Wednesday, May 11th Demo Stage & Session Descriptions

9:15am Demo Stage

Saving Resources With Managed Detection and Response	Tim Otis	In this session we will demonstrate the capabilities of Managed Detection and Response. We will show how teams with limited resources can benefit from outsourcing event monitoring to a team of cyber security experts.

9:45am Breakout Sessions

What Safety Science taught me about Information Risk	John Benninghoff	Two years of study and research has changed how I see risk. Safety science taught me that improving performance is the key to managing risk, and studying successes is the key to risk analysis. The 'New School' of safety argues that you can't have a science of non-events; safety comes through being successful more often, not failing less. Research in DevOps, Software Security, and Security Programs show a strong link between general and security performance. In many (but not all) cases, organizations most effectively reduce cybersecurity risk by improving general performance, not by improving one-dimensional security or reliability performance. This talk presents a new model for security performance that informs how we can maximize the value of our security investments, by focusing on improving existing or creating new organizational capabilities in response to new and emerging threats, where general performance falls short. It will review both the theory that improving performance improves safety, how that relates to cybersecurity risk, evidence from my own and others' research that supports this theory, and how it can be used to analyze and manage risk more effectively.
Recovery Amid Threat Innovation: How the Lasting Impact of COVID-19 Has Altered the Threat Landscape	Christopher Conrad	In the first half of 2021, cybercriminals launched approximately 5.4 million Distributed Denial of Services (DDoS) attacks, increasing 11% over 1H2020 figures. Further, data projections from NETSCOUT expect this long tail of attacker innovation to last, fueling a growing cybersecurity crisis that will continue to impact public and private organizations. The massive shift in the

		way we work and live (i.e. telehealth, remote work, distance learning, etc.) has created a massive opportunity for threat actors to increase attack frequency. As these challenges have emerged and increased, security leaders in every sector - from healthcare to telecommunications to education - have scrambled to simultaneously understand and mitigate threats to their organizations, forcing them to reexamine strategies and best practices. Over two years into the COVID-19 pandemic, we have made great strides - but threat actors are abundant and innovative. Richard Hummel, Threat Intelligence Lead at NETSCOUT, shares how the unique experiences of 2021 shaped the current threat landscape, and how we can use this knowledge to our advantage as we navigate new security challenges in 2022 and beyond.
Easiest Catch: Don't Be Another Fish in the Dark 'Net	Mark Lanterman	You've read the headlines. Unfortunately, the question now is not if your information is going to be accessed or stolen, but when. To inform the attendees of current developments in the digital underground as well as provide realistic advice for cyber protection, Mark Lanterman will be discussing recent high-profile cybercrime events, including website breaches impacting a variety of organizations and sectors. Mark will discuss particularly dangerous types of threats that might affect organizations involving the Dark Web, the Internet of Things, and phishing.
Metrics To Energize the BCP Lifecycle	Kathy Davis	Hear how metrics brought more collaboration and energy in the partnership between the business continuity team and the continuity plan owners and senior leadership. Work through the process the business continuity team used and consider how to adapt the process we used to your business context. Metrics can motivate! This session will show how the C. H. Robinson team developed metrics that brought new energy into their business continuity plan life cycle. Be prepared for interactivity! We'll go through the key questions in the process so that you can adapt the process to your own business context.
GRC Potpourri: Past, Present, Future	Kathy Washenberger	Governance Risk and Compliance (GRC) - something that has been around for quite some time, today is more important than ever, and will most certainly be needed well into the future! This session will allow for a quick review of

		the past and current standardized processes, trends, compliance requirements, etc., more importantly, it will also look to the future so that we as an industry can prepare our programs! While GRC will focus more on the process side of security, there is no doubt much room for maturity as we enter into the next level of cybersecurity, technology growth and protecting our most precious assets!
Understanding Invisible Disabilities in the Workplace	Cindy Edwards	"You don't look disabled." "You look fine." Invisible disabilities are not immediately apparent, "masked" to an observer, and provide unique workplace and career challenges. Invisible disabilities sometimes, or always, limit daily activities, range from mild to severe, and vary from person to person. Because of this, people with invisible disabilities can feel stigmatized because of the health issues they have, however; having an invisible disability does not mean that work cannot be successful. Drawing on research and experience, this course offers a look at the need to raise awareness around invisible disabilities and their impact in the workplace today.
Seize The Breach: Why Breaches Occur & How to Mitigate Them	Jim Chrisos	Breaches happen and 2021 was a record-breaking year for them. According to Identity Theft Resource Center (ITRC) research, there were 1,291 breaches publicly reported in 2021 as of Sept. 2021 compared to 1,108 breaches in 2020; that’s a 17% year-over-year increase. Meanwhile, millions are spent on security operations centers that aren’t stopping the breaches from happening. Join us for a discussion on: • Why SOC and security teams are way too limited by legacy SIEM • How machine learning-driven analytics and automation technologies provide unmatched threat detection, investigation, and response (TDIR) capabilities so security teams can respond more quickly and accurately to seize the breach and mitigate damage. • A simple maturity model based on outcomes and use cases that can vastly improve Security Operations
Learn How to Safeguard the Enterprise	Mark Buvari	Join Skybox Security to learn how to safeguard the enterprise. You'll discover how to mitigate the cost of cyber threats and data breaches before they happen. We'll share how to: - Achieve smarter cybersecurity - Prevent data breaches and lateral movement - Operationalize complex policy management

		efficiently - Maintain continuous compliance while alleviating audit pressure - Expedite reporting compliance with NIST, PCI and ISO 27000

10:50am Demo Stage

What does it mean to have "Good Visibility"?	Steve Goers	In today's modern attack surfaces, "good visibility" is often mentioned as a key success criteria for any security tool. Frequently, EDR is cited as a "solution" to a lack of visibility into an incident or day to day events. If a 'lack' of visibility refers to being blind to something, presumably "good visibility" means more things are seen. So, what should a security analyst actually expect to see from a modern solution? When there is good visibility, what actual data should an analyst to be able to see? Come see what "visibility" the CrowdStrike Falcon sensor enables. Leave wondering the myriad of actionable steps this data can provide to truly transform your organization's security posture.

11:15am Breakout Sessions

Knowing What Risks Matter--And Don't--In Your Open Source	David Lindner	As digital transformation accelerates, software developers face increasing pressure to speed up their work, and open-source software helps them meet aggressive timelines by dropping standardized code into an application. But cyber criminals are targeting more attacks on the software supply chain, exploiting software vulnerabilities that occur in production. As a result, organizations must prioritize protecting the open-source code in their applications. Attend this session to learn about the findings from the telemetry of thousands of real-world applications revealing trends of library usage, vulnerabilities, and best practices. You will learn about surprising findings such as: * Less than 10% of code in the typical application is open-source code actually used by the software. * Legacy software composition analysis (SCA) tools have a false positive rate of up to 69%. * The average library uses a version that is 2.5 years old, increasing risk and promising future headaches. * High-risk licenses are present in 69% of Java applications and 33% of Node applications. In a world of accelerating

		development and frequent exploitation of vulnerabilities, protecting applications containing open-source libraries and frameworks requires a different approach. Organizations need a comprehensive picture of active and inactive libraries and classes, library age, vulnerabilities, and licensing issues. Such observability enables an organization to address the riskiest issues""and not waste time with vulnerabilities that pose no risk.
Into the Abyss: Evaluating Active Directory SMB Shares on Scale	Scott Sutherland	During this presentation, we'll talk about how to identify and triage the large volume of excessive access most standard Active Directory users have to common network shares. Over the course of hundreds of internal network penetration tests and audits one theme has stood out, vulnerability management programs do not adequately identify excessive share privileges. The excessive shares have become a risk for data exposure, ransomware attacks, and privilege escalation within enterprise environments. During this discussion, we will talk about why this gap exists, how to inventory excessive share across an entire Active Directory domain quickly, and how to triage those results to help reduce risk for your organization.
Crypto Crime - Recent Trends in Cryptocurrency and Cyber Crime	Jacob Iverson	Join us for a high-level discussion of the overlap between cryptocurrency and cyber crime from the perspective of the FBI, including an open Q&A about crypto crime or other FBI cyber topics.
Navigating the Ransomware Challenge: Lessons in continuity, crisis, cybersecurity, and leadership	Bryan Strawser	Organizations of all sizes are confronted today by the continuity and reputational challenges inherent in the challenges we face with the ransomware threat. Some of these challenges include coordinating across multiple silos, effective high-availability and disaster recovery strategies, lack of investment in business continuity, the lack of crisis communications capabilities, and an ad-hoc crisis management process. In this presentation, Bryghtpath Principal & Chief Executive Bryan Strawser will share the keys to successful ransomware preparedness and response, including how to cut across silos, enhance your organization's resilience,

		leverage exercises to identify gaps in your planning and preparedness process, and how to lead your organization through the crisis.
Think Like a Jazz Musician	Ty Hollins	You want your GRC Program to feel more like Jazz rather than Classical music. The jazz musician's capability to improvise, take risks, adapt to change, and forge new ground are the exact skills we all need to develop in our current economy of bureaucratic sameness. This session will explore Governance, Risk, and Compliance and its synchronization and interrelation with business objectives.
Contrary to Hollywood belief - information security is more than firewalls (and dark lit rooms)	Aaron Wampach	How many times have you watched a movie or TV show and the catch phrase is "Need to get past the firewall". Teaching an entry level class in cybersecurity I have seen over and over again students thinking installing AV is "Good Enough" for their home network. Many students don't realize when they first start there is more to information security than AV and firewalls. This presentation will lay out some of the different paths students can follow; and the skillsets they need to develop (both in class and out) to be a successful security practitioner.
Ransomware: the New Cold War	Jamison Utter	Over the last 15 years I have worked on the dark web to build relationships and inroads with real ransomware Gangs, tool makers, and and providers. I export this research and a campaign I built from scratch. I will show how easy it is, how attackers do it (or at least some ways) and then show how cyber insurance is impacting this.
Blast Radius & Active Attack Paths: The Keys to Securing Your Cloud with Agility & Speed	Jeff Moncrief	Security teams need a new mindset to keep up with the risks created by modern DevOps practices in the cloud. But one constant, from on-prem to the cloud, is the importance of vulnerability management in protecting your most sensitive data. However, just identifying a vulnerability is not enough. With the speed and scale of the cloud, and therefore, the high volume of vulnerabilities within it, organizations need a way to prioritize and remediate severe risks quickly. Visibility into attack paths and a vulnerability’s blast radius is required to truly manage security risks. Teams need to evaluate and prioritize vulnerabilities based on their

		potential impact on the business, with insight into the risks unique to the host. For example, if you don't know every identity on your workload and what access their permissions allow, you can't see which vulnerabilities could lead to an over permissioned identity with crown-jewel data access. Join our cloud expert to see how security teams are benefiting from the unique combination of agentless vulnerability scanning, CSPM, CIEM, data protection, and automation to bring their public cloud to a state of security excellence. Jeff Moncrief, Field CTO of Sonrai Security, will discuss and demonstrate the following: - Why workload vulnerability scanning is only step one in a comprehensive cloud security strategy - How attackers are exploiting vulnerabilities in your cloud through attack paths that lead to your most sensitive data - The technological advantages of agentless scanning and governance automation for managing risk "at the speed of cloud" - How understanding "blast radius", "risk amplification" and vulnerabilities unique to the host can help you prioritize risks in your cloud and speed up your remediation strategies.

12:15pm Demo Stage

Cloud Security Demo for Trending Security Features: CSPM, CIEM, CWPP, Identity Security and Data Security	Jeff Moncrief	Join cloud security expert, Jeff Moncrief, for an in-depth demo of the latest trends in AWS, Microsoft Azure, and Google cloud security, including Cloud Infrastructure Entitlement Management (CIEM), Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), identity security and data security features. We will highlight the capabilities Sonrai Security offers and get the answers to the most frequently asked questions our customers have about this cloud security feature trends. If you're curious to know more about the most complete and effective approaches available for securing your people and non-people identities, managing

		identity entitlement risks, preventing misconfiguration, and overall securing your workloads, than you need to see this demo.

12:45pm Demo Stage

Demo Exabeam Automation & Advanced Analytics	Jim Chrisos	While protecting your organization from external threats is critical, external threats may not pose the biggest risk to your business. The trusted employee or contractor that breaks bad can cause untold damage to your business, all while operating in plain sight. Your security stack often is oblivious to these actions, giving you a false sense of security while in reality the company jewels are pilfered. To combat these insider threats you must baseline, monitor, and analyze behavior of users and assets around the clock, and react fast when something suspicious is identified. Exabeam helps organizations around the world gain new insights into the inner workings of their environments, while simultaneously rooting out threats hiding in the open.

1:15pm Breakout Sessions

Incident Response In The Wild: Three Real World Incident Autopsies	John Harmon	As an information security professional, you are likely no stranger to thinking in worst-case scenario terms. Considering what the worst case would be can help you prepare for it. Of course, learning from the experience of others can help as well. During this engaging session, you will hear the story of a real incident, what went wrong (hint: a lot of things went very, very wrong), and how to avoid meeting the same fate as the unfortunate victim. Join John Harmon and learn how to plan for the worst.

Value Control: Optimizing Data Management and Business Value	Kyle Schiemo	There is a basic rule in security: don't spend more to protect an asset than what it's worth. It's a simple concept but difficult to apply, especially for data. Data is an asset, but the means of data valuation is still an open question. Existing data valuation methodologies are qualitative or semi-quantitative at best. The question may be, how can data be quantitatively valued so that the costs of data security controls can be assessed? We say that data value and data security are not independent concepts to be addressed separately. Instead, they are mutually dependent. We propose a systematic framework that embeds the costs and benefits of security controls directly into data valuation. The result is the management of business functions, value, and risk. We call this framework value control. This framework resulted from our capstone project done in collaboration with the University of Minnesota Technological Leadership Institute. We will share the analysis that led us to this concept of value control, how it was applied to produce recommendations for our organization, and show how it may be used at yours.
2022, the Year the SEC Changed the Rules about Cyber Risk	Chris Veltsos	In March 2022, the SEC issued a proposed rule change about the way public companies should go about tracking and reporting on cyber risk. This session will: 1) Shed light on this cyber risk governance earthquake moment by covering the SEC's key changes to its disclosure rules; 2) Outline the implications of this change for business leaders and for cybersecurity leaders; 3) Provide recommendations for corporations — public or private — to implement given this greater level of scrutiny.
Stump the Stumper : Foundations for Building an InfoSec Program	Karl Krug, Ken Shaurette	Lots of new and even senior Information Security professionals wonder how to build a robust program. Scott and Ken will provide a unique Q&A interview style presentation that will provide a lively and entertaining oppotunity to advance your fundamentals of InfoSec and understand clearly that Compliant does NOT mean Secure.
Communicating the Business Value of Your Information Security Program	Adam Stone	When communicating with corporate executives, some CISOs experience skepticism and resistance to requests for support and resource allocation to the information security function. Thinking about possible root causes, industry experts point to the fact that these CISOs often present tactical metrics instead of articulating a clear,

		mission-aligned message of *business value* for the organization. Further, CISOs need to be able to articulate the return on investment for any given expenditure and to develop predictive capabilities regarding where to invest. During this session, we will discuss ways to elevate your conversations with executives and improve your effectiveness as an information security leader.
Dwell Time - The Consequence of Not Watching	Tim Otis	In this session we will discuss lessons learned from real incident response investigations where evidence of threat actor activity was available. Evidence of activity that nobody saw for months and was only uncovered after serious damage occurred when the Check Point Incident Resposne Team was called in to investigate. Time and time again it is cyber security basics that could have prevented compromise.
Supercharging Microsoft Sentinel with Cribl + ReliaQuest	Alex Volk, Bill Larsen	It's difficult to parse logs natively and in real-time, especially considering how rapidly Microsoft is building additional connectors. ReliaQuest and Cribl work together to solve this problem: • First, Cribl normalizes the log data coming through, making it consistent and compatible with Microsoft Sentinel. • Next, ReliaQuest uses the data to identify and mitigate threats more effectively through the magic of automation. Through our partnership, ReliaQuest and Cribl help your organization get the best bang for your buck out of Microsoft Sentinel while also increasing visibility, reducing complexity, and managing risk. Join our live webinar to learn how ReliaQuest and Cribl are the ultimate dream team for getting the most out of Microsoft Sentinel.

2:45pm Breakout Sessions

World of Modern Apps: Dissecting Ransomware and Botnet Threats in Cloud Databases	Aditya K Sood	Attackers are targeting cloud databases used for modern applications to subvert the integrity and confidentiality of the stored data. Databases include MongoDB, Elasticsearch, etc., are being infected with ransomware and exploited in the wild to conduct data exfiltration, and data destruction. In this talk, we present a threat landscape of ransomware and botnet infections in the databases deployed for modern applications. The talk unveils the techniques and tactics for detecting ransomware and botnet infections in the cloud databases by practically

		demonstrating the detection of real-world infections using developed tools. The audience can use the tools to conduct efficient security assessment of cloud databases against stringent infections. The talk equips the threat researchers and penetration testers to build threat intelligence that can be consumed at a large scale.
Street Cred: Increasing Trust in Passwordless Authentication	Wolfgang Goerlich	Good security gets out of the way of users while getting in the way of adversaries. Passwords fail on both accounts. Users feel the pain of adhering to complex password policies. Adversaries simply copy, break, or brute-force their way in. Why, then, have we spent decades with passwords as the primary factor for authentication? The industry needs to trust passwordless authentication. Adversaries and then criminals have circumvented our authentication controls for decades. From the very first theft of cleartext passwords to the very latest bypass of a second-factor, time and again improvements in defenses are met with improved attacks. What holds us back from getting rid of passwords? Trust. In this session, we will propose a framework of technical controls to ensure only trusted sessions authenticate, regardless of faults or failures in any one factor. We will share a path forward for increasing trust in passwordless authentication.
Exercising Resilience: Lessons for the Private Sector	John Blood	Increasingly, private sector critical infrastructure firms are being asked to exercise their resiliency. This session will discuss how the Homeland Security Exercise and Evaluation Program (HSEEP), used in the public sector, can be easily adapted for use in the private sector. HSEEP and its many templates and best practices can make quick work of exercise planning, conduct, evaluation, and continuous quality improvement. The difference between the sectors is that with the private sector there is often less executive investment in spending multiple days on an exercise. And yet, exercising is vital to your preparedness and your resilience. We will explore the basics of HSEEP and describe a few examples of how a private enterprise can exercise smartly and efficiently while still building senior governance support.
Open-Source Software as a Double-Edge Sword	Hannah Connolly	Open source and third-party code are ubiquitous in everything from proprietary codebases to community projects - the question isn't whether your organization has

		open source software in projects, it's how much there is. The past two years have demonstrated the continuing and evolving threat of malicious dependencies and software libraries, with actors increasingly using these foundations of the software supply chain to push malware. Learn from a Cyber Threat Intelligence analyst about how the threats have evolved, hear lessons learned, and explore where this threat is going in the future.
The Singularity Has Happened, Not with a Bang but with a Whimper	Richard Thieme	Thinking differently is easy to talk ABOUT but actually thinking differently is really hard. Yet what confronts us are a set of conditions that suggest the future will not be what it used to be. So we need to think differently about it. 25 years ago Richard Thieme's keynote for Def Con, 'Hacking as Practice for Trans-planetary Life in the 21st Century,' correctly outlined what the tech revolution would bring. Looking out now requires leaping to the meta-level which that revolution has brought about. We need to operate on the meta-level because the meta-level is operating on us. This presentation illuminates this daunting challenge and how we might respond.
Beyond Advanced Persistent Threats: Common Tradecraft and High Value Detection Opportunities	Lauren Podber	Most adversaries don't need to be advanced or sophisticated to execute code or persist in a compromised environment. In this presentation, we'll break down some of the most pervasive threats we see and show how defensive strategies for commodity and state threats are not mutually exclusive.
Solving for X with XDR: Widening the Aperture for Rapid Detection, Investigation and Response	Ken Westin	There has been a lot of buzz around Extended Detection and Response (XDR) as an evolution of Endpoint Detection and Response (EDR), however definitions vary depending on who you talk to. Given the dramatic changes to network architectures as organizations move workloads to the cloud, leverage disparate SaaS tools, while also still relying on traditional on-premise networks has increased data volumes and the complexity of detecting threats across these environments. In this session we will discuss the evolution of security from the endpoint and beyond, from legacy aniti-virus, to EDR and now XDR. We will show how detection use cases and workflows that used to require complex and manually configured SIEM and SOAR solutions can

		be automated and streamlined with XDR, for rapid detection, investigation and response.