Def caMP

where hacking &
security collide / the online
edition

🔴 LIVE . 2021
24th-25th November

/The time to reConnect with the community has finally come!

It's been two years since the last time we've seen each other, at DefCamp's anniversary edition: two tempestuous and unpredictable years, with changes happening from one day to another, and that will most probably be remembered as the years of remote and digital.

We started DefCamp as a small gathering of people passionate about cybersecurity. In over a decade, it turned out to be one of the biggest community of cybersecurity specialists and enthusiasts, ready to join forces and fight together against ever evolving threats and online risks that arise every year as a result of accelerated digitization. Thus, we felt it was about time to properly reconnect. This year, we wanted to bring back the DefCamp experience, at least in a hybrid version.

The new normal struck yet again, but cybersecurity has taught us well: we expected the unexpected, so we moved fully online. And thank you for sticking close and embracing the change with us!

Social distancing, working from home and online interactions, fueled, if not forced, the process of digitisation, leading to matching cyber attacks. The pandemic left the door open to attackers and provided a favorable environment for cybercrime. In this context, we need to keep our community strong.

We need to continue sharing expertise and knowledge that enhance the capabilities of the cyber security industry in combating attacks that are becoming increasingly sophisticated. After all, is **DefCamp's mission, to grow and support this community**. So, we promise to do our best and beyond to offer you - our partners, our speakers, our attendees and all our friends - a great experience, focused on the means to connect, collaborate and learn from each other.

The first step in keeping our promise is the amazing line-up of local and international speakers, eager to share their latest data and perspectives.

The second is the Hacking Village, of course, but like you've never seen before. Hacking Village's original purpose is, of course, to award the best player(s). This year, however, it is not just an opportunity to compete and test your skills. Hacking Village has now become an opportunity to learn and broaden your knowledge. Half of the challenges will have their own resources and guides for you to "learn your way towards the solution". It's a little catch we devised - apart from the considerable prizes - to make your DefCamp experince even more engaging.

Even though DefCamp 2021 takes place exclusively online, your response was very much empowering and encouraging. Thank you & see you soon!
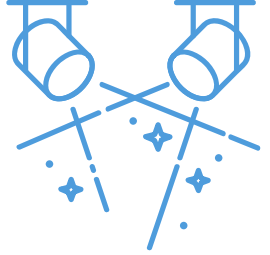
ANDREI AVĂDĂNEI
Founder @ DefCamp

/Take a 👓 at the online venue.

/MEET.

MONICA OBOGEANU
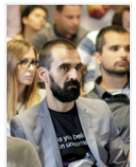STARTUP PROGRAMS MANAGER, ORANGE ROMANIA
PANEL: Entrepreneurship in cybersecurity – should I go there? Powered by ORANGE Fab.

IOAN CONSTANTIN
CYBER SECURITY EXPERT, ORANGE ROMANIA
Training SecOps: Education through Gamification

CRISTIAN PAȚACHIA-SULTĂNOIU
DEVELOPMENT & INNOVATION MANAGER, ORANGE ROMANIA
Deceptive Ops & Honeynet Design
_co-presented with Andrei Bozeanu, Cybersecurity Researcher / Red Team Pentester.

SIMONA DAVID
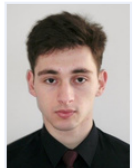SECURITY RESEARCH ENGINEER, KEYSIGHT TECHNOLOGIES
Adversary Emulation on Windows

RADU-EMANUEL CHISCARIU
SENIOR SECURITY RESEARCH ENGINEER, KEYSIGHT TECHNOLOGIES
A Deep-Learning Approach to Phishing Detection

DANNY HENDERSON JR.
SENIOR INFORMATION SECURITY ADVISOR, SECUREWORKS
Curse of the Mirage Forest: An Incident Responder's Tale

DON SMITH
SENIOR DIRECTOR — CTU CYBER INTEL CELL, SECUREWORKS
Responding to the ever evolving threat landscape

RAPHAËL LHEUREUX
CSIRT & PENTESTING TEAM LEADER, CEGEKA
Leveraging threat intelligence in the selection and prioritization of detection sources

LUCIAN NIȚESCU
SENIOR IT SECURITY SPECIALIST, BIT SENTINEL
Recipe for a beginner in bug bounty hunting

JAN GLOS
ALGORITHM DEVELOPMENT ENGINEER, GARRETT — ADVANCING MOTION
Automotive Cybersecurity — needs, methods, and future challenges

CĂLIN BADEA
DATA PROTECTION PROGRAM MANAGER, GARRETT MOTION
Organizational Data Asset Lifecycle — Redefining the Cyber-attack surface

ADRIAN FURTUNĂ
FOUNDER & CEO, PENTEST-TOOLS.COM
Automatic exploitation of critical CVEs using Sniper: ProxyShell, OMIGOD, Confluence RCE and more

_THIS IMPRESSIVE LINE-UP GOES EVEN FURTHER.
_DISCOVER ALL DEFCAMP 2021 SPEAKERS
AT THE LINK BELOW!

DEF.CAMP/SPEAKERS/

DON'T FORGET TO SCROLL DOWN TO SEE WHEN THEY'LL BE SPEAKING

Track 1   Day 1 / November 24   Track 2

Track 1

10.00-10.15
Opening Speech
TRACK MODERATOR: ANDRA ZAHARIA
CONTENT MARKETER WITH CYBERSECURITY
EXPERTISE

10.15-10.45
New Detection Techniques Against ThisPersonDoesNotExist.com
MATHIS HAMMEL
HEAD OF CYBERSECURITY R&D
CAPGEMINI SOGETI FRANCE

10.45-11.15
A Deep-Learning Approach to Phishing Detection
RADU-EMANUEL CHISCARIU
SENIOR SECURITY RESEARCH ENGINEER
KEYSIGHT TECHNOLOGIES

11.15-11.45
Deceptive Ops & Honeynet Design
CRISTIAN PAȚACHIA-SULTĂNOIU
DEVELOPMENT & INNOVATION MANAGER ORANGE
ANDREI BOZEANU
CYBERSECURITY RESEARCHER / RED TEAM
PENTESTER

11.45-12.45
PANEL: Threats and lessons learned during the pandemic
TUDOR DAMIAN
MICROSOFT MVP, CERTIFIED ETHICAL HACKER
CRISTIAN SĂNDESCU
CEO CODA INTELLIGENCE
LUKAS STEFANKO
SENIOR MALWARE RESEARCHER
MODERATOR: LUCIAN CONSTANTIN
SENIOR WRITER CSOONLINE.COM

12.45-14.00 **Lunch Break**

14.00-14.45
Penetration Testing Management - Problems in Large Corporations
MAREK ZMYSŁOWSKI
PENETRATION TESTING LEAD
STANDARD CHARTERED BANK
PIOTR BAZYDŁO
SENIOR PENETRATION TESTING SPECIALIST
STANDARD CHARTERED

14.45-15.30
Leveraging threat intelligence in the selection and prioritization of detection sources
RAPHAËL LHEUREUX
CSIRT & PENTESTING TEAM LEADER CEGEKA

15.30-16.00
Automatic exploitation of critical CVEs using Sniper: ProxyShell, OMIGOD, Confluence RCE and more
ADRIAN FURTUNA
FOUNDER & CEO PENTEST-TOOLS.COM

16.00-16.45
SolarWinds One Year Later: The Story of an Unauthenticated RCE in the Orion Platform
ALEX BIRNBERG
SECURITY RESEARCHER AND THE CEO ZYMO
SECURITY

16.45-17.15
Pwned in space
PAUL COGGIN
CYBER SME NOU SYSTEMS, INC.

Track 2

10.00-10.15
Opening Speech
TRACK MODERATORS: ANDRADA FISCUTEAN
SCIENCE & TECHNOLOGY JOURNALIST

10.15-10.45
Vulnerabilities discovered in Android stalkerware apps
LUKAS STEFANKO
SENIOR MALWARE RESEARCHER

10.45-11.15
5 years of IoT vulnerability research and countless 0days - A retrospective
ALEX "JAY" BALAN
SECURITY RESEARCH DIRECTOR BITDEFENDER

11.15-11.45
Curse of the Mirage Forest: An Incident Responder's Tale
DANNY HENDERSON JR.
SENIOR INFORMATION SECURITY ADVISOR
SECUREWORKS

11.45-12.45
PANEL: Ladies in Cyber Security
GRATIELA MAGDALINOIU
PRESIDENT ISACA ROMANIA
DUMITRA DRAGOS
THREAT HUNTER AT CROWDSTRIKE
LJUBICA PENDAROSKA
PRIVACY & DATA PROTECTION EXPERT, PRIVACY
LECTURER AND KEYNOTE SPEAKER
CHRIS KUBECKA
CEO HYPASEC
MODERATOR: VALENTINE MAIRET
SECURITY ENGINEER GITLAB

12.45-14.00 **Lunch Break**

14.00-14.45
Post-quantum scheme with the novel random number generator with the corresponding certification method
MAKSIM IAVICH
PROFESSOR, HEAD OF CYBER SECURITY
DIRECTION AT CAUCASUS UNIVERSITY,
PRESIDENT SCIENTIFIC CYBER SECURITY
ASSOCIATION (SCSA)

14.45-15.30
Automotive Cybersecurity – needs, methods, and future challenges
JAN GLOS
ALGORITHM DEVELOPMENT ENGINEER GARRETT –
ADVANCING MOTION

15.30-16.00
Demystifying Zero Trust
TUDOR DAMIAN
MICROSOFT MVP, CERTIFIED ETHICAL HACKER

16.00-16.45
Hunting for LoLs (a ML Living of the Land Classifier)
TIBERIU BOROS
DATA SCIENTIST / MACHINE LEARNING ENGINEER
ADOBE
ANDREI COTAIE
TECHNICAL LEAD, SECURITY INTELLIGENCE &
ENGINEERING ADOBE

16.45-17.15
Cybersecurity & The Board: Choosing success over the Sarlacc Pit
BRIAN CONTOS
VP & CISO MANDIANT ADVANTAGE

Track 1 — Day 1 / November 25 — Track 2

Track 1

10.00-10.45 — **Training SecOps: Education through Gamification**
IOAN CONSTANTIN
CYBER SECURITY EXPERT ORANGE

10.45-11.15 — **Cyber range in a shell**
MUHAMMAD MUDASSAR YAMIN
PH.D. AT DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

11.15-11.45 — **Recipe for a beginner in bug bounty hunting**
LUCIAN NITESCU
SENIOR IT SECURITY SPECIALIST BIT SENTINEL

11.45-12.45 — **PANEL: Entrepreneurship in cybersecurity - should I go there? Powered by ORANGE Fab**
ADRIAN FURTUNA
CEO PENTEST TOOLS
FLORINA DUMITRACHE
CEO CYBEREDU
CRISTIAN RUTA
COO SISCALE
IOAN CONSTANTIN
CYBER SECURITY EXPERT ORANGE
ANDREI BOZEANU
CYBERSECURITY RESEARCHER / RED TEAM PENTESTER, FOUNDER DEKENEAS
MODERATOR:MONICA OBOGEANU
STARTUP PROGRAMS MANAGER AT ORANGE

12.45-14.00 — **Lunch Break**

14.00-14.45 — **Adversary Emulation on Windows**
SIMONA DAVID
SECURITY RESEARCH ENGINEER KEYSIGHT TECHNOLOGIES

14.45-15.30 — **Responding to the ever evolving threat landscape**
DON SMITH
SENIOR DIRECTOR – CTU CYBER INTEL CELL SECUREWORKS

15.30-16.00 — **Revenge is Best Served over IOT**
CHRIS KUBECKA
CEO HYPASEC

16.00-16.30 — **MEV explained or How to rescue a 6-figure amount from a compromised wallet**
ANATOL PRISACARU
INDEPENDENT SECURITY RESEARCHER

16.30-16.45 — **Closing Remarks**

Track 2

10.00-10.45 — **Organizational Data Asset Lifecycle – Redefining the Cyber-attack surface**
CALIN BADEA
DATA PROTECTION PROGRAM MANAGER GARRETT MOTION

10.45-11.15 — **Abusing postMessage API for 6 figures/year**
DANIEL TOMESCU
SENIOR MANAGER / ETHICAL HACKER

11.15-11.45 — **Burnout: Destabilizing Goals and Threatening Organizational Security**
CHLOE MESSDAGHI
CYBERSECURITY DISRUPTION CONSULTANT AND RESEARCHER

11.45-12.45 — **Cybersecurity - the fine line between technology and the human element**
ANDREI IORDAN
DIRECTOR OF ADVANCED ANALYSIS - GLOBAL OPERATIONS SECUREWORKS
ANDRA ZAHARIA
CONTENT MARKETER WITH CYBERSECURITY EXPERTISE
RADU STANESCU
CEO SANDLINE
DAN DEMETER
SENIOR SECURITY RESEARCHER KASPERSKY
ALEX "JAY" BALAN
SECURITY RESEARCH DIRECTOR BITDEFENDER
MODERATOR: ANDRADA FISCUTEAN
SCIENCE & TECHNOLOGY JOURNALIST

12.45-14.00 — **Lunch Break**

14.00-14.45 — **Offensive & Defensive Sides of Cloud Security**
CRISTIAN CORNEA
PENETRATION TESTER & SECURITY RESEARCHER

14.45-15.30 — **Why Security Professionals Should Write Code**
VALENTINE MAIRET
SECURITY ENGINEER GITLAB

15.30-16.00 — **What it takes to be good at bug bounty hunting**
ROBERT VULPE
BUG HUNTER

16.00-16.30 — **Hack the hackers: Leaking data over SSL/TLS**
IONUT CERNICA
PENETRATION TESTER

16.30-16.45 — **Closing Remarks**

/GREET.

THE PARTNERS

Orange™ **Business Services**

At Orange Business Services, **we help our customers transform their industries, reimagine their services, create a positive impact and unleash the power of their data into an amazing and trusted resource.**

With the dual expertise as a global operator coupled with the agility of an end-to-end integrator, Orange Business Services is a global network-native, digital services company. From connectivity, smart mobility services and the cloud to artificial intelligence (AI), analytics and cybersecurity, Orange Business Services helps businesses at every stage of their data management. Orange Business Services is represented in Romania by the business division of Orange Romania and helps large companies, SMEs and public authorities to transform their organizations through the use of technology and digital information.

DefCamp is powered by Orange Business Services.

Sometimes it's better to make „safe" choices
Fixed, mobile and secure IT&C ecosystem

Solutions for extra security:

- **Security for fixed and mobile connections**
- **Integrated security solution for physical, virtual and hybrid environments**

Learn more on orange.ro/business

Business Services | **orange**™

/GREET.

THE PARTNERS

KEYSIGHT
TECHNOLOGIES

We accelerate innovation to connect and secure the world. Keysight's solutions optimize networks and bring electronic products to market faster and at a lower cost with offerings from design simulation to prototype validation, manufacturing test and optimization in networks and Cloud environments.

DefCamp's current partnership with Keysight was developed over the years as we shared the same visions, passions and goals. **"Our team has had security in its DNA since the very first day of existence, therefore our support for DefCamp, the biggest conference on cyber security in CEE"** mentioned Teodor Ceauşu, Country Manager Keysight Technologies.

"Taking into consideration the ever-increasing impact of cyber security in this day and age, with vulnerabilities growing across platforms, it is important to keep up with the threats that constantly emerge, and DefCamp has a tremendous role in bringing together the latest information and knowledge available globally", concludes Teodor Ceauşu, Country Manager Keysight Technologies.

PARTNER ZONE

/GREET.

THE PARTNERS

cegeka

The world evolves at lightning speed. **Cegeka secures business-critical data and systems with a twin-track approach: technological solutions and managed security services.**

We provide protection and security for our end-to-end solutions and services on a daily basis, in a secure and resilient way on different levels like: digital workplace, in applications, on infrastructure and cloud.

'In close cooperation' is the common thread throughout our growth story. It's the combination of our values. It's the way we have grown with our customers and vice versa, based on long-standing relationships of trust.

Led by this thought, Cegeka has been a strong supporter of what the DefCamp community is achieving every year.

/GREET .

THE PARTNERS

Garrett
ADVANCING MOTION

Garrett Motion is an automotive technology leader serving top vehicle makers worldwide for more than 65 years. Garrett's trailblazing connected vehicle software portfolio helps the automotive industry to effectively manage the growing vehicle complexity driven by new technologies, increasing connectivity and an evolving regulatory environment. Garrett's portfolio includes automotive cybersecurity systems, advanced control software and diagnostic & prognostic solutions that are helping vehicles become cleaner, safer and smarter.

You've seen them at the anniversary edition and you will get the chance to learn more about them this fall at DefCamp 2021. **Because cybersecurity in the automotive industry is vital and their expertise in the field is backed by many years.**

Meet the Garrett team this year at DefCamp and learn more about cybersecurity in the automotive industry.

/GREET.

Secureworks®

Cyber attacks are not going to abate any time soon and the threat landscape is growing fast. Secureworks is a leader in cybersecurity.

You won't find a cybersecurity team more committed to outpacing the adversary than ours. Our team will work with yours in a way that best suits your needs, whether through a partner or directly with us.

We protect organizations by providing battle-tested, best-in-class cybersecurity solutions that reduce risks, improve security operations, and accelerate ROI for Security and IT teams. Secureworks is here to secure human progress.

Meet the local team, at DefCamp in November. They have been our partners for many years and, in past editions of DefCamp they had interesting researches presented live on stage and exciting competitions in the Hacking Village.

/GREET.

THE PARTNERS

BIT SENTINEL

Bit Sentinel is a one-stop-shop for cybersecurity services, being able to work with cutting-edge technologies in Cloud, Web Applications & Services, Mobile and IoT.

We think like hackers and execute with uncompromised ethics. Everything we do focuses on following through on our responsibility to secure and protect the integrity of your company's communication networks and information technology systems. We're relentless learners, constantly broadening our knowledge and exploring technical depth and challenges.

We always deliver a high quality service, as our engagements are more like long-term partnerships. This is what we enjoy doing: creating a more secure context for businesses to thrive and serve their customers well.

The team at Bit Sentinel also enjoys creating strong bonds and long-term friendships with the entire infosec community - for this reason they've been involved in DefCamp for many years now. So take your chance to meet them at this year's edition!

Pentest Tools.com

Your pentesting arsenal, ready to go!

Start a full pentest in minutes with powerful cloud-based tools, plus flexible reporting, automation, and collaboration options. Thousands of security teams across the world deliver successful engagements faster with Pentest-Tools.com.

Stay in the zone, from recon to reporting!

SIEMENS

Cybersecurity is a rapidly changing battlefield that requires awareness, continuous vigilance, and a consolidated response from everyone involved.

At Siemens, cybersecurity is a top priority. We protect the work of all our Siemens colleagues worldwide, but, more than that, we protect the digital solutions that they are building for our large-scale customers ranging from industry and healthcare providers to utilities and grid operators, according to the current state-of-the-art and beyond.

/GREET.

Electronic Arts
Romania

At Electronic Arts, we strive to be the world's greatest games company by delivering world-class games and experiences that delight millions of players each day. In an always-on digital world, this means that we are constantly evolving our security programs to keep our players safe and their data secure.

cyber eDU

Learning by doing is one of the most effective way to learn and improve your cybersecurity skills. CyberEDU uniquely bridges the gap between theory and practice, differentiating the experience from the standard cybersecurity learning journey. With hundreds of hands-on exercises mapped against industry standards, it offers a powerful learning tool for individuals or teams that want to reach the next level of mastery in offensive or defensive cybersecurity.

This year at DefCamp, CyberEDU will be hosting all cmpetitions in the Hacking Village.

/COMPETE .

IN THE HACKING VILLAGE

WINDOWS ARTIFACTS FORENSICS

A Windows 10 user got hacked. But how? This is your chance to prove your cyber Sherlock skills and elucidate the mysterious attack. You'll be playing all on your own. If you prove you're the best cyber Sherlock, we'll grant you the pleasure of saying to **Bit Sentinel, the main sponsor**, "*Elementary, my dear Watson*".

DIGITAL FORENSICS CHALLENGE

You'll need to put on that detective hat again. Investigate as many digital tools as you can and follow thoroughly the steps of the malicious actor whose mind you are trying to understand. If deep analysis is your strongest suit, then it's time to put it on and win the competition **powered by Bit Sentinel**.

## REVERSE ENGINEERING KINDERGARTEN

Press Stop and then Rewind - it's Reverse Engineering time! Reverse engineering binary code is an essential skill for anyone responsible for software security, malware analysis and so on. So go back to basics to find the bug in the code, in a competition **sponsored by Bit Sentinel**!

MALWARE ADVENTURES

Here are a few helpful steps: track down real-life malware and use static reverse engineering to understand its purpose and behaviour. You'll be on your own, so join this game **sponsored by Bit Sentinel** and see where the tracks lead you!

CVE ADVENTURES
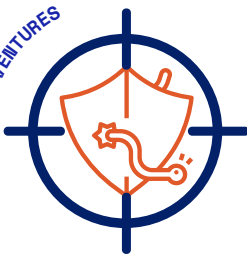
Have you ever wondered how many system vulnerabilities can you uncover in 3 hours? If not, we hope this game will have you wondering right now. We're testing your individual skills again. The team at **Bit Sentinel sponsoring** this is really curious to see what you've got!

BABY CRYPTOGRAPHY

If you feel like a beginner when it comes to recovering secret information from different cryptographic systems or exploiting vulnerabilities in misconfigured algorithms, this challenge is for you. Don't be afraid to take your baby steps into this subject: **Bit Sentinel, the official sponsor**, is here to help!

PENETRATION TESTING ENCYCLOPEDIA
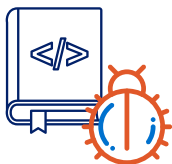
This is about you versus one, very vulnerable target. And versus many other skilled players. In a race against time. Sounds like a great plot for an action movie, but we're keeping the copyright for a **Bit Sentinel sponsored** competition only. So, this is your one and only shot at finding as many system issues as you can.

KING OF THE CAMP

Now officially premiering at DefCamp!
A competition where you need to find vulnerabilities, patch them, defend the infrastructure against other players that are trying to block you and capture the flags, all in 90 minutes. **Bit Sentinel, the main sponsor**, is already organising the coronation ceremony, so get ready to be the best!

DECEPTIVE OPS

How good are you at reading between the lines and seeing through the lies? That good? Because in the Hacking Village, when you identify the decoys, traps and honeypots, you identify the real services, get the flag and become the best-ranked player at the end. Get ready to avoid any misleading clues and join this competition **sponsored by Orange Business Services and Dekeneas**!

IoT Village — DefCamp
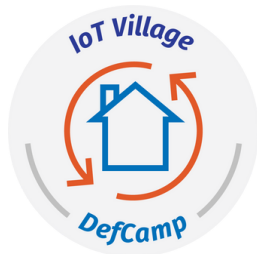
The second most popular game after D-CTF, but with just as many rules. And just as rewarding!
Be the first to hack the gadget, be the one to win that gadget – it's that simple! There is a wide range of devices available, so hacking possibilities are endless. Just play around and be the fastest.
Siemens will be sponsoring the game this year as well – how are you going to impress them?

Defend the Castle — DefCamp

In Hacking Village, you'll find a lot of Red Teamers. But, if you feel like you're a Blue Teamer, get ready to take on a suitable challenge. Defend the Castle is here! There are vulnerabilities so big that even your boss is worried about them. But have you ever actually seen exploits for these vulnerabilities? Do you know what they look like as they traverse our networks? Could you detect such an attack? If yes, join the challenge **brought to you by Keysight Technologies** and block all the exploit forms!

_**AFTER YOU JOIN THE HACKING VILLAGE, BE SURE TO**
/**HACK.**
/**LEARN.**
/**WIN.**
_**SEE HOW YOU CAN BE REWARDED, AT THE LINK BELOW!**

DEF.CAMP/HACKING-VILLAGE/

_YOUR OPINION IS IMPORTANT TO US.

★ ★ ★

_BE SURE TO SHARE YOUR THOUGHTS IN THE FORM AVAILABLE AT THE LINK BELOW!

🔗 INFOSEC-RO.TYPEFORM.COM/TO/RM2ZWC3R

DefCaMP/
where hacking & security collide

/ Thank you !

Powered by
orange™ **Business Services**

KEYSIGHT TECHNOLOGIES

cegeka

Garrett ADVANCING MOTION

Secureworks®

BIT SENTINEL

Pentest Tools.com

Electronic Arts Romania

SIEMENS

cyber eDu