MARCH 11, 2020 - DAY 1 AGENDA

TIME	TYPE	SPEAKER NAME	SPEAKER TITLE AND ORGANIZATION	PRESENTATION TITLE	PRESENTATION ABSTRACT (150 WORDS OR LESS)
7:00 - 8:00 AM	Networking Check-in with Breakfast	NA		open	
8:00 AM -8:45 AM	KEYNOTE	**Mr. Charlie Margiotta**	**Director of the National Insider Threat Task Force**	counterintellingence; psych.; policies; rise of suicide …root of int is tension	INSIDER THREAT – A DISCUSSION OF WHERE WE'VE BEEN AND WHERE WE'RE GOING - With the recent roll-out of the National Counterintelligence Strategy, signed by the President in January, 2020, the U.S. government has shifted from focusing on the threats posed by top foreign nation-state adversaries (THE WHO), to focusing on where they're hitting us hardest and where we need to devote greater attention (THE WHERE/WHAT). The areas being targeted the most include Critical Infrastructure, Supply Chains, the Economy, Democratic Institutions, and Cyber. The new strategy also accepts that the U.S. government cannot address these threats alone, and needs the assistance of the private sector, an informed American public, and our allies. Proactive insider threat reporting can provide early warning, intervention, and assistance for individuals at risk, while strengthening our national resilience, and the resilience of our private sector partners, and academic institutions.
8:45 AM -9:30 AM	SPEAKER	Greg Pierson	Greg Pierson, Co-Founder, iovation, a TransUnion Company		Detecting fraud as part of an insider threat program - A comprehensive insider threat program should include external information like credit and public records, among others, to fully inform security managers of potential risks. In this session, TransUnion's Greg Pierson will discuss what kind of external information to look for and how you can apply it to an insider threat program. Greg will also reveal a new approach to uncovering hidden insider risks that requires little to no personal information.
9:30 AM - 9:45 AM	COFFEE BREAK	na	LexisNexis	HOSTED BY LEXISNEXIS - Please visit our sponsors, without them iTS6 would not be possible.	na
9:45 AM - 10:30 AM	SPEAKER	**Brian Thompson**	**Departmental Security Branch / Royal Canadian Mounted Police**		Balancing the use of Technology and Behavioural Indicators of an Insider Threat - The Royal Canadian Mounted Police (RCMP) is a national policing agency that encompasses Municipal, Provincial and Federal policing responsibilities relating to Criminal Law Enforcement, National Security, and International Policing. The RCMP implements a unified approach to existing Insider Threats, partnering with Internal Business Lines in an effort to respond to each Insider Threat incident. This collaborative approach adds effectiveness and efficiency to the process, ensuring that threats are mitigated. Canadian "Case Scenarios" of actual Insider Threats (Desjardin Banking, Whettlaufer) will be provided relating the perspective of balancing Behavioural and Technological Indicators.
10:30 AM -11:15 AM	SPEAKER	**JT MENDOZA**	**Deputy Director, United States Air Force (USAF) Insider Threat Hub**		**Insider Threat Program Assessment Abstract: While organizations approach the insider threat challenge differently, most struggle with the consistent requirement to assess and/or justify program existence. Often this includes efforts trying to determine ROI, effectiveness, etc. to senior leaders or stakeholders who may not understand the impact of not having an insider threat program. In his presentation, J.T. Mendoza leverages his experience with two mature insider threat programs within the USG to share a general framework for evaluating an insider threat program.**
11:15-12:15 PM	LUNCH BREAK	na	Advanced onion	hosted by Advanced Onion, Inc.	NA
12:15 PM - 1:00 PM	SPEAKER	Eric Anderson	observeit		**Insider Threat Common Questions** - We will explore a deeper look into the Ponemon Study on insider threats and a more general exploration of metrics, skill sets and processes when it comes to program development, internal operations best practices and components in between. The session is intended to be open-ended gathering participation from the attendees, no right or wrong answers just sharing experience from within the crowd.
1:00 PM - 1:45 PM	SPEAKER	Chris Grijalva	Perspecta	Senior Technology Director at Perspecta	Continuous Evaluation: Evolution to the Trusted Workforce Abstract This presentation will go through the history of Personnel Security with origins all the way back to the 1800's and journey through the policy and legal changes that have led up to this point. The discussion will also cover the current state of the Personnel Security Program including advantages and weakpoints. Finally, we will talk about the migration toward Continuous Evaluation/Continuous Vetting and what this migration means.
1:45 PM - 2:00 PM	BREAK	na	lexisNexis		

TIME	TYPE	SPEAKER NAME	SPEAKER TITLE AND ORGANIZATION	PRESENTATION TITLE	PRESENTATION ABSTRACT (150 WORDS OR LESS)
2:00 PM -2:45 PM	SPEAKER	Mark Wilson	Director of Sales, Radiant Logic		Federated Identity & Virtualization: Removing Identity Integration as a Roadblock for Security and Digital Transformation - Data can be both our greatest Achilles' heel and the most powerful tool for building innovative and secure defense solutions. To be successful, we need to understand attributes of identities (both structured and unstructured) across the enterprise and harness this data to be interoperable across multi-domains for decision making. We must also deal effectively with the complexity associated with a wide variety of evolving data sources. Identity is the new boundary. Breach is assumed and focus is applied in a different place: identity data and integration.Our approach to solving this dilemma involves abstracting identities from underlying repositories into a flexible, scalable infrastructure built on virtualization and big data technology. Without disrupting existing identity sources, RadiantOne builds a future-state, reusable unified identity layer for consuming applications. The result: identity becomes an enabler, not a security bottleneck, allowing you to build on your legacy and accelerate your future identity objectives.
2:45 PM - 3:30 PM	SPEAKER	Dr. Bob Roland	Operational/Clinical Psychologist		Personality assessment and the individual fit in organizations is an interesting consideration for those with a digital focus. On the other hand - it might be a foreign language. None-the-less, without the human dimension what really matters?
3:30 PM - 3:45 PM	COFFEE BREAK	na		OPEN	
3:45 PM - 4:45 PM	OPEN PANEL DISCUSSION		Michael Douglass, President of Advanced Onion, Moderating; Major Ryan Kelly, Ph.D., Army Research Facilitation Laboratory; J.T. Mendoza, Deputy Director, United States Air Force (USAF) Insider Threat Hub; Bill Falk, Chief Revenue Officer, AC Global Risk; Eric Hanna, Insider Threat Unit, DHS/TSA		tbd
5:00 PM -8:00 PM	NETWORKING RECEPTION with food and beverages	na		Sponsored by Transunion and Advanced Onion	na

MARCH 12, 2020 - DAY 2 AGENDA					
TIME	TYPE	SPEAKER NAME	SPEAKER TITLE AND ORGANIZATION	PRESENTATION TITLE	PRESENTATION ABSTRACT (150 WORDS OR LESS)
7:00 - 8:00 AM	Networking Check-in with Breakfast	NA			
8:00 AM -8:45 AM	KEYNOTE	**Rich McComb**	Chief Security Officer at the Office of the Chief Security Officer (OCSO) for the US Department of Homeland Security (DHS)		**Evolving Faster Than the Threat: An Information-centric Approach to Insider Threat Operations - As every security professional knows, guns, guards, gates, and walls don't usually keep insider threats out of organizations. Such threats may already be lurking in your organization despite your best efforts on the exterior edges to keep them at bay. Just as threats have evolved, our operations, responses, and understanding of them have needed to evolve. In this session, Richard McComb, Chief Security Officer for the Department of Homeland Security, using recent case studies, will discuss his department's information-centric approach to insider threat operations and explain how its program has grown more proactive and refined its detection, analysis, information sharing, and case management methods.**
8:45 AM -9:30 AM	SPEAKER	Dustin Burns	Senior Scientist, Exponent		Can AI predict human behavior? - Given the rapid increase of novel machine learning applications in cybersecurity and people analytics, there is significant evidence that these tools can give meaningful and actionable insights. Even so, great care must be taken to ensure that automated decision making tools are deployed in such a way as to mitigate bias in predictions and promote security of user data. In this talk, Dr. Burns will take a deep dive into an open source data set in the area of people analytics, demonstrating the application of basic machine learning techniques, while discussing limitations and potential pitfalls in using an algorithm to predict human behavior. In the end, Dustin will draw a comparison between the potential to predict human behavioral propensity to things such as becoming an insider threat to how assisted diagnosis tools are used in medicine to predict development or reoccurrence of illnesses.
9:30 AM-9:45 AM	COFFEE BREAK	TBD	TBD		
9:45 AM -10:30 AM	SPEAKER	Caitlin Gremminger	Cyber & Counterintelligence Strategic Partnership Coordinator, Special Agent at FBI		SA Gremminger will share current examples about how YOU are being targeted by cyber criminals and foreign adversaries and what you can do to protect yourself.
10:30 AM - 11:15 AM	SPEAKER	Pete Ruppert	United States Army in Europe - Insider Threat Program Manager		Implementation of an Insider Threat Program from the Ground Up. - Mr. Ruppert discusses his approach on standing up an insider threat program in Europe from a sheet of paper to full operational capability as well as some organizational challenges and solutions that transcend the military and government.
11:15-12:30 PM	LUNCH BREAK				

12:30 PM -1 :15 PM	SPEAKER	Bill Kalogeros	Acalvio		The Never-Ending Battle Against Insider and Advanced Persistent Threats How Next-Generation Deception Technology Goes on the OffenseThe US government is engaged in a constant battle against well-funded, motivated attackers. The "front line" extends well beyond government networks and is broadly distributed in private organizations (defense contractors and service providers). Traditional security technologies focus on trying to look for "evil." Evil, in the case of your SEIM/IDS, would be to pattern the SEIM/IDS configuration to look for signatures/anomalies. As a result, all an attacker needs to do to avoid detection is to appear "not evil." This is the problem with traditional detection technologies. Instead of looking for evil, we can look for abnormal. If we know what happens on our networks normally, we can identify abnormal behavior and investigate it as suspicious. This is the reason deception technologies are an important part of any cybersecurity arsenal. On today's digital battlefield, organizations need to deploy Next-Generation Deception Technology: decoys/lures, misdirections, and systems to attract and snare attackers.
1:15 PM - 2:00 PM	SPEAKER	Riley Bruce	Code 42		The Insider Threat: You're Flying Blind Abstract: Studies show that 90% of data loss that manifests from inside organizations goes undetected. What's worse, nearly 70% of organizations that were breached from the inside had a data loss prevention solution in place. The brutal truth - prevention solutions are not effective at stopping insider threats. Attend this session from Code42 to learn how data risk detection and response ensures you and your organization are not blindsided.
2:00 - 2:15 PM	BREAK				
2:15 - 3:00 PM	SPEAKER	Matthew St Sure,	System Engineer II at Stanislaus County, CA		
3:00 PM -3:45 PM	SPEAKER	Stephanie L. Jaros,	Director of Research, DoD Counter-Insider Threat Program Defense Personnel and Security Research Center (PERSEREC) Office of People Analytics (OPA)		
	end		end		end
AGENDA TIMES AND SPEAKERS ARE SUBJECT TO CHANGE					