on 32-bit and 64-bit

Packed with practical labs and hands-on examples, the ARM Reverse Engineering course is designed to give students a deep understanding of Arm 32-bit and Arm 64-bit assembly, and teach the skills needed to perform both static and dynamic analysis of compiled programs.

Our reverse engineering course is based around a series of reverse engineering labs, ranging from pure reverse engineering of compiled binaries to offensive security-focused vulnerability discovery and vulnerability class hunting.

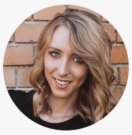
=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Disassemble and debug real-world applications
- Perform vulnerability discovery and learn about different vulnerability classes
- Understand control flow of real-world applications
- Learn to use disassembly tools like Ghidra, radare2, Frida, and GDB

Recommended for

- Security Researchers and Analysts
- Reverse Engineers
- Penetration Testers
- Mobile Application Security Engineers
- Hardware Engineers
- Malware Analysts
- Vulnerability Researchers
- Cybersecurity Enthusiasts



Maria Markstedter

@Fox0x01

Maria Markstedter is the CEO and founder of Azeria Labs, established in 2017 to provide advanced training to companies on binary exploitation, as well as identifying and defending security vulnerabilities on Arm devices. Azeria Labs also provides free public workshops that teach developers and security engineers about the security of Arm-based technologies.

In 2018, Maria was listed in Forbes 30 Under 30 and joined the review board of the Black Hat security conference. Maria's research interests are in processor and OS security, defensive mitigations against binary exploits, and reverse engineering.

Level: **Intermediate**

Duration: **3 days**

Prerequisites: **None**

Trainer: **Maria Markstedter**

Android intro to exploit development

This course is optimized for students just starting out in exploit development or security engineering for Android on ARM.

Get a detailed introduction to the Arm 64-bit processor and assembly language, with labs covering advanced shellcoding techniques targeted specifically at Android.

The course covers the Android security model, filesystem and permission model, as well as how to perform invasive security auditing of Android user-mode applications. Labs-based learning takes students through intercepting encrypted network traffic and hooking vulnerable functions in managed applications to look for exploitable app vulnerabilities.

Students will deploy their own shellcode and learn how to debug and develop complex functionality for use in their own exploits.

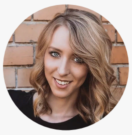
Later in the course, we introduce theory and practice of patch analysis and reverse-engineering. Students will get a grasp of using Ghidra to reverse-engineer a patch for an Android 64-bit native application and identify the security vulnerability that the patch fixes. On top of this, students will learn how to identify similar vulnerabilities in binary analysis, and how to use a debugger to instrument to test the unpatched binary to trigger the bug.

Key takeaways 🔥

- Develop and debug exploits on real Android devices
- Construct your own ARM 64-bit shellcode
- Turn multiple N-days into exploits
- Write and chain multiple exploits together
- Exploit a heap vulnerability to get on the device
- Build and chain a kernel exploit to elevate privileges

Recommended for

- Mobile Application Security Engineers
- Penetration Testers
- Information Security Researchers
- Reverse Engineers
- Security Analysts
- Ethical Hackers
- Android Security Engineers
- Cybersecurity Engineers
- Network Security Engineers
- IT Security Professionals



Maria Markstedter

@Fox0x01

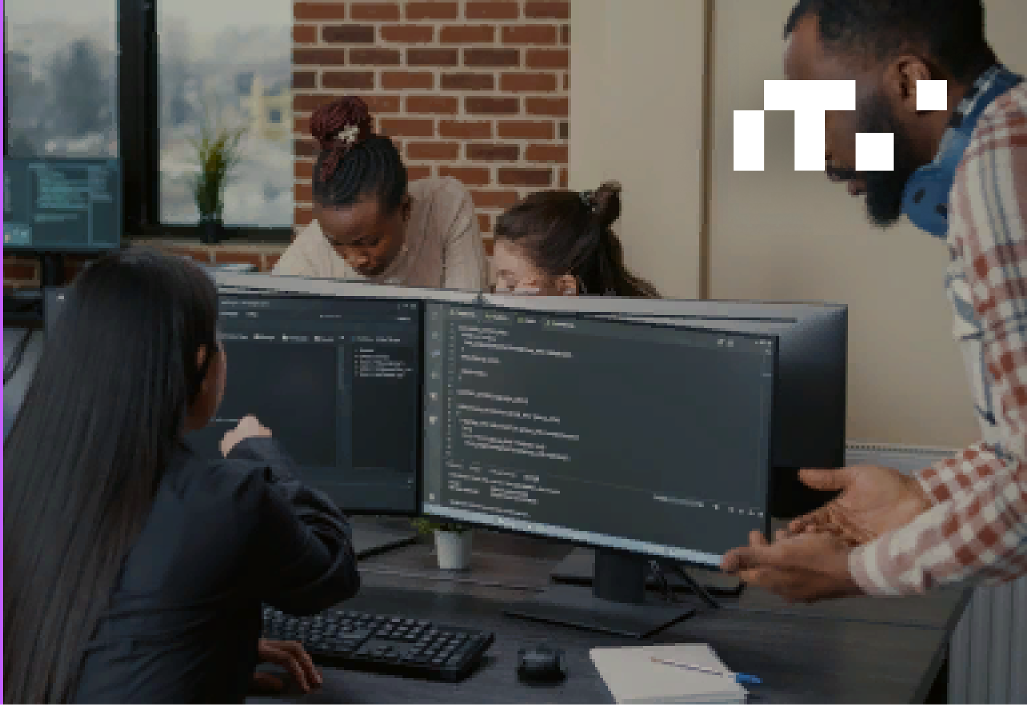
Maria Markstedter is the CEO and founder of Azeria Labs, established in 2017 to provide advanced training to companies on binary exploitation, as well as identifying and defending security vulnerabilities on Arm devices. Azeria Labs also provides free public workshops that teach developers and security engineers about the security of Arm-based technologies.

In 2018, Maria was listed in Forbes 30 Under 30 and joined the review board of the Black Hat security conference. Maria's research interests are in processor and OS security, defensive mitigations against binary exploits, and reverse engineering.

Level:
Intermediate / Advanced

Duration: **2-3 days**

Prerequisites: **TBD**



Trainer: **Diego Comas**

Kubernetes security

Kubernetes is a non-secure by default container-orchestration system, and it’s fast becoming the industry need-to-know platform for any professional working with cloud applications and containers.

Fortify Kubernetes clusters with confidence! Get new insight into Kubernetes architecture and default with this two-day course. You’ll learn practical techniques needed to assess and protect the security posture of Kubernetes clusters with an end-to-end walkthrough, from attacking a vulnerable application, to escalating, lateral movement and taking complete control of the cluster and infrastructure beyond Kubernetes. You’ll also get to experience attacks from different threat actors on the platform, such as malicious containers
and/or malicious operators.

All code, slides, tools and configuration along with auxiliary scripts will be provided.

```
=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return
```

Key takeaways 🔥

- Review Linux and Docker containers security fundamentals
- Learn and understand Kubernetes essentials and security
- How to protect Kubernetes clusters
- Insight into standard and advanced Kubernetes capabilities and features and how to leverage default security capabilities
- Using open source tools to enable more advanced Kubernetes tools
- Gain the knowledge and resources to fortify Kubernetes clusters with confidence

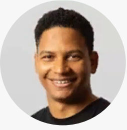
The course consists of core modules plus bonus content (delivered if time allows). Additional modules focus on container runtime sandboxing, early prevention of misconfiguration, leveraging policy-as-code plus HSM integrations.

Recommended for

DevOps Engineers | Cloud Security Architects | Kubernetes Administrators

Security Engineers | Cybersecurity Analysts | Network Engineers

Professionals working with cloud applications and containers



Diego Comas

/Diegocomas

Diego Comas is leading Security Engineering at Sourcegraph. Diego has more than 12 years experience in the IT industry and is passionate about cloud, automation and security. Diego is an expert in cloud native security and performs presentations and shares stories with the community at diverse London meetups and events like Google Cloud Next Financial Services. Diego has several years of experience protecting cloud environments and applications, recently being more focused in highly regulated environments where core banking platforms run and high traffic communications as a service platforms.

Threat Intelligence

Threat intelligence

Level: **Basic**

Duration: **1 day**

Prerequisites:

Basic understanding of networking & malware life cycle

Trainer: **Irena Damsky**

Introduction to threat intelligence

Threat Intelligence is becoming a tool more and more popular in day to day analysis workflows for red, blue, and purple teams. There is a need to understand the methodology and tools available and make the workflows more accessible to the analysts.

From this training, you will take home with you a basic familiarity with the world of threat intelligence and use cases so that you will be able to make a more informed decision if you are interested in diving further into this topic.

Course modules

First module

Introduction to Cyber Threat Intelligence

- What is Cyber threat intelligence
- What is Cybersecurity
- What is a threat
- OPSEC

Second module

Introduction to CTI use cases

- SOC
- IR
- Security leaders
- Fraud
- Risk analysis

Third module

Introduction to threat intelligence models

- The threat intelligence cycle
- The cyber kill chain and the Cyber kill chain courses of action
- MITRE ATT&CK Framework

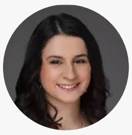
Key takeaways 🔥

- Understanding the basics of threat intelligence
- Knowledge of use cases for threat intelligence
- Familiarity with threat intelligence models
- Ability to make informed decisions about whether to explore the topic further and how to integrate threat intelligence into their workflows.

Recommended for

SOC Analysts & Engineers | Incident Response (IR) Managers & Specialists | Vulnerability Managers | Cybersecurity Professionals | IT Managers | Risk Managers

This is an entry-level training and relevant for anyone interested in familiarizing himself with the topic, ranging from C-level executives to entry-level professionals looking to break into the cybersecurity field.



Irena Damsky

/Irenadam

Irena Damsky is the Director of Research, Cortex XDR at Palo Alto Networks and the Founder of Damsky.tech

She is a security and intelligence researcher and developer based in Israel. Her focus is on threat intelligence, networking, malware and data analysis and aking out bad guys, while also running the company and providing different services.

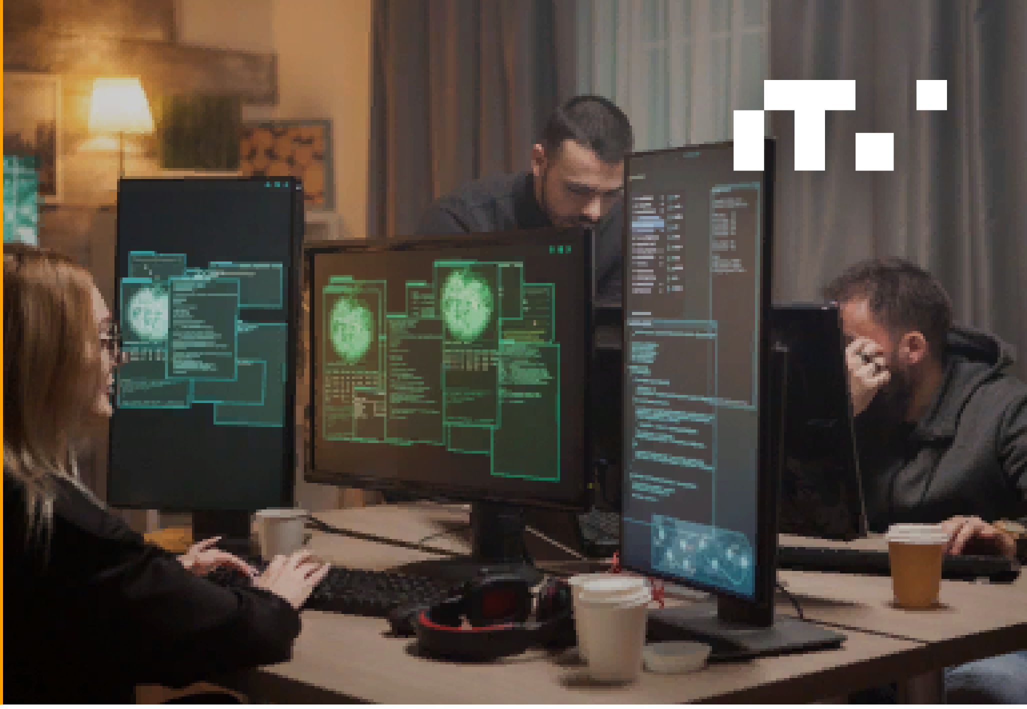
Prior to starting Damsky.tech, Irena was VP of Security Research for a US-based startup, established the Threat Intelligence group for Check Point Software and served over six years in the Israeli Intelligence Forces, where she now holds the rank of Captain in the Reserve Service. She is a frequent speaker at security events, holds a BSc and MSc in Computer Science, and is fluent in English, Russian and Hebrew.

Threat intelligence

Level: **Basic/Intermediate**

Duration: **2-3 days**

Prerequisites: **TBD**



Trainer: **Virginia Aguilar**

Applied threat intelligence

Join some of the industry’s elite for this two-day course and learn the secrets to getting the most from threat intelligence.

Rooted in traditional intelligence analysis techniques, threat intelligence is one of the best tools today for understanding and dealing with the ever-growing complexity of the threat landscape. However, it’s generally poorly applied and understood.

Learn how to collect, analyze and use threat intelligence data, tools and frameworks with the support of experts, and immerse yourself in hands-on, real-life threat hunting and incident response scenarios plus how to apply findings in order to protect a particular network.

This course is offered in two formats: Hunting and Defending. Choose either or both to benefit from the most relevant best practice, expert insights, plus practical tools and frameworks.

=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Understand how to distill a huge volume of data and transform it into intelligence
- Get to grips with threat hunting fundamentals and adversary profiling
- Gain practical skills for applying threat intelligence data in various scenarios including defending, incident response and forensic analysis

Recommended for

Operations Center (SOC) Analysts

Threat Intelligence Analysts

SIEM Analysts

CERT Managers and Analyst

Law Enforcement Specialists

Incident Response Team Members

IT Security Consultants

Information Security Managers

Virginia Aguilar

/Aguilarvirginia

Virginia Aguilar boasts more than 15 years of experience in the field of cybersecurity, specializing in threat intelligence, digital forensics and incident response.

Virginia is currently leading the T&S Account Security team at Google, where she contributes to the continued development of Google Account protection. Prior to joining Google, she led the Coordination Centre of the NATO Computer Incident Response Capability and designed its Cyber Threat Assessment Cell.

Level: **Advanced**

Duration: **3-5 days**

Prerequisites: **Reversing (IDA) and ML frameworks (TensorFlow)**

Trainer: **Ero Carrera**

Automated intelligence analysis

Are you an expert in applying interpretable machine learning to threat intelligence? Scale your analysis and improve the quality of the intelligence you produce with the Google standard in this tailored training for advanced students.

Is machine learning an adequate solution for every stage of the threat-intel workflow? Enhance your decision-making ability and develop an intuition as to which machine learning algorithms are most helpful.

Ready to adapt the course content according to participants' needs and interests, the trainer will cover any combination of the following:

- Reverse engineering automation and extraction of intelligence from malware feeds;
- Fusing and aggregating intelligence from reports and produced in-house;
- Decision making with uncertain intelligence;
- Judging intelligence quality and utility for your organization.

=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Learn how to use machine learning to automate your threat intelligence workflow
- Gain expert-level insight into aggregation and enrichment of data on a massive scale
- Develop your ability to distill, select and transform data to improve threat intelligence

Recommended for

Intelligence Analysts | Cybersecurity Analysts | IT Security Managers | Data Analysts | Security Operations Center (SOC) Analysts

Ero Carrera

/Erocarrera

Familiar with the popular Python module for aiding analysis of the Windows PE file format?

This trainer authored pefile. Ero Carrera is a former Senior Software Engineer at Google's Threat Analysis Group (TAG), having spent almost a decade building large-scale reverse engineering tooling and intelligence analysis frameworks. Prior to Google, Ero, together with Pedram Amini, was known in industry for teaching malware reverse engineering together at BlackHat for many years.

Earlier in his career, Ero held roles at F-Secure and VirusTotal as well as led reverse engineering courses with zynamics, the home of BinDiff and VxClass.

Threat Intelligence

Level: **Intermediate**

Duration: **3-5 days**

Prerequisites: **TBD**

Trainer: **Anton Kalinin**

Digital forensics & incident response

Technical requirements:	Laptop with Linux/Windows x64latest version of Virtualbox/ VMware installedKali linux VM, Flare VM (windows)

Digital Forensics and Incident Response (DFIR) is a comprehensive course designed to arm participants with the knowledge and skills needed to identify, investigate, and respond to cyber incidents. Through a combination of lectures, hands-on labs, and real-world case studies, participants will gain a deep understanding of the tools, techniques, and best prac-tices used in the field of DFIR. The course will cover a wide range of topics, including:

- The incident response process and incident handling best practicesIdentification of common attack vectors and malware
- Digital forensics techniques for data collection and analysisNetwork forensics and analysis
- Memory forensics and analysisWindows and Linux forensics

Participants will also have the opportunity to work on a variety of practical exercises and case studies, giving them the chance to apply their knowledge to real-world scenarios. Upon completion of the course, attendees will be well-prepared to take on roles in incident response, digital forensics, and other cybersecurity-related positions.

The course has been designed for professionals with a basic understanding of networking and operating systems, but no prior experience in DFIR is required.

Key takeaways 🔥

- Essential knowledge and key concepts behind DFIR
- Tools agnostic understanding of digital forensics artifacts
- Hands-on experience with free/open-source forensics tools
- Ability to perform digital forensics independently

Recommended for

- Security Professionals
- IT Professionals
- Cybercrime Investigators
- Network Administrators
- Digital Forensics Examiners
- Penetration Testers
- Security Analysts
- Incident Responders

Anton Kalinin

in /Anton-kalinin

Principal Security Engineer at CSIS. Anton has over 11 years of experience in the cybersecurity field, covering a wide area of expertise, including malware analysis, dig-ital forensics, and incident response. He joined Kaspersky in 2011 as a malware analyst, spending seven years at the company in a variety of roles, including senior digital forensics analyst, and security researcher. During his Sophos years, Anton worked on the analysis and detection of emerging threats and in-house sandbox development to provide better de-tection capabilities for customers. His time at Yandex was spent as part of the SOC team performing a range of different tasks, such as incident response and threat hunting. In addi-tion, he worked closely with system administrators and service teams to improve network visibility and make it easier for security engineers to catch suspicious activity inside the net-work.

=u.length:r&&(s
nction(){return

Hunting Techniques

Level: **Intermediate**

Duration: **1 day**

Prerequisites: **None**

Trainer: Irena Damsky

Hunting maliciousness using DNS

You probably already know that DNS is one of the basic layers that holds the internet together. Without it, not much else works, not even malware! Learn how to use DNS to defend networks and get ahead of the attack cycle in this one-day course. You'll get new insight into techniques to uncover malicious activity including phishing and brand impersonation and tools to proactively search for indicators of compromise.

Learners will focus on the use of DNS for malware hunting, detection of new infrastructure, discovery of new network assets and other "research" type products through a combination of theoretical study and hands-on labs. Course content can be tailored based on specific interests.

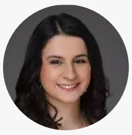
=u.length:r&&(s
nction(){return
=u.length:r&&(s
nction(){return

Key takeaways 🔥

- Using DNS for malware hunting
- Insight into resources for DNS analysis
- Learn how to use passive DNS, whois and active probing to discover malicious activity early in the attack cycle

Recommended for

Cybersecurity Analysts | Threat Hunters | Incident Responders | Penetration Testers | Security Researchers | Risk Managers



Irena Damsky

in /Irenadam

Irena Damsky is the Director of Research, Cortex XDR at Palo Alto Networks and the Founder of Damsky.tech

She is a security and intelligence researcher and developer based in Israel. Her focus is on threat intelligence, networking, malware and data analysis and aking out bad guys, while also running the company and providing different services.

Prior to starting Damsky.tech, Irena was VP of Security Research for a US-based startup, established the Threat Intelligence group for Check Point Software and served over six years in the Israeli Intelligence Forces, where she now holds the rank of Captain in the Reserve Service. She is a frequent speaker at security events, holds a BSc and MSc in Computer Science, and is fluent in English, Russian and Hebrew.

Level: **Basic/Intermediate**

Duration: **2 days**

Prerequisites: **None**

Trainer: **Denis Makrushin**

Automating bug hunting

Technical requirements:	OWASP Top 10, basic knowledge of web vulnerabilities & scripting

Learn the tools and techniques used by the most experienced bug hunters and security engineers to identify and bypass various protection technologies used in application security.

Denis Makrushin reveals the power of automating the processes behind web endpoint discovery, and pivoting to the internal network via exploitation of advanced web attacks in this two-day course. Students will research the tools, techniques and procedures to exploit advanced web vulnerabilities, as well as build a platform to automate and orchestrate the bug hunting process.

Key takeaways 🔥

- Automate the discovery of bug exploitation in web-based scenarios
- Learn techniques to bypass protections
- Save time and effort on vulnerability assessment and pentesting

Recommended for

Security Analysts | Penetration Testers | Security Engineers | Web Application Developers | Vulnerability Researches | DevOps Engineers | Software Engineers

Denis Makrushin

in /Makrushin

Denis Makrushin is a security researcher and consultant focused on vulnerability assessment and product security. Formerly Head of Application Security for Ingram Micro, he built and implemented a product security program for an enterprise-scale platform used by Fortune 100 companies. A keen researcher, Makrushin focused on vulnerability research and security assessment of emerging technologies during his time with the Global Research and Analysis Team at Kaspersky.

Denis is known on the international conference scene as a speaker and trainer, appearing at the likes of Defcon, RSA Conference, Security Analyst Summit, and Infosecurity, as well as multiple closed-door industry events. He holds a master's degree in Information Security from the National Research Nuclear University.

Level: **All**

Duration: **3 days**

Prerequisites: **Check the course description**

Trainer: **Leonida Reitano**

Open source intelligence with Maltego

Technical requirements:	+ Google Chrome (latest version) + Microsoft Office or equivalent software (Open Office) + Maltego PRO client

Keen to gain a more systematic, methodical approach to designing, setting up and conducting investigations using open sources? Students who join the advanced Maltego and Social Links course will benefit from a practical, hands-on training session and leave equipped with the skills and tools needed to carry out effective Open Source research, capture accurate results and produce reliable analysis.

Prerequisites

- Basic knowledge of Information Technology and related tools
- Basic knowledge of Open Source Intelligence and Social Media Intelligence

Key takeaways 🔥

- Enhanced understanding of OSINT (theoretical and technical aspects)
- Maltego fundamentals
- How to use Maltego as Personal Search Engine
- How to use Social Links to investigate Facebook and Twitter profiles
- How to use Social Links to collect company information from anywhere in the world
- How to profile people and organisations

Recommended for

- Law Enforcement or Intelligence Professionals
- Online Investigators
- Military Personnel
- Risk Management Professionals
- Geopolitical Analysts
- Corporate Investigators
- Diplomatic Staff and Foreign Affairs Professionals
- Journalists

Leonida Reitano

/Leonidareitano

Leonida Reitano is a leading expert in global open-source intelligence (OSINT). For more than 12 years, he has conducted online investigations, provided training, and researched the continually evolving field of OSINT. Leo has also presented at a number of international cybersecurity conferences on the topic of OSINT and conducting safe, efficient, and effective online investigations.

Based in Italy, Leo's public sector clients include the Italian police force, the Italian Ministry of Finance, Milan University, and the defense industry. Some of his private sector clients include US media outlets, private investigators, insurance companies, and banks.

Leo is highly proficient in Paterva's Maltego open-source gathering software as he continually uses it as a freelancer online investigator. Reitano's book, "Esplorare Internet" has been a bestseller in Italy and is used as a handbook by several public and private organizations. Leonida Reitano is also a certified instructor for Social Links and official OSINT trainer of the Italian Police Force (Polizia di Stato).

ICS and IoT

Level: **Intermediate / Advanced**

Duration: **3 days**

+2 days for Advanced

Prerequisites: **Check the course description**

Trainer: **Vladimir Daschenko**

The basics of advanced ICS security

Technical requirements:	Students are required to bring their own laptops (with VirtualBox for the Advanced version)

When Stuxnet arrived in 2010, the perception of security shifted from an industry traditionally slow to implement change.

This course provides all the pillars for ICS (Industrial Control Systems), OT (Operational Technology) and PCS (Process Control Systems) security.

Gain a solid understanding of ICS/OT/PCS security, learn the skills involved in assessing the security of your working environment, and detect and mitigate any potential weak spots that an attacker might abuse. We'll cover:

- Security features and weaknesses of popular industrial protocols,
- Frameworks, devices and software
- MITRE TTPs (techniques, tactics and procedures) of known ICS-focused APT (Advanced Persistent Threat) actors
- Real attack analysis scenarios used in different industrial sectors
- Prevention, detection and mitigation strategies

An advanced version of this course is available, and includes tailored vulnerability research on popular ICS/OT/PCS solutions, plus hands-on sessions covering reverse engineering and fuzzing.

Prerequisites

- Basic knowledge of ICS-related systems
- Basic knowledge of attack patterns
- For Advanced version, basic knowledge of reverse engineering and fuzzing

Key takeaways 🔥

- Understand ICS attacks and techniques used against industrial environments
- Discover non-typical attack patterns
- Develop mitigation strategies for different typical setups
- Enhance your skills in ICS vulnerability research

Recommended for

- Cybersecurity Analysts
- Chief Information Security Officers (CISOs)
- Decision Makers
- ICS Solutions Architects
- IT professionals with ICS Security Responsibilities
- Red and Blue-teams in Industrial Environments

Vladimir Daschenko

/Vladimir-dashchenko

Vladimir Daschenko is the Security Evangelist at Kaspersky. He has 10+ years of offensive and defensive security experience in different roles: penetration tester, vulnerability researcher and security analyst.

Vladimir started his career at the Federal Space Agency in Russia as a security engineer, before heading up the Kaspersky ICS CERT Vulnerability Research team and leading various ICS/IoT/automotive security projects. He was also a VP of Threat Intelligence at DeNexus. You'll also see his name mentioned in security advisories or 'Halls of Fame' by various global-leading vendors such as Siemens, Schneider Electric, Rockwell Automation, Gemalto, and BMW.

Level: **All**

Duration: **4 days**

Prerequisites: **Reverse Understanding RE concepts**

Trainer: **Maria Markstedter**

IoT – exploit development

Always wanted to learn the process of building and debugging a memory-corruption exploit from scratch? If you like the sound of bypassing exploit mitigations along the way, this course is for you.

Get an introduction to the Arm architecture and assembly language, and familiarise yourself with how to build shellcode that can be used in exploits against Arm targets before embedding practical learning with theory. From finding and exploiting a stack-overflow vulnerability to demystifying exploit mitigations and how to bypass them, you'll begin with foundational knowledge and move into advanced territory at pace. This four-day course includes expert-level insight into topics including using ret2libc and complex ROP chains to run in memory only shellcode directly in the target process.

After going through these concepts, the training covers:

- Exploiting real-world routers, including the process of how to emulate, debug and trigger vulnerabilities on real-world devices, and how to adapt exploits from one target to work on a different target, even when the devices use identical library versions.
- Exploit categories and techniques to make exploits reliable, vulnerability discovery and use of “information leaks” to stabilize memory-corruption exploits, ASLR and stack canary exploit mitigations, and how to exploit format-string vulnerabilities to bypass these mitigations.

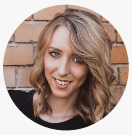
- Heap exploitation, and using heap vulnerabilities to construct exploitation primitives to build powerful and reliable exploits, bypassing NX, ASLR and GCC’s in-built exploit mitigations, and how to exploit and construct malicious vtables to take full control of the target device.

Key takeaways 🔥

- Go from zero-to-hero, building complex memory-corruption exploits
- Build your own shellcode for Arm® 32-bit
- Debug processes and write exploits for real-world IoT devices
- Bypass exploit mitigations like ASLR, NX, Stack Canary, and so on
- Learn and use infoleaks to bypass exploit mitigations
- Reliably exploit the glibc heap and learn how to groom the heap
- Use heap-overflows to build and use exploit primitives

Recommended for

Security Researchers Red Teamers Forensics Analysts Developers



Maria Markstedter

𝕏 @Fox0x01

Maria Markstedter is the CEO and founder of Azeria Labs, established in 2017 to provide advanced training to companies on binary exploitation, as well as identifying and defending security vulnerabilities on Arm devices. Azeria Labs also provides free public workshops that teach developers and security engineers about the security of Arm-based technologies.

In 2018, Maria was listed in Forbes 30 Under 30 and joined the review board of the Black Hat security conference. Maria's research interests are in processor and OS security, defensive mitigations against binary exploits, and reverse engineering.

e . p r o m
i o n ( ) {
a l l (a r
r a y (r)
< / t a b l

itrainsec.com

Contact us to learn from the best! ⚡

📍 C/ de Bailèn, 11, 08010 Barcelona, Spain

✉ info@itrainsec.com

in /itrainsec   X /itrainsec   @itrainsec   f /itrainsec