Speaker	Title	Bio	Abstract
@LimitedResults	**Pwning IoT Lightbulbs**	Offensive side, hardware hacker. Not a big talker/writer.More hack to come…always @limitedResults www.limitedresults.com	This talk will present a security investigation of popular IoT devices, such as Wi-FI lightbulbs. It will introduce to the audience how to pwn these devices using low-cost hardware tools and techniques.After a general overview of IoT security context, It will explain what is a smart light bulb, why it is interesting to look into it and why people should think twice when they install these (sneaky) devices at home. Vulnerabilities of different manufacturers such as Xiaomi, Lifx, Wiz…will be reported. Some of them are still not fixed. Enjoy! Keywords: IoT security, hardware hacking, reverse
William Baggett	**Applied Social Engineering to assist domestic abuse victims escaping from hostile conditions**		I provide pro bono work to US Doctors & Therapists to eliminate technical surveillance of abuse victims after they escape. I can discuss searching for wired/wireless cameras in a house, the use of honeypot style emails to ascertain technical surveillance, and using social media to identify
William Baggett	**U.S. Voting Machine vulnerabilities and flaws**		I work with Hacking Democracy to highlight current U.S. voting machine weaknesses and flaws. I have imaged and analyzed almost 40 machines and have found universal weaknesses.
William Baggett	**Modern Identity Theft**		I present this module to NATO SOF and demonstrate how identify theft has shifted from physical identity to a virtual identity and what data is leaked unwittingly. I will also present this module to NATO in Estonia in Fall 2019.
William Baggett	**Broken Arrow**		An infosec practitioner/former intel officer found themselves in an abusive relationship after a long trip overseas and how they used their skillset to escape from the abuse. (covers TechCounterSurveillance, routers, social media, iOS & Mac Forensics and legal theory.
Philipp Krenn	**Scale Your Auditing Events**	Philipp lives to demo interesting technology. Having worked as a web, infrastructure, and database engineer for over ten years, Philipp is now working as a developer advocate at Elastic — the company behind the open source Elastic Stack consisting of Elasticsearch, Kibana, Beats, and Logstash.	The Linux Audit daemon is responsible for writing audit records to the disk, which you can then access with ausearch and aureport. However, it turned out that parsing and centralizing these records is not as easy as you would hope. Elastic's new Auditbeat fixes this by keeping the original configuration, but ships them to a centralized location where you can easily visualize all events. You can also use Auditbeat to detect changes to critical files, like binaries and configuration files, and identify potential security policy violations. This talk shows you what can you do to discover changes, events, and potential security breaches as soon as possible on interactive dashboards. Additionally, we are combining Auditd events with logs, which are security relevant
Philipp Krenn	**NoSQL Means No Security?**		New systems are always interesting targets since their security model couldn't mature yet. NoSQL databases are no exception and had some bad press about their security, but how does their protection actually look like? We will take a look at three widely used systems and their unique approaches: * MongoDB: Widely criticized for publicly accessible databases and a common victim of ransomware. Actually, it provides an elaborate authentication and authorization system, which we will cover from a historic perspective and put an emphasis on the current state. * Redis: Security through obscurity or how you can rename commands. And it features a unique tradeoff for binding to publicly accessible interfaces. * Elasticsearch: Groovy scripting has been a constant headache, but the new, custom-built scripting language Painless tries to take the pain away literally.
Christopher Bleckmann-Dreher	**How does ASCII and Unicode affect our Security**		A short overview about how ASCII evolved to Unicode. Afterwards some insights about how Unicode and their different encodings UTF8,16 and 32. Then comes the interesting part for bounty hunters about how to break applications that are not aware of Unicode. Problems include Javascript, MySQL, Filter-Bypasses and also some real world bounty stories about how guys used that to break stuff.

Miriam Wiesner	**What the log?! So many events, so little time…**	Miriam Wiesner works as a Sr. PFE at Microsoft with a focus on Secure Infrastructure, Windows Event Logs, Active Directory Security, Just Enough Administration & PowerShell and many more. In her spare time, she enjoys writing articles for her private blog also as developing tools to help the community and speaks on international conferences and events. She's a life-long learner, always excited about new technologies and empowering others.	Detecting adversaries is not always easy. Especially when it comes to correlating Windows Event Logs to real-world attack patterns and techniques. Join me to find out how to match Windows Event Log IDs with the MITRE ATT&CK framework and methods to simplify the detection in your environment. After this session I will release a tool, that will revolutionize event log based detection: Import either MSFT Baselines or custom GPOs Find out immediately which Events are being generated and what MITRE ATT&CK techniques are being covered by the selected Baseline/GPO Choose MITRE ATT&CK techniques and generate GPOs to generate the events needed for detection Generate Agent Forwarder Configs to only cover the events needed for the detection (avoid being "Log spammed") Generate Queries to detect the chosen MITRE ATT&CK techniques, regardless of the SIEM solution used
Miriam Wiesner	**JEA.complexity = $false** **Simplifying the deployment for Just Enough Administration**		When implementing JEA, it takes a lot of effort to audit and restrict your service accounts and administrators in your environment. Do not let this be a showstopper for deploying JEA! See how you can efficiently build the JEA modules you need. What once took weeks can now be done in seconds!
Julian Totzek-Hallhuber	**Wie rechtfertigen Sie die Kosten eines AppSec-Programms?**	Julian Totzek-Hallhuber ist Solution Architect beim Spezialisten für Anwendungssicherheit Veracode und bringt mehr als 15 Jahre Erfahrung im IT-Sicherheitsumfeld mit. In seinen verschiedenen Funktionen war er für die Anwendungsentwicklung, für Penetrationstests sowie für die Sicherheit von Webanwendungen zuständig. Zudem ist er Autor zahlreicher Artikel, ist regelmäßig als Sprecher auf Messen anzutreffen und hat bei Projekten von www.webappsec.org (wie zum Beispiel WAFEC) mitgewirkt	Application Security bedeutet immer einen weiteren Schritt in die Kette einzubauen. Eine weitere Aufgabe kostet erneut Zeit und Security sehr oft sogar recht viel. Wie muss ich Application-Security-Testing in meinen Prozess einbauen damit ich so wenig Zeit wie möglich verlieren und sehr wahrscheinlich sogar Geld einsparen kann. Grundlegend, wie kann ich einen positiven ROI erreichen wenn ich Application-Security-Testing in meinen Prozess einbinde.
Luc Gommans	**Your Stack Traces are Leaking CVEs**	Luc Gommans is an IT Security consultant at X41 D-Sec. Throughout his studies, his projects involved breaking as well as building stuff: Targeted GPS Spoofing, Practical Passphrase Cracking, and a security-oriented Educational Escape Experience. For the latter, his team won the ICTalent Award 2016. He graduated from the master's System & Network Engineering in Amsterdam in the summer of 2018.	Stack traces provide detailed information about an application's internals: which language the application is written in, which libraries were called, and what kind of error is being triggered. What if you could also see the versions of each library? The version numbers are not shown in the trace, but they can be extracted through fingerprinting. We developed such a fingerprinting tool and hooked it up to a CVE database to find which vulnerabilities are present in the identified versions. This presentation will explain how it works under the hood and how you can use it in your own pentests.

Dirk Leopold	**“Security by Design” in the Automotive Development Process**		Security is becoming more and more important – especially for connected, (semi-)autonomous vehicles.Already during the design phase of the automotive development process, security needs to be taken into consideration.But how to achieve “security by design” in the automotive domain?We will look at the following aspects:What are the fundamental differences between the safety and security in the development and lifecycle process? What are the external parameters influencing the security design process (e.g. norms, external and internal requirements)?What are the security relevant aspects of the solution that need to be taken into consideration when designing the system (e.g. functions, components, connections and data)?How to systematically identify assets, potential attacks and controls to mitigate attacks?Why it is important to perform the security design in an iterative process and how requirements, functional design and system design influence one another.How to achieve traceability of security design aspect across the entire development process? In the presentation will look at methods and tools that allow a model based security risk analysis approach as an essential part of security by design. This can be applied during the requirements and design phase for all vehicle components and software.Based on the defined functions, components and data, security related damages, threats and controls can be modeled and evaluated.In a scenario based, iterative approach, suitable controls can be chosen for the subsequent implementation and test process.In the presentation we share best practice approaches based on our experience from past 3 years of
Fabio Leite	**Automotive Ethernet Security 101 - what you need to know**		Security in modern vehicles became a critical concern for OEMs, car manufacturers, and suppliers due to the digitalization of the control units, which are responsible to rapidly and reliably control and assist the driver in multiple tasks, such as providing stability when driving in a German Autobahn or solely breaking the vehicle under any critical conditions. Historically, safety and efficiency were the main concerns with regards to embedded software quality, for obvious reasons. Today, with new technologies, speeds, services & applications running in a car, new attack surfaces have been introduced in modern vehicles, not surprising, as well as new requirements such as dependability. Automotive Ethernet, is the perfect example. Different protocols and physical layers have been standardized under the IEEE association, providing a strong set of rules and requirements for its usage as an In-Vehicle-Networking (IVN), where a single link is able to transmit data at rates of thousands of times faster than a “classic” CAN bus. Critical factors like the lack of determinism and the switched topology require new and complex protocol stacks to be designed and integrated as part of the Electric/Electronic Architecture of a modern car, due to the stringent nature of the automotive requirements. Each of these new elements brings a taste of new vulnerabilities and new attack surfaces for the system. This talk will discuss all the security aspects of Automotive Ethernet networks when integrated to the E/E Architecture, possible attack surfaces of the protocol stacks and a security overview of automotive switches. Additionally, an overview of the possible mitigations and security mechanisms to prevent

Eric Sesterhenn	**Context Switching your Kernel Fuzzing**	Eric Sesterhenn is working as an IT Security consultant for more than 15 years, working mostly in the areas of source code auditing and penetration testing. He has identified vulnerabilities in various software projects including the Linux kernel, X.org and multiple IoT Operating Systems. In 2018 he has been a Speaker at nullcon, warcon and defcon	Fehler im Kern des Betriebssystem gewinnen immer mehr an Bedeutung, da sie den Ausbruch aus Sandboxen erlauben können. Fuzzing ist eine Methode um diese Fehler zu erkennen, stösst beim Betriebssystemkernel jedoch an Grenzen. Wird der laufende Kernel getestet, stoppt ein kritischer Bug unter Umständen den kompletten Prozess. Wird der Kernel im Emulator getestet leidet die Performance. Dieser Talk zeigt Ansätze auf, die es erlauben Kernel Code im Userspace zu fuzzen.
Philipp Schmied	**An Introduction to Car Hacking: Analyzing proprietary automotive systems with CANalyzat0r**	IT Security Consultant at SCHUTZWERK GmbH. A big part of my free time is dedicated to computer science and information security. This year, I’ve graduated at Aalen University with a Master of Science degree in IT security.	While car manufacturers steadily refine and advance vehicle systems, requirements of the underlying networks increase even further. Striving for smart cars, a fast-growing amount of components are interconnected within a single car. This results in specialized and often proprietary car protocols built based on standardized technology. Most of these protocols are based on bus protocols: All network nodes within such a bus network are connected using a single shared data link. This technology provides a feasible way of real time communication between several security, safety and comfort systems. However, often no or insufficient authentication and encryption or other security mechanisms are implemented in today’s car systems. As described previously, most of the interchanged data structures on a car network bus, including associated systems, are proprietary. This includes both software and hardware. Without a comprehensive information base, performing holistic audits and reverse engineering can be complex. On top of that, there’s a need for open source, extensible, easy to use and publicly available software to analyze the security state of such networks andprotocols. The proposed talk tries to provide an information base for software and hardware to get started in the field of car hacking. Also, results of analyses, experiences from the bug bounty event and the released
Juliane Pirnat	**GRC - Nerd, Nerd - GRC**	Juliane Pirnat ist Beraterin für Informationssicherheit in Finanzinstituten. Nach ihrer mehrjährigen Tätigkeit bei Banken im Bereich der Verhinderung von Geldwäsche und sonstigen strafbaren Handlungen beschäftigt sie sich daher mit Themen rund um Governance, Compliance und Risk.	In Projekten rund um IT-Governance, -Compliance und -Risk treffen Fachbereich und IT aufeinander. Oft ist auch die eine oder andere Seite externe/r Berater*in. In der Jahresabschlussprüfung sitzen Wirtschaftsprüfer auf der anderen Seite des Tisches. Das Thema die Vortrags ist das fachliche Verständnis zwischen "Business Menschen" und "Nerds", mit dem Schwerpunkt worauf "Business Menschen" achten, damit "Nerds" besser damit umgehen können.
David Szili & Eva Szilagyi	**Elastic Stack for Security Monitoring in a Nutshell**	Eva Szilagyi is managing partner and CEO of Alzette Information Security, a consulting company based in Luxembourg. She has more than eight years of professional experience in penetration testing, security source code review, vulnerability management, digital forensics, IT auditing, telecommunication networks, and security research	

David Szili	**Introduction to OSQuery**	David Szili is managing partner and CTO of Alzette Information Security, a consulting company based in Luxembourg. David is also an instructor at SANS Institute, teaching FOR572: Advanced Network Forensics. He has more than eight years of professional experience in penetration testing, red teaming, vulnerability assessment, vulnerability management, security monitoring, security architecture design, incident response, digital forensics and software development.	Maintaining real-time insight into the current state of your endpoint infrastructure is crucial. It is very important from operational, continuous security monitoring, and incident response perspective. Created by Facebook in 2014, osquery is an open-source instrumentation framework for Windows, OS X (macOS), Linux, and FreeBSD operating systems. Osquery exposes the operating system as a relational database and allows you to write SQL queries to explore system data. The generic SQL tables represent running processes, loaded kernel modules, open network connections, browser plugins, hardware events, file hashes, etc. These SQL tables are implemented via an easy to extend API and several tables already exist and more are being written. The main advantage of osquery is that it allows you to use one platform for monitoring complex operating system state across an entire infrastructure. It has a high-performance and low-footprint distributed host monitoring daemon, osquery and also an interactive query console, called osqueryi. During this two-hour workshop, we will learn about osquery’s capabilities and cover the following topics: - Osquery basics (installation, osqueryi, osqueryd, osquery schema); - SQL refresher (SELECT, FROM, WHERE, LIKE, JOIN, etc.); - Osquery configuration (flagfile, packs, schedule, logging, file integrity monitoring, etc.); - Fleet management (Kolide Fleet, Doorman, SGT, etc.); - Osquery extensions. Technical requirements for the workshop: - A laptop with at least 8 GB of RAM and 30-50 GB of free disk space; - VMware Workstation, VMware Fusion or VMware Player installed.
Jörg Simon	**OpSec+++ the FastTrack**	Joerg works in Security at audius, is the creator of the Fedora Security Lab and an ISECOM Team Member since 2009.	A talk how to make sense out of your technical findings and how to translate them into unbiased results and metrics. The OSSTMM, maintained by the non profit ISECOM is breaking the common paradigms around operational security and is considered unpractical by the uninitiated. This talk gets you started using the OSSTMM as a helping hand for your future Security Tests.
Tobias Györfi	**Robustness of malware sandboxes against evasive behavior**	IT-Security Consultant	Sandbox-based application behavior analysis and reputation assignment steadily supplements traditional antivirus software. As malware development never rests, malware becomes increasingly capable of behavior analysis evasion by detecting sandbox presence. This talk presents a manifold testing methodology to detect and evade malware sandboxing and compares the test results of five publicly available malware sandbox products.
Thomas Daniel Wagner	**Cyber Threat Intelligence for Enterprise IT and Products**		Cyber Threat Intelligence (CTI) has gained the interest of Cyber Security practitioners to be more proactive instead of only reactive in form of CTI consumption. Cyber threats are increasing due to their profitable nature and sometimes simple execution. This talk will provide the audience with information about Cyber Threat Intelligence (CTI). Especially how to use it in an Enterprise and product environment. Furthermore, the talk will touch various areas that must be considered in CTI consumption and sharing such as Threat Intelligence Platforms (TIPs), Regulations and human behavior.

Stefan Hager	**Weaponizing Layer 8**	Stefan works for the Internet Security Team at German company DATEV eG. Having started with computers and starting to be puzzled by reality in the 80s, he started out as a programmer in the early 90s. Since 2000 he has been securing networks and computers for various enterprises in Germany and Scotland. His main focus nowadays is security research, raising security awareness, coming up with creative solutions to security problems and discussing new ideas concerning threat mitigation. When not trying to do any of the stuff mentioned above, he is either travelling, procrastinating or trying to beat some hacking challenge. Stefan also writes blog posts (in English and German) on his site	Do you think users are the weakest link in the security chain? Here is some duct tape to change that, and to raise the bar for social engineers and other attackers alike. Over the last few decades, sysadmins and people working in IT have called users names and generally rolled their eyes at the antics of those allegedly lazy, stupid and uneducated people. From PEBKAC to ID-Ten-T we have been calling them names and didn’t want them on our networks. This way of destructive thinking needs an overhaul, and here are some easy tricks how users can become the valuable asset in corporate security that indeed they should be. Finding creative solutions to existing problems has been a standard skill for red teamers, whereas those defending networks often rely on standards. Discover some creative solutions people have come up with to significantly raise their security - most of them are easy to implement - and how users can become a major asset of any security team.