Tuesday, May 10th, 1:15pm Sessions

Purple Haze: Turning Network Defenders into Network attackers	Chris Hernandez | Laura Farvour	The modern enterprise environment is (hopefully) stacked heavily in favor of network defense. We all know defenders have to be right all of the time and an adversary only has to be right once. Or do they? Join me as I uncover how i turned the tables defending my enterprise environment and turned every enterprise defender at my disposal into an adversary. This talk will be an exploration of how to take the concept of purple teaming and crank it up to 11, with the ultimate goal of making sure that the adversary has to be right 100% of the time and the defender can finally take a well deserved nap.
Advice for IoT Use in a Post-Pandemic World	Brian Halbach	Global Internet of Things (IoT) spending is projected to total $15 trillion dollars between 2019 and 2025. This comes as no surprise as in addition to convenience in an increasingly chaotic world, IoT devices offer a slew of values and benefits to the user. While nearly all retailers agree that the benefits of IoT devices outweigh the risks, the rise in IoT devices and IoT app development means new security challenges that demand attention. IoT devices have become so integral to our daily lives, that it can be difficult to see a smart fridge as posing a security risk. But for cybercriminals, leveraging IoT devices like smart speakers, smart gadgets, smart appliances, smart toys, and smart security to gain access to homes and offices is easier than you might think, and provides the added benefit of a major payload. While a single smart watch can be used as a gateway to access confidential information on other devices on the same network, thousands of smart devices can take down the infrastructure of an entire country. In this session, RedTeam Security will address the risks associated with IoT devices, provide real-world examples of IoT attacks showing just how damaging they can be, and give practical solutions to help balance convenience and security in your own life.
FBI Crime Scene Collection: How to Play with Luminol	Lizabeth Lehrkamp	For approximately 11 years I have presented to (many of) you regarding the FBI's stance on crime and investigation. Well, last year I decided to take on a different kind of job for the FBI, I now run our Evidence Response Team (aka CSI team). We collect forensic evidence on federal crime scenes. Yup, we take blood/DNA samples. We use luminol and we use alternate light sources (it

		illuminates body fluids, you know). How does that apply to cyber/physical security? It doesn't. But it is a pretty cool job and I, for one, am very excited with it. Take a little break from heavy thoughts on security and join me to learn about what I do and why it is so cool.
Adopting a Zero Trust Framework	James Ringold	Moving to a Zero Trust architecture can be difficult. Through this presentation, I will talk about the benefits of adopting a zero trust architecture and how integration with threat prevention/detection technologies is essential to successful defense from modern attacks. Session Key Learning Points: 1) Zero Trust isn't really new, we have been on this journey a long time, just didn't know it. 2) Zero Trust isn't a technology to be implemented, it's a transformation of approach to security. 3) You do not necessarily need to buy new technologies to begin a Zero Trust journey. To be successful, a Zero Trust architecture requires integration with threat prevention and detection technologies. 4) Zero Trust and Secure Access Services Edge are complimentary, not competing capabilities
Sharing Is Caring - How Responsible Public Disclosure Can Help Clients With Third Party Risks	Daniel Sandau	Vulnerability disclosure policies may put vendors on the spot, but how does a pentester use that to protect their clients? This talk will cover the basic setup and drawbacks of a vulnerability disclosure policy, how it can be positive for a client, and a real life example of an unfortunate situation (for the third party).
Bringing Security from the Basement to the Boardroom	Kurt Kapsner	The days of security teams hiding behind keyboards in a basement are over. It is time to polish off those sales skills and talk to the 'customer.' In this session you will be hear about methods to get business buy in for security initiatives, and drive security best practices throughout the business. Learning to speak the language of the business will be key to getting others to follow where you lead.
Risk Mitigation through Cloud Adoption	David Stone	Learn the megatrends in cyber security and how cloud adoption advances the industry, key trends in making the transition successfully and key lessons learned by previous cloud transformations. Finally we will discuss some of the key topics that make the journey truly transformational by implementing key concepts like "Security-as-Code" and how to measure success.

The Importance of Engaging Developers with Software Security, & How to Get Better At It	Nick Saunders	Today, companies' success or failure has never relied more on the security of their software and technology. Security and GRC teams understand that they need collaboration from engineering and development groups to succeed in their initiatives. This session will discuss how to engage developers with security by listening to their pain-points and offering timely, useful resources.

Tuesday, May 10th, 2:45pm Sessions

How to Build and Validate Ransomware Attack Detections	Scott Sutherland	Ransomware is a strategy for adversaries to make money - a strategy that's proven successful. During this presentation, we will cover how ransomware works, ransomware trends to watch, best practices for prevention, and more. At the core of the discussion, Scott will explain how to build detections for common tactics, techniques, and procedures (TTPs) used by ransomware families and how to validate they work, ongoing, as part of the larger security program. Participants will leave this webinar with actionable advice to ensure their organization is more resilient to ever-evolving ransomware attacks.
Zero Trust: A story of growing up	Aaron Wampach	The buzz going around today is the need for Zero Trust. The idea has been around for a while but hasn't caught on. The question is why? This presentation will explore the pitfalls of trying to obtain Zero Trust and why it seems so difficult to implement. It will also explore the theory that Zero Trust is more of a people and process issue and not a technology issue (as some vendors would like you to believe). Organizations need to understand they need to know how to walk before they can run (with Zero Trust).
Defending against Advanced Threats	Tim Crothers	While there are no shortage of breaches, not everyone is failing. Some industries like Defense Industrial Base face significant threats on a constant basis yet still manage to defend themselves well. In this talk we'll discuss techniques the most advanced cyber teams are using and how you can leverage those same approaches in the defense of your organization.
Strengthening Your Program Through Strategic Communications	Kathy Davis	Focus your communication for different stakeholders Find the key communication points in your program process Build communications that are right-sized, strategically focused on the future and efficient.

		Kathy will discuss both examples and the process her company's program developed to communicate strategically.
Data Management to Reduce Risk and Comply With Mandates	Heather Engel	With every framework, it's nearly impossible to apply security controls unless you understand how your data moves. This session will look at identifying and managing information, data categorization, boundary definitions and data flows. Working with real examples from the NIST SP 800-171 framework, ISO, PCI, and FedRAMP, cuick trac™ Director of Strategic Security Heather Engel will help you understand how to manage data to limit the damage from a breach and reduce overall security risk.
The Hand that Rocks the Cradle: Why HR is your Best and Worst Advocate in Workplace Violence Prevention	Carrie Ackerman	The pandemic has created a piling on effect with financial stressors, political stressors, racial tensions, increased substance use/abuse, increase in reports of mental health concerns and domestic violence which has put people on edge more than ever before. This is true across the nation and, unfortunately, this is true with employees. Attend this informative session that will discuss why HR is the "Hand that Rocks the Cradle" at every organization. HR is a necessary partner in combatting workplace violence and can be a great advocate; however, HR also is your worst advocate. Learn about steps you can take to foster and build a strong partnership with HR and Legal so that you all rock the cradle together - otherwise as the song goes: "..and down will come baby, cradle and all..."
A Non-techie Thriving in a Cybersecurity World	Lauren Rudek	I don't code (much) and didn't know what an API was or could tell you what OWASP stood for until this past year, but after 13 years in the non-tech roles at Target I am finding enjoyment, success, and energy in a fulfilling Cybersecurity role, doing what I love: training & awareness, helping team members succeed, and learning every day. Learn from a Lead Cybersecurity Analyst about how a mindset of continuous learning and inward reflection can help you navigate your career journey, determine direction when you hit a fork in the road, and proactively find the next pit stop in your collection of fulfilling experiences.

The Data-First Approach; Managing the Tension between Security and Productivity	Brian Vecci	Businesses have grown increasingly data driven and data dependent. Attackers that would steal or hijack data are highly motivated and grow more sophisticated, yet data remains overly accessible and under watched.
2022 Threat Landscape, An Overview and Strategic Considerations based on Real Attacks	Duke McDonald	This briefing will cover CrowdStrike's latest and most relevant intelligence trends pertaining to nation-state and criminal threat actor groups with a focus on how these groups have changed their tactics, techniques, and procedures (TTPs) accounting for modern day security controls. Leveraging insights derived from CrowdStrike's unrivaled intrusion telemetry, the briefing will highlight notable adaptations and trends in modern attacks, alongside strategic considerations based on the changes seen in the threat landscape.

Tuesday, May 10th, 4:15pm Sessions

All Speed and No Security	Aakash Shah	Over the last 5 years software delivery has completely transformed. Infrastructure today is designed and delivered as-code in languages such as Terraform, CloudFormation, ARM templates, Kubernetes Manifests and more. Increasingly this ownership of this code is now falling under the umbrella of software development. This code today represents the entire application architecture and enables development teams to deliver infrastructure capabilities in an agile manner where foundational architectural changes are made from release to release. This has enabled development teams to achieve incredible velocity and agility. However, every security design & engineering team that I have worked with has unfortunately struggled to keep up with the velocity and unprecedented rate of change that infrastructure-as-code (IaC) adoption brings. In this talk we will provide a practical guide to how security teams can adapt to IaC. We will outline the typical challenges security teams face when their development team embraces IaC. We will also present the opportunity that this presents to security design & engineering teams. We will discuss how security design & engineering teams can transform their practices to drive improved standardization and adoption of security design patterns to ensure that applications are secure and compliant by design.

Lessons Learned from an Important Vulnerability Disclosure: Kerberos Bronze Bit Attack	Jake Karnes	In late-2020, pentester Jake Karnes found and responsibly disclosed a serious Microsoft vulnerability: The Kerberos Bronze Bit Attack. When exploited, it allows an attacker to bypass security features and escalate privileges within an Active Directory domain. If you attended security conferences over the past year, you may have stumbled upon Jake presenting a deep dive on the inner workings of the vulnerability and its exploit. But now that the dust has settled and the issue has been remediated, he is taking a step back to reflect on the lessons he learned throughout the experience. During this session, Jake looks back to December 2020 to share key insights he learned when finding and disclosing CVE-2020-17049, including: Persistence is vital: Real adversaries are persistent and pentesters should be too. It's vital for pentesters to take weird behaviors and exhaust all angles to ensure it is not a more serious issue. The importance of information sharing and collaboration: If researchers Elad Shamir and Will Schroeder had not published their initial findings, it's likely the vulnerability might still exist today. You don't have to be an expert to uncover impactful findings: Jake started this process simply wanting to learn more about Kerberos protocol... then one thing led to another.
A Data-Driven Story on Vulnerabilities	Benjamin Edwards | Jay Jacobs	“Vulnerability” is an absolutely fundamental concept in computer security. Without these flaws that allow attackers to manipulate software in ways it was never intended, most of what we do in security would be obviated. In this talk, we’ll dig into the data around vulnerabilities and trace patterns we see from their inception as flaws in software development through their exploitation and remediation in enterprise environments. Along the way we’ll examine the current landscape of known vulnerabilities and how they’ve evolved over time. We’ll use advanced machine learning techniques to demonstrate how groups of seemingly unrelated vulnerabilities tend to cluster, and how we can use the same techniques to fill in information gaps in the data. Finally, we’ll leverage our knowledge to better prioritize remediation efforts. We’ll show that you can do much better than just using CVSS to prioritize vulns and that even bumming around on social media might be an improvement over CVSS. Finally, we’ll discuss improvements to the latest version of the Exploit Prediction Scoring System (EPSS, https://www.first.org/epss/) and how to leverage it to make your organization safer.
Disaster Fatigue - It's real! So what will we do about it?	Fred Klaptezky	Disaster fatigue may not be topmost on your mind, but the effects of it are real and you can see it in the people within your company or organization. This session is designed to be interactive. Bring your observed problems and if you have solutions to share - definitely bring those. We'll cover the impact to fatigue on your programs, where auditors should look to get indicators (works for the professionals as well), strategies that have worked, strategies that have not. How one organization has started to redefine the Business Continuity program to be proactive rather than reactive to bring staff back into

		the program. These presentations are best when everyone participates. The target audience is experienced to very experienced professionals, but even entry level practitioners will benefit.
The PCI Dream Team: Solving the biggest PCI DSS nightmares	Art Cooper | Ben Rothke | David Mundhenk | Jeff Hall	Since 2006, PCI DSS compliance has been required for any company that stores, processes or transmits credit card data. But as networks, payments and applications get more complicated, and security threats increasing, so too do the potential PCI solutions. This panel brings some of the smartest and most experienced PCI professionals in the industry to the table. There have seen the best and the worst in the payment industry, and will share the successes to make you effective, and a number of horror stories so you don't lose your job. The panel will detail a number of eloquent solutions to common PCI issues, and answer pesky problems that are plaguing attendees. No good question will be left behind.
One Hop from the Heart - Securing Cardiac Implantable Devices	Kyle Erickson	Medical device security is hard for a reason. This talk will discuss industry collaboration needed to continue to advance implantable device security. In the presentation, I'll show you novel techniques and leading practices in the detection, response, and security testing space that comes together in an operational Product Security Fusion Center. I will also spark discussion and encourage feedback on risk management strategy including threat modeling and practical implementation of constrained system patching with a scalpel and not a machete. We will also demo exploiting an Implantable Cardiac Defibrlater via BTLE. Finally, explore ways that Medical Device Manufacturers, Hospitals, and the general security community can share knowledge coordinate responses.
Managing Stress and Building Resilience using the 7 Levels of Effectiveness	Cindy Edwards	Are you are stressed out or bored with work? Both conditions create the same response: a lack of energy to do anything! Come learn up to date and proven, brain-based, stress management techniques to improve your productivity, find your focus, manage your time, and get back on track towards achieving your goals. Learn and walk through the Seven Levels of Effectiveness self coaching tool in the session and get help managing your stress immediately. Let's do this!

What XDR Is And Isn't	Bryan Flores	Since Nir Zuk, Palo Alto Networks CTO, coined XDR in 2018, XDR has captured and shifted the collective imagination of security teams and analysts alike. It has also led to confusion on what XDR is and isn't. Many see extended detection and response, or XDR, as the key to breaking down data silos, reducing security blind spots and improving SOC efficiency. However, not all users know the use cases for XDR and which vendors are offering true XDR. You will learn: • The top features and benefits of XDR solutions • How organizations are using XDR for security operations today • Tips to identify XDR imposters • How to choose the right XDR product for your environment To help you realize the true benefits of XDR, attend our session!
Fast and Furious Attacks: Using AI to Surgically-Respond	Connor Lind	Fast-moving cyberattacks can strike at any time, and security teams are often unable to react quickly enough. Join to learn how Autonomous Response takes targeted action to stop in-progress attacks without disrupting your business. The discussion includes real-world threat finds. Explore today's threats and challenges and learn how advances in AI have been leveraged to allow for very surgical actions to be taken autonomously - where humans can no longer react fast enough.