AREA41 CONFERENCE

AGENDA 2024

Day 1 June 6	Track 1 (main hall)	Track 2 (underground)
08:30	Door Opening Registration and Coffee	
09:00	Opening Ceremony	
09:30	Keynote: Hacker's Perspective on New Risks: Revising the Cybersecurity Priorities for 2024 Paula Januszkiewicz Founder & CEO of CQURE	
10:00	Coffee Break	Coffee Break
10:30	Switching 400'000 Volts with a TCP packet [Cyrill Brunschwiler]	Action Anomalies: A hackers guide to Github Actions [Elliot Ward]
11:20	Nearing the ePOcalypse: A tale of vulnerabilities & incentives in the infosec industry [Alain Mowat]	Insert coin: Hacking arcades for fun [Ignacio Navarro]
12:10	Lunch Break	Lunch Break
13:40	Armored Witness - Building a Trusted Notary for Bare Metal [Andrea Barisani]	Shufflecake, AKA Truecrypt on Steroids for Linux [Tommaso Gagliardoni]
14:30	Automating Malware Development: A Red Teamer's Journey [Gian Demarmels]	Did You Say Out of Scope? Reconsidering Self-XSS and Exploring Novel Attacks with Cookie Tossing [Thomas Houhou]
15:20	Intelligence-Driven Threat Hunting: Exposing the Invisible Enemy [Sylvain Hirsch]	Call on me, Unify! - Hacking Desktop Phones [Michael Oelke]
16:10	Coffee Break	Coffee Break
16:40	New stories of money – Crypto, DeFi, Hacks & Attacks [Marco Preuss]	Guardians of the Grid: Purple Playoffs in OT Adversary Emulation [Jeroen Vandeleur + Nick Foulon]
17:30	Exploiting Bluetooth - from your car to the bank account$$ [yso]	Eyes Wide Open: Mastering the Art of Supply Chain Attacks with Client-Side Monitoring [Juerg Fischer + Dai Littlewood]
18:30 21:30	Networking BBQ – 1.floor	

Day 2 June 7	Track 1 (main hall)	Track 2 (underground)
09:30	Door Opening Registration and Coffee	
10:00	The CTF to Career Pipeline [Jam (Vie) Polintan]	Cloud-native software supply chain security: the hard truth [Daniel Drack]
10:50	Shells at Midnight: Turning a Spam Filter Against Itself [Michael Imfeld]	Balancing Efficiency and Security - Unveiling the Risks in Cloud-Based Endpoint Management [Oleksandr Kazymyrov]
11:40	Defeating behavior detection of remote code injection abusing shared sections and handle inheritance [Rafael Salema Marques]	Public Cloud public attacks: A summary of attacks seen by CloudIntel [Himanshu Anand]
12:30	Lunch Break	Lunch Break
14:00	Phishing the Phishing Resistant - Phishing for Primary Refresh Tokens in Microsoft Entra [Dirk-jan Mollema]	Actionable Incident Response Documentation - When The Ink Meets The Road [Gergana Karadzhova-Dangela]
14:50	Technical Deep Dive into the XZ backdoor [Timo Schmid]	Digital Self Defense for Investigative Journalists [Rico]
15:40	Coffee Break	Coffee Break
16:10	Machine Learning for Enhanced Malware Detection & Classification [Solomon Sonya]	Red Cell - Mimicking Threat Actors for Realistic Responses [Thomas Chopitea]
17:00	Closing Ceremony	

DAY 1 — 6. JUNE 2024

09:30 - Day 1 - Track 1

Keynote: Hacker's Perspective on New Risks: Revising the Cybersecurity Priorities for 2024

Paula Januszkiewicz (Founder & CEO of CQURE)

Abstract:

The transformation is gaining momentum! Over the last tumultuous years, investments in digital transformation have been growing, with companies worldwide exploring its potential by introducing new technologies, approaches and social changes. As more data than ever is put online, cybersecurity is now a major concern for everyone – large corporations, governments, and companies of all sizes. The transformation, however, also has its dark side. Thanks to it, the hackers are able to exploit vulnerabilities in the infrastructure with even greater precision than before.

As the financial, operational, legal, and reputational implications of neglecting cybersecurity risks could be considerable, well-known analysis & protection methods should be developed and complemented.

During this presentation, the most serious risks of 2024 will be explored and explained. Paula Januszkiewicz will demonstrate how hackers and cybercriminals identify and exploit threats using the most up-to-date techniques, so that you are able to observe them on your monitoring system and prevent them in the future. You will also become familiar with the most advanced phishing attacks, credential theft techniques, ransomware distribution methods, and ways of gaining access to vendor-controlled systems.

Join Paula to understand what actually is possible in the year of 2024. As the cyber transformation leads to better effectiveness of hackers' activities, there is no time to lose!

Bio:

Paula Januszkiewicz is the Founder and CEO of CQURE and CQURE Academy, companies she established back in 2008. She is also an Enterprise Security MVP, honorable Microsoft Regional Director, and a world-class cybersecurity expert, consulting Customers worldwide. In 2017, Paula graduated from Harvard Business School. She delivers keynotes and sessions at the biggest world conferences such as RSA, Black Hat, Microsoft Ignite, SecTor Canada, Australian Cyber Conference, GISEC, GITEX, LEAP, and many others. She is often a top-rated speaker, including being chosen as the No. 1 Speaker at Microsoft Ignite (among 1,100 speakers at a conference with 26,000 attendees) and at Black Hat Asia 2019. At the RSA Conference, two of her sessions were among the top 5 best rated. Paula is known for her unique stage presence that is always well-received among diverse audiences, often gathering thousands of people!

Paula has over 19 years of experience in the cybersecurity field, performing penetration tests, architecture consulting, trainings, and seminars. Every year, she takes over 200 flights to provide cybersecurity services for CQURE's Customers. Paula and her Team also design security awareness programs for various organizations, including awareness sessions for top management. Together, they create various security tools (CQTools) supporting penetration tests, incident response, and forensics, which are shared with the community. Paula is a member of the Technical Advisory Board at the Royal Bank of Scotland/Natwest. And to top it all off, she has access to the source code of Windows!

10:30 - Day 1 - Track 1

Switching 400'000 Volts with a TCP packet

Cyrill Brunschwiler (Compass Security)

Abstract:

With the history of blackouts in the Ukraine and the appearance of the suspended nuclear plant Muehleberg in the Vulkan leak its time to beef-up Swiss blue and red teamers with knowledge on the Swiss electrical grid and substations in particular. This talk aims to pass-on what I learned about the electrical grid along my hacker journey and to prevent you from blowing stuff and being outsmarted by OT devices. The presentation will provide an overview of the Swiss electrical grid, including its network levels and electrical substations. We will delve into the workings of substations, the protective equipment used, and the logical representation of such. The role of Intelligent Electronic Devices (IEDs) will be explored, along with the communication processes between these devices. We will also discuss the IEC 61850 and IEC 60870-5-104 protocols, which are integral to the functioning of these systems. Additionally, we will discuss the pentest tool landscape, the concept of interlocking, and important considerations when dealing with protocols. Essentially, a talk about electrical grids from a hacker perspective.

Bio:

Cyrill developed application security hands-on exercises in his early days. Since 2005, he has supported numerous projects with expertise in the areas of penetration testing, red teaming, incident response and digital forensics. Cyrill is a proud crew member of Compass Schweiz and is having a hard time to flee the boring paperwork and slide shows to rekindle his true passion for bits and electrons.

10:30 - Day 1 - Track 2

Action Anomalies: A hackers guide to Github Actions

Elliot Ward (Snyk)

Abstract:

In the DevOps era of frequent releases, CI tools such as Github actions are powerful platforms to enable secure and rapid software releases, but what additional attack surface do these often privileged components come with? This talk covers a recent research project from Snyk Security Labs to understand Github actions in depth and how they can be attacked to leak cloud environment access tokens, arbitrary secrets and result in a full compromise of the repository. Security engineers, pentesters and bug hunters alike will come away knowing the threat landscape for Githubs CI platform, and through case studies of high impact vulnerabilities we have uncovered, be equipped to exploit and secure Github actions.

Bio:

Elliot is a senior security researcher at software security company Snyk. He has a background in software engineering and application security.

11:20 - Day 1 - Track 1

Nearing the ePOcalypse: A tale of vulnerabilities & incentives in the infosec industry

Alain Mowat (Orange Cyberdefense)

Abstract:

It has generally been accepted that vulnerabilities will endlessly be discovered and patched because the humans developing the software or hardware are prone to making errors. Though this holds some truth, accepting it as a foregone conclusion has given vendors an easy excuse to sell vulnerable products and even profit from it.

During a vulnerability research project, my team and I discovered several vulnerabilities in McAfee (now Trellix) products, ranging from trivial Cross-Site Scripting issues to SQL injections and Admin account takeover in the ePolicy Orchestrator. Most of these issues were discovered within just a couple weeks of effort using command-line tools such as find and grep.

These vulnerabilities will be presented and used as a steppingstone to discuss why we so easily discover SQL injections or even Buffer Overflows in the query strings of popular products.

Though it may seem utopian to have a vulnerability-free world, aligning incentives and allowing customers to know how much vendors value the security of their own products (and ultimately that of their customers) could go a long way in improving on the current state and better protect everyone.

Bio:

Alain Mowat joined SCRT in 2008 as a penetration tester and subsequently led the pentesting team in the same company for many years until turning towards Research & Development. While still performing various engagements throughout the year, Alain is also dedicated to exploring new approaches to be used by the offensive security industry to better secure client infrastructures. Aside from these activities, Alain was an active member in the 0daysober CTF team that finished 3rd at DEFCON CTF in 2015 and has responsibly disclosed vulnerabilities in multiple products such as Citrix NetScaler, SonicWall SRA & SMA, Barracuda, Twitter and McAfee's ePolicy Orchestrator. Alain is also responsible for giving various security-related trainings at SCRT and has presented at several Swiss conferences, such as Insomni'hack, Secure IT VS CyberSecurity Alliance and SIGS.

11:20 - Day 1 - Track 2

Insert coin: Hacking arcades for fun

Ignacio Navarro

Abstract:

Since we were children we wanted to go to the arcade and play for hours and hours for free. How about we do it now? In this talk I'm Since we were children we wanted to go to the arcade and play for hours and hours for free. How about we do it now? In this talk I'm gonna show you some vulnerabilities that I discovered in the cashless system of one of the biggest companies in the world, with over 2,300 installations across 70 countries, from arcades in Brazil, amusement parks in the United Arab Emirates to a famous roller coaster in Las Vegas. We will talk about API security, access control and NFC among other things.

Bio:

Ignacio Navarro, an Ethical Hacker and Security Researcher from Cordoba, Argentina. With around 6 years in the cybersecurity game, he's currently working as an Application Security. Their interests include code analysis, web application security, and cloud security. Speaker at Hackers2Hackers, Security Fest, BSides, Diana Initiative, Hacktivity Budapest, 8.8, Ekoparty.

13:40 - Day 1 - Track 1

Armored Witness - Building a Trusted Notary for Bare Metal

Andrea Barisani (WithSecure)

Abstract:

We are building an Open Source https://transparency.dev/ witness, in collaboration with Google. This project entailed creating new hardware (USB armory LAN with PoE) software (Trusted OS and Applet) leveraging on TamaGo and GoTEE frameworks. This presentation aims to discuss the journey of this project, achievements (such as bare metal Go IRQ handlersâ€¦in space!) and results.

Bio:

Andrea Barisani is an internationally recognized security researcher. Since owning his first Commodore-64 he has never stopped studying new technologies, developing unconventional attack vectors and exploring what makes things tick...and break. His experience builds on large-scale infrastructure defense, penetration testing and code auditing with particular focus on safety critical environments, with more than 15 years of professional experience in security consulting. His main focus lies on the converge between secure hardware and software, an interest consolidated in the authorship of the USB armory hardware project and the TamaGo bare metal framework. He is a well known international speaker, having presented at BlackHat, CanSecWest, Chaos Communication Congress, DEFCON, Hack In The Box, among many other conferences, speaking about innovative research on automotive hacking, side-channel attacks, payment systems, embedded system security and many other topics.

13:40 - Day 1 - Track 2

Shufflecake, AKA Truecrypt on Steroids for Linux

Tommaso Gagliardoni (Kudelski)

Abstract:

Shufflecake is a novel, free, open-source data encryption tool that allows the creation of hidden volumes on a storage device in such a way that it is very difficult, even under forensic inspection, to prove the existence of such volumes. This is useful for people whose freedom of expression is threatened by repressive authorities or dangerous criminal organizations, in particular: whistleblowers, investigative journalists, and activists for human rights in oppressive regimes. You can consider Shufflecake a "spiritual successor" of tools such as TrueCrypt and VeraCrypt, but vastly improved: it is fast, supports any filesystem of choice, and can manage multiple layers of nested decoy volumes, so to improve user experience and make deniability of the existence of these partitions really plausible. Shufflecake is the result of a multi-year research aimed at solving fundamental limitations of plausible deniability tools. It has been peer-reviewed and presented at top IT conferences such as DEF CON Demo Labs and ACM CCS. It is under active development, and the open source community is welcome to contribute. In this talk we will present the history and limitations of other existing solutions, we will show how Shufflecake works and solves such limitations, and we will see why Shufflecake is an indispensable tool in the arsenal of users facing violent or coercive investigation.

Bio:

Tommaso "tomgag" Gagliardoni is a mathematician, cryptographer, and privacy advocate. He published influential peer-reviewed papers in the areas of cryptography, quantum computing, security, and privacy, and spoke at many international conferences in these fields. Additionally, he has a background in privacy hacktivism, investigative journalism, and ethical hacking, and being a strong advocate of the FOSS philosophy and digital freedoms. Tommaso obtained a PhD in cryptography at the Technical University of Darmstadt, Germany. He worked at IBM Research before joining Kudelski Security in 2019, where he is currently technical lead for the initiatives in quantum security and advanced cryptography.

14:30 - Day 1 - Track 1

Automating Malware Development: A Red Teamer's Journey

Gian Demarmels (Redguard)

Abstract:

Adversary simulation and red team operations play a crucial role in fortifying defences against sophisticated adversaries. As defences getting better and EDR systems being deployed everywhere, malware development is becoming an important skill for red teamers.

Red teamers are often in need to develop custom loaders capable of bypassing these defences. Developing a modern, customizable, and evasive loader involves multiple steps, which can be a time-consuming and complex process. Often multiple existing malware techniques need to be combined and adapted to the respective situation. This talk delves into my journey of automating malware development to create loaders for red team operations and discusses the challenges I faced.

Bio:

Gian Demarmels is a former information security engineer in the e-commerce field and now works as a security tester at Redguard. As part of Redguard's offensive security team, Gian conducts penetration tests, attack simulations and red teaming operations, with a special interest in EDRs, evasion tactics and malware development in general. During the last year, Gian delved deep into this fascinating world of malware development and went down the rabbit hole of creating an internal framework to generate customizable and evasive shellcode loaders for various red team operations.

14:30 - Day 1 - Track 2

Did You Say Out of Scope? Reconsidering Self-XSS and Exploring Novel Attacks with Cookie Tossing

Thomas Houhou

Abstract:

Cookie tossing is a web attack that consists of injecting cookies from a vulnerable or malicious subdomain in order to poison other websites under the same parent domain. As part of a coordinated vulnerability disclosure with the Swisscom Bug Bounty program and Project Jupyter, this talk will describe how such a technique can systematically turn Self-XSS into a high-impact bug and then explore how it also results in novel web attacks. Ultimately, the aim is to draw attention to the strong capabilities of cookie tossing and the many creative attack vectors it enables.

Bio:

Bug Bounty Hunter and Cyber Security MSc student at ETH Zürich.

15:20 - Day 1 - Track 1

Intelligence-Driven Threat Hunting: Exposing the Invisible Enemy

Sylvain Hirsch (Mandiant)

Abstract:

Advanced Persistent Threats (APTs) exploit gaps in traditional defenses, but their tactics, techniques, and procedures (TTPs) offer a roadmap for detection. This presentation reveals a proven methodology for uncovering and hunting APTs, leveraging the power of intelligence, frontline expertise, and deep TTP analysis. Gain actionable insights and learn how to apply these intelligence-driven techniques to enhance your organization's threat hunting capabilities. This presentation will illustrate the methodology with real-world examples, including the identification of APT39 and APT41 cyber espionage campaigns.

Bio:

Sylvain Hirsch is a cyber security professional with extensive experience in incident response, cyber threat intelligence and cyber resilience strategy. He started his journey in cyber security with a master's degree in digital investigation and identification at the University of Lausanne. Sylvain worked for Credit Suisse's Threat Detection and Response team in Zurich and Singapore. He then worked as an Incident Responder at Mandiant in Singapore. In this role, Sylvain led investigations of advanced and persistent threats, performed Purple Team Exercises to identify security gaps, and conducted trainings to enhance organization's defense and response capabilities. Sylvain is currently part of Mandiant Strategy Services, now part of Google Cloud, helping organizations with their cyber resilience strategy, assessing their cyber maturity, improving their defense and response capabilities, and conducting cyber attack simulations with technical and executive teams. Sylvain is a guest lecturer at the University of Lausanne and has presented at multiple cyber security conferences over the past 3 years. Sylvain is also actively involved in several cyber communities and is leading a network of cyber professionals from the public, private and academic sectors in Singapore.

15:20 - Day 1 - Track 2

Call on me, Unify! - Hacking Desktop Phones

Michael Oelke (Pentagrid)

Abstract:

In this talk, we dive into the vulnerabilities discovered in various Unify desktop phones during a research project. Insecure default settings and improper permission configurations expose these devices to remote compromise. We will explore the step-by-step process of identifying and exploiting these vulnerabilities. Additionally, the session will demonstrate how a seemingly benign screenshot tool was leveraged to escalate privileges. Due to the vendor's insecure by default approach, we believe there are many vulnerable installations outside. We will also discuss considerations for securing these devices within your network infrastructure to prevent similar threats.

Bio:

Michael studied business informatics at the Humboldt University, Berlin. He worked as a game developer and subsequently as a teacher for maths and computer science before starting his career in IT security. He currently focuses on web application security at Pentagrid.

16:40 - Day 1 - Track 1

New stories of money – Crypto, DeFi, Hacks & Attacks

Marco Preuss (Kaspersky)

With current Bitcoin price increase, Crypto got more attention in the public, again - though underlying misuse, attacks and hacks are going on for many years. In this talk I will dig into different recent attacks, problems and common “how to behave”. I will cover starting from the more common attack methods to advanced and stepping into DeFi.

Bio:

Marco Preuss has been working in the area of networking and IT security since the early 2000s. Having a long time experience in his role, he is responsible for monitoring the threat landscape in Europe while specializing in threat intelligence, darknet research, password security, IoT security. and privacy. In addition to research-related projects, Preuss is a regular speaker at both closed and public events.

16:40 - Day 1 - Track 2

Guardians of the Grid: Purple Playoffs in OT Adversary Emulation

Jeroen Vandeleur + Nick Foulon (NVISO)

Abstract:

This session dives deep into the evolution of cyber defense tactics, laying bare the necessity of a holistic approach where offensive and defensive techniques are harmoniously amalgamated. By juxtaposing IT and OT, we unravel their innate intricacies and spotlight the compelling need for a harmonized security blueprint, especially during those critical junctures of incident analysis and swift breach detection. As we journey further, attendees will be introduced to the groundbreaking utility of adversary emulation, spotlighting CALDERA's prowess for OT-specific plugins and submodules. This enlightening segment not only showcases the tactics, techniques, and procedures (TTPs) of potential adversaries but also delineates how defenders can counteract, adapt, and prepare. Our exploration doesn't stop there. The crux of defense, as we advocate, hinges on a potent blend of technology and architecture. Learn how a meticulously crafted architectural model can become the lighthouse, illuminating dark spots and enhancing visibility within sprawling OT terrains. Moreover, we dissect state-of-the-art detection technologies, detailing the operational capabilities and unique advantages of Microsoft Defender for IoT. The climax of our discourse is an immersive emulation exercise set within the confines of a virtualized electric plant. This ambitious endeavor is a precursor to our groundbreaking project—a tangible, physical firing range tailored for OT security testing. Experience firsthand the strategies deployed, challenges faced, and the riveting results of this emulation.

Bio:

Jeroen Vandeleur is a highly skilled and experienced senior security expert at NVISO, specializing in security architecture, cloud security, and automation within cloud and virtual environments. With more than 15 years of experience in the cybersecurity field, Jeroen has tackled complex challenges and provided concrete advice on avoiding, detecting, and responding to cybersecurity incidents. In addition to his work at NVISO, Jeroen is also a respected SANS author and training instructor for their "SEC598: Security Automation for Offense, Defense and Cloud" course. He is a certified Cisco CCNP Security expert and a GIAC-certified penetration tester, as well as holding a MS-500 Security Administrator Associate certification and an AZ-500 certification in Microsoft Azure Security Technologies. Jeroen's expertise in security engineering, cloud security, and incident management has enabled him to build a significant body of knowledge in these areas. He is passionate about improving security through innovation and automation and is always looking for ways to stay ahead of the curve. Whether he's advising clients on best practices for cybersecurity or teaching others about the latest trends and

techniques, Jeroen is a highly respected figure in the industry. He brings a wealth of experience and knowledge to every project he works on, and is a valued member of the NVISO team

Bio:

Nick Foulon

I like to play around with electronics & cyber stuff!

17:30 - Day 1 - Track 1

Exploiting Bluetooth - from your car to the bank account$$

yso

Abstract:

Over the past decade, infotainment systems experienced a growth in functionality, broader adoption and central incorporation into the vehicle architecture. Due to the ever-growing role of wireless protocols such as Bluetooth and a known lack of patches alongside the difficulty of patch installation, this poses a new attack surface and a genuine threat to the users. At the same time, the tools and methodologies required for testing are scattered across the Internet, absent and need a rigorous setup. In this talk, we share a comprehensive framework BlueToolkit to test and replay Bluetooth Classic vulnerabilities. We provide practical information and tips. Additionally, we release new exploits and a privilege escalation attack vector. We show how we used the toolkit to find 64 new vulnerabilities in 22 modern cars and the Garmin Flight Stream flight management system used in several aircraft types. Our work equips Bluetooth hackers with necessary information on novel implementation-specific vulnerabilities that could be used to steal information from target cars, establish MitM position or escalate privileges to hijack victims' accounts stealthily. We believe our research will be beneficial in finding new vulnerabilities and making Bluetooth research more accessible and reproducible.

Bio:

yso (also known as schwytz and en_de_ru_cn) is a bug bounty hunter who also holds an MSc degree in Computer Science from ETH Zurich and EPF Lausanne. He is one of the top hackers in live hacking events organized by Meta, Intel, Louis Vuitton, Intigriti and YesWeHack, as well as numerous public and private programs. His interests include finding critical vulnerabilities, red teaming, bug bounty hunting, and proactively securing systems. Twitter - @0a_yso

17:30 - Day 1 - Track 2

Eyes Wide Open: Mastering the Art of Supply Chain Attacks with Client-Side Monitoring

Juerg Fischer (Splunk) + Dai Littlewood (Splunk)

Abstract:

We often say in the cyber security world, you can't detect what you can't see. In the SOC, visibility is everything, and the days of relying solely on the network perimeter and server-side monitoring is no longer enough. Today, breaches are plenty and with it comes reputational damage and hefty fines. So as defenders, what can we do? Dive deep into the cyber battlefield where attackers, armed with cunning and creativity, launch indirect web skimming attacks through your digital supply chain. This high-stakes game often involves the exploitation of third-party javascript — the unsung heroes that power everything from your slick payment gateways to those addictive social media widgets and chic web fonts. Whilst your users are loving these new features, you've opened up yet another gap in visibility and posed a formidable challenge to SOC teams tasked with the herculean task of monitoring and neutralizing code modifications that could lead to disastrous data exfiltration. But we defenders can also get creative...walk with us in to the client side as we sift through a data set which likely already exists in your environment but you just don't know it...yet. This is not your monitoring 101 class, and we're not going to sit here and tell you about HTTP response codes. We're talking about the offensive side and defense; we're talking about strategies to spot exfiltration attempts through third-party code, turning your blindness into visibility and assurance. What's on the Agenda? Decrypting the code behind web skimming breaches via third-party integrations. Unveiling the tactics of attackers and their modus operandi in exploiting third-party code. Effective methods for collecting telemetry of third parties, including where and how to source it Analytical approaches to detect anomalies and correlate data Join the cyber guardians and elevate your security game to legendary status.

DAY 2 – 7. JUNE 2024

10:00 - Day 2 - Track 1

The CTF to Career Pipeline

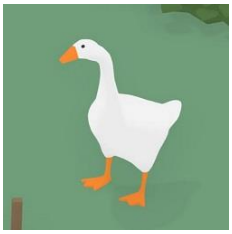
Jam (Vie) Polintan (Google)

Abstract:

CTFs are a fantastic way to learn about and develop one's skills into cybersecurity. They're accessible, open-source most of the time, and consistently offer top-tier challenges to improve your hacking acumen. But are they realistic? When someone wants to make the jump into their cybersecurity career, they'll often find themselves asking the same questions and wondering as to the answer. Jam (Vie) Polintan discusses her experiences and outlines some common techniques and methods that she learned from CTFs which prove to be effective in her starting and maintaining her career.

Bio:

Jam (Vie) Polintan is a security engineer at Google's Red Team and two-time DEF CON CTF winner.



10:00 - Day 2 - Track 2

Cloud-native software supply chain security: the hard truth

Daniel Drack

Abstract:

Everybody is talking about SBOM, attestation, MFA, signatures and other security measures - but who is actually implementing them?

This session will provide you with a technical overview of current cloud-native software supply chain security best-practices. Plus it will give you an idea of the adoption of said best-practices in the industry.

10:50 - Day 2 - Track 1

Shells at Midnight: Turning a Spam Filter Against Itself

Michael Imfeld (modzero)

Abstract:

The RFCs for email addresses are surprisingly flexible in regards to what is considered a valid address - a fact that is most often overlooked by developers. In this talk, we will show that attackers can abuse assumptions of what developers consider safe input and how this can be exploited. Using a real-world example, we will disclose multiple vulnerabilities which we identified in a mail spam filter appliance used by governments, universities and healthcare institutions.

Bio:

Michael's professional journey began in full stack development, leading him through roles in DevOps and system engineering before discovering his passion for cybersecurity. Currently Michael is working as a security analyst at modzero.

10:50 - Day 2 - Track 2

Balancing Efficiency and Security - Unveiling the Risks in Cloud-Based Endpoint Management

Oleksandr Kazymyrov

Abstract:

As organizations shift to cloud environments, they increasingly rely on tools like Microsoft Intune for efficient endpoint management. This transition from traditional to cloud-based infrastructures introduces a complex array of risks, including possible misconfigurations and new vulnerabilities.

This presentation encapsulates our comprehensive examination of transitioning to a modern cloud platform. Our research reveals that configurations aimed at enhancing efficiency can, paradoxically, turn into vulnerabilities, allowing adversaries to exploit and compromise the integrity of endpoints, despite being originally designed to streamline IT operations. We will discuss in detail methods for privilege escalation, addressing both the enrollment and device usage phases. Through real-world examples, we plan to demonstrate the process of creating a backdoor, exemplified by the creation of a user account with administrative privileges. The backdoors not only bypasses device security controls, but also allow you to bypass the “known device” checks in Entra ID conditional access policies. Such vulnerabilities are particularly concerning in scenarios where internal threats collaborate with external actors, significantly increasing risk. The technical findings are translated into business risks, highlighting the critical need for a balance between endpoint security and operational usability.

Attendees will acquire important knowledge about the nuances of cloud security for endpoints, the importance of vigilant configuration management, and strategies for securing against both internal and external threats in a cloud-centric world.

Bio:

Oleksandr is a seasoned cybersecurity professional driven by a fervor for offensive security. With a track record of leading impactful engagements spanning diverse industries, he excels in assisting clients in pinpointing and remedying critical security vulnerabilities within their systems and infrastructure. As the Offensive Security Manager at Storebrand, Oleksandr has played a pivotal role in cultivating and overseeing a robust red team program. This initiative has significantly contributed to enhancing Storebrand's security posture and providing a comprehensive understanding of its risks and vulnerabilities. Combining his background in software engineering with a profound knowledge of offensive tactics, Oleksandr is uniquely positioned to guide organizations in adopting contemporary and efficient defensive/offensive security practices.

11:40 - Day 2 - Track 1

Defeating behavior detection of remote code injection abusing shared sections and handle inheritance

Rafael Salema Marques / SWaNk

Abstract:

The injection of arbitrary code in a remote process is a well-know technique exploited by malwares. As defenders continue to intensify their efforts to uncover these actions, attackers must come up with new techniques and attack variations to evade detection. In this talk, I will present a novel approach to remote code injection that utilizes shared sections and handle inheritance between generations of processes to defeat behavior detection techniques. Additionally, I will be providing a detailed explanation and a proof of concept (PoC).

Bio:

Rafael Salema Marques (SWaNk) is an old-school VX who tends to define himself as a malware enthusiast. He has been coding malware since early 2000. Today is leading a small and cool Red Team. He also conducts lectures, campaigns, and training on malware development, analysis, and reverse engineering. His MSc research focused on employing an artificial immune system approach to detect rootkit activities, while his PhD research introduced a novel method for detecting pivot attacks. SWaNk's main skills are related to offensive security, creating new malwares techniques to bypass defense solutions and penetrate the audited networks. Always available for coffee, beer, and malware projects. Peace.

11:40 - Day 2 - Track 2

Public Cloud public attacks: A summary of attacks seen by CloudIntel

Himanshu Anand

Abstract:

In an era where cloud computing is ubiquitous, the security of cloud environments has never been more critical. Our presentation delves into the intricate landscape of cloud security through an exhaustive analysis of data from CloudIntel, a comprehensive dataset of cloud-based attacks. This dataset, accessible at https://github.com/unknownhad/CloudIntel, offers a unique window into the types of attacks targeting public cloud platforms, the malware employed, and the tactics, techniques, and procedures (TTPs) used by adversaries. By dissecting incidents across various public clouds, we reveal the nuanced differences in attack methodologies, initial foothold, and exploitation tactics. Our research not only sheds light on the current threats but also paves the way for enhanced defense mechanisms against cloud-based vulnerabilities.

Bio:

Over 12 years of Cybersecurity research experience. Talk to me about CTF, product and exploits. Play CTF with WaterPaddlers.

14:00 - Day 2 - Track 1

Phishing the Phishing Resistant - Phishing for Primary Refresh Tokens in Microsoft Entra

Dirk-Jan Mollema (Outsider Security)

Abstract:

Microsoft Entra ID (formerly Azure AD) offers many options to harden your tenant against attackers. Most of these options are enforced using Conditional Access policies, which for example allow you to

restrict users to authenticate with only phishing resistant MFA methods such as Yubikeys and Windows Hello for Business. These MFA methods are resistant against common attacks, such as attacker-in-the-middle attacks via fake login pages, because they will only authenticate against the real Microsoft websites. There is however a catch: the provisioning of such MFA methods is often done from scenarios where such strong authentication cannot be enforced, such as during the device setup. In this talk we will see that by phishing for regular refresh tokens, using some tricks that Microsoft uses during the Windows installation, we can actually obtain a Primary Refresh Token and even provision these Phishing Resistant authentication methods by ourselves. The talk will also cover new mitigations that Microsoft introduced to combat these attacks, and what you can do to protect your tenant.

Bio:

Dirk-jan Mollema is a hacker and researcher of Active Directory and Microsoft Entra (Azure AD) security. In 2022 he started his own company, Outsider Security, where he performs penetration tests and reviews of enterprise networks and cloud environments. He blogs at dirkjanm.io, where he publishes his research, and shares updates on the many open source security tools he has written over the years. He presented previously at TROOPERS, DEF CON, Black Hat and BlueHat and has been awarded as one of Microsoft's Most Valuable Researchers multiple times.

14:00 - Day 2 - Track 2

Actionable Incident Response Documentation - When The Ink Meets The Road

Gergana Karadzhova-Dangela (Cisco Talos)

Abstract:

This presentation will be a bold attempt to highlight the primordial importance of actionable incident response documentation for the overall response readiness of an organization. The audience will be challenged to think critically about their attitudes towards the creation of procedures and documentation, which are often associated with compliance audit checkboxes, and gain a new perspective on the value generated by documents such as an incident response plan and a ransomware playbook.

During this talk Gergana Karadzhova-Dangela, a Senior Incident Response Consultant with Cisco Talos IR, will share commonly observed mistakes when writing IR documentation and ways to avoid them. She will draw on her experiences as a responder who works with customers both during the proactive activities but also during actual cybersecurity breaches.

Bio:

I'm an Incident Response Consultant at Cisco Talos, based in Switzerland, with a focus on helping customers during a cybersecurity incident. I am part of a global, 24x7 team of responders and threat intelligence analysts who provide technical analysis and coordination support to retainer customers during an active security breach. Additionally, I work with Talos customers to improve their security posture through planned services, such as tabletop exercises, compromise assessments and the development of IR process documentation. My background is in digital forensics and data analytics.

14:50 - Day 2 - Track 1

Technical Deep Dive into the XZ backdoor

Timo Schmid (Google)

Abstract:

In March 2024 a backdoor was discovered in xz-utils packages of Debian and Fedora, originating from the upstream XZ project. This talk will take a deeper look into the techniques used by the backdoor to infect its primary target sshd and the different evasion techniques employed in an attempt to hide itself and why these ultimately led to the backdoors discovery.

Bio:

Timo Schmid is a Security Engineer at Google, performing red team operations and research, always looking for novel ways of evading defenders and preventing malicious actors from doing the same. Before working as a red teamer, Timo worked as penetration tester and researcher and worked as a trainer for web application and infrastructure pentesting and secure coding. As such, Timo was a recurring speaker at the TROOPERS conference.

14:50 - Day 2 - Track 2

Digital Self Defense for Investigative Journalists

Rico (SRF)

In today's digital age, investigative journalists face unprecedented threats to their work and their sources. As an IT Security Engineer working for the public Swiss radio and television (SRF) I’m working on privacy solutions and secure communication methods with potential sources. I'll share practical strategies for journalists to navigate the digital realm securely.

Topics include digital surveillance in Switzerland, threat modeling, secure communication tools, data protection, source anonymity, digital footprint management, and legal/ethical considerations. Join me to empower journalists to safeguard their work and uphold freedom of press.

Bio:

Rico Walde is a young Cyber Security Engineer based in Zurich, Switzerland who worked for media companies like Bertelsmann and Cyber Security Consulting firms like Orange Cyberdefense. He finished his Master in 2021 in IT-Security and Forensics and is consulting different companies in the area of Threat Intelligence and blue teaming in general. He is currently working for the public Swiss radio and television (SRF) and creating solutions for (investigative) journalists. He is author of the in 2018 published book "WLAN Hacking".

16:10 - Day 2 - Track 1

Machine Learning for Enhanced Malware Detection & Classification

Solomon Sonya

Malware continues to increase in prevalence and sophistication. VirusTotal reported a daily submission of 2M+ malware samples. Of those 2 million malware daily submissions, over 1 million were unique malware samples. Successfully exploiting networks and systems has become a highly profitable operation for malicious threat actors. Traditional detection mechanisms including antivirus software fail to adequately detect new and varied malware. Artificial Intelligence provides advanced capabilities that can enhance cybersecurity. The purpose of this talk is to deliver a new framework that uses Machine Learning models to analyze malware, produce uniform datasets for additional analysis, and classify malicious samples into malware families. Additionally, this research presents a new Ensemble Classification Facility we developed that leverages several Machine Learning models to enhance malware classification. To our knowledge, this is the first research that utilizes Machine Learning to provide enhanced classification of an entire 200+ gigabyte-malware family corpus consisting of 80K+ unique malware samples and 70+ unique malware families. New, labeled datasets are released to aid in future classification of malware. It is time we leverage the capabilities of Artificial Intelligence and Machine Learning to enhance detection and classification of malware. This talk provides a pathway to incorporate Artificial Intelligence into the automated malware analysis domain.

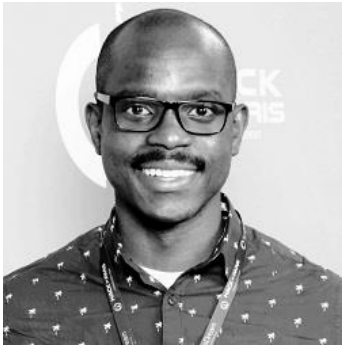
Bio:

Solomon Sonya (@0xSolomonSonya) is a Computer Science Graduate Student at Purdue University. He earned his undergraduate degree in Computer Science and Master's Degrees in Computer Science, Information Systems Engineering, and Operational Art and Strategy. Solomon routinely develops new cybersecurity tools and presents his research, leads workshops, and delivers keynote addresses at cyber security conferences around the world.

Prior to attending Purdue, Solomon was the Director of Cyber Operations Training . Prior to that position, Solomon was a Distinguished Computer Science Instructor at the United States Air Force

Academy, Research Scholar at the University of Southern California, Los Angeles, and an Adjunct Faculty Instructor with the Advanced Course in Engineering Cyberspace Security (ACE) at the Air Force Research Lab in Rome, NY.

Solomon's previous keynote and conference engagements include: DEFCON and BlackHat USA in Las Vegas, NV, SecTor Canada, Hack in Paris and LeHack, France, HackCon Norway, ICSIS – Toronto, ICORES Italy, BruCon Belgium, CyberCentral – Prague and Slovakia, Hack.Lu Luxembourg, Shmoocon DC, BotConf - France, CyberSecuritySummit Texas, SANS Digital Forensics Summit, DerbyCon Kentucky, SkyDogCon Tennessee, HackerHalted Georgia, Day-Con Ohio, TakeDownCon Connecticut, Maryland, and Alabama, and AFCEA – Colorado Springs and Indianapolis.



16:10 - Day 2 - Track 2

Red Cell - Mimicking Threat Actors for Realistic Responses

Thomas Chopitea (Google)

Abstract:

Many organisations make use of offensive security exercises to test their security posture - including Google. As part of testing of Google's Detection and Response capability, engineers undertake a variation of this testing, mimicking the behavior and techniques of real-world, highly sophisticated adversaries. This talk discusses Google's approach to these exercises, why they're important, and how other organisations can benefit from this approach.

Bio:

Thomas has been a DFIR practitioner for 10+ years. He's currently a Security Engineer in the DFIR team at Google who loves running towards the proverbial cyber fires. He enjoys detective work and poking malware with a long stick, and has given talks about DFIR, malware analysis, and threat intelligence at many conferences throughout Europe and the US.