SANS DFIR CYBER THREAT INTELLIGENCE Summit

Agenda | Thursday, January 21

#CTISummit

View the complete agenda **here**. Add all of the CTI Summit presentations to your schedule by subscribing to the **CTI Summit Calendar**.

9:00–9:15 am EST 14:00–14:15 UTC	Hosted in Track 1 ***Welcome & Opening Remarks*** **Rebekah Brown**, @PDXBek, Summit Co-Chair **Rick Holland**, @rickhholland, Summit Co-Chair **Robert M. Lee**, @RobertMLee, Summit Co-Chair **Katie Nickels**, @likethecoins, Summit Co-Chair	
9:15–9:45 am EST 14:15–14:45 UTC	Hosted in Track 1 ***Keynote*** **Chris Krebs**, @C_C_Krebs, Fmr. Director, US Cybersecurity and Infrastructure Security Agency (CISA); Founder, Krebs Stamos Group	
9:45–10:00 am EST 14:45–15:00 UTC	**Break**	
	TRACK 1	TRACK 2
10:05–10:40 am EST 15:05–15:40 UTC	***Riding the WAVE to Better Collaboration and Security*** **Kelsey Helms**, Lead Cyber Threat Intelligence Analyst, Target Corporation **Nate Icart**, Lead Threat Intelligence Detection Engineer, Target Corporation	***Hack Your Stakeholder: Eliciting Intelligence Requirements with Design Thinking*** **Brian Kime**, @BrianPKime, Senior Analyst, Forrester
10:00–11:30 am EST 15:00–16:30 UTC	**Workshop: Threat Intelligence the "EASY" Way** **Chris Cochran**, Founder & Producer, Hacker Valley Media	
10:40–10:50 am EST 15:40–15:50 UTC	**Break**	
10:50–11:25 am EST 15:50–16:25 UTC	***Asleep at the Wheel? The Effects of sSleep on CTI Professionals*** **Lincoln Kaffenberger**, @LincolnKberger, Threat Intelligence Service Lead, Deloitte Global	***Better Than Binary: Elevating State-Sponsored Attribution via Spectrum of State Responsibility*** **Joshua Miller**, @chicagocyber, Senior Intelligence Analyst
11:30 am – 12:05 pm EST 16:30–17:05 UTC	***xStart When You're Ready*** **John Southworth**, @BitsOfBinary, Threat Intelligence Analyst, PwC UK	***Cyber-Espionage: Out of the Shadows, Into The Digital Crosshairs*** **John Grim**, Distinguished Architect – Head of Research, Development, Inn0vation, Verizon Threat Research Advisory Center

You will receive 12 CPEs for attending SANS Cyber Threat Intelligence Summit live (6 for each day). Your Certificate of Completion and CPEs will be issued within a week of the Summit's conclusion. At this time, we are not able to issue CPEs to those that view the Summit recording.

SANS DFIR

CYBER THREAT INTELLIGENCE

Summit

Agenda | Thursday, January 21 (Continued)

#CTISummit

View the complete agenda **here**. Add all of the CTI Summit presentations to your schedule by subscribing to the **CTI Summit Calendar**.

12:05–1:00 pm EST 17:05–18:00 UTC	**Lunch**	
	TRACK 1	**TRACK 2**
1:00–1:35 pm EST 18:00–18:35 UTC	***Not That Kind of Vulnerability! Human Trafficking During Coronavirus*** **Sherrie Caltagirone**, @GblEmancipation, Founder & Executive Director, Global Emancipation Network	***The Joy of Threat Landscaping*** **Gert-Jan Bruggink**, @gertjanbruggink, Co-founder, CTI Analyst & Defensive Specialist, FalconForce
1:40–2:15 pm EST 18:40–19:15 UTC	***Jackpotting ESXi Servers For Maximum Encryption – How One Criminal Organization is Upping The Stakes for Targeted Ransomware*** **Eric Loui**, Senior Intelligence Analyst, CrowdStrike **Sergei Frankoff**, Senior Security Researcher, CrowdStrike	***Threat Intel for Everyone: Writing Like A Journalist To Produce Clear, Concise Reports*** **Selena Larson**, @selenalarson, Cyber Threat Analyst, Dragos
2:20–2:55 pm EST 19:20–19:55 UTC	***The CTI Shadow Army: Tales from the Trenches – Small Business Owner/Solopreneur Edition*** **Xena Olsen**, @ch33r10	***The Cognitive Stairways of Analysis*** **Nicole Hoffman**, @threathuntergrl, Intelligence Analyst, GroupSense
2:55–3:05 pm EST 19:55–20:05 UTC	**Break**	
3:05–3:40 pm EST 20:05–20:40 UTC	***Spooky RYUKy: Chapter 2*** **Van Ta**, Senior Threat Analyst, Mandiant **Aaron Stephens**, Senior Threat Analyst, Mandiant	***Data Matters: More Effective Threat Hunting and Defense with Internet Scan Data*** **Derek Abdine**, @dabdine, Chief Technology Officer, Censys
3:45–4:20 pm EST 20:45–21:20 UTC	***Collections and Elections: How The New York Times Built an Intel Collections Program in 2020*** **Neena Kapur**, Security Intelligence Manager, The New York Times **Emily Wilson**, @thirdemily, Intelligence Collections Manager, The New York Times	***Full Cycle: Blending Intelligence Requirements and Custom Dissemination Tools to Drive Operations*** **Jon Jurado**, Principle Associate, Cyber Threat Intelligence, Capital One **Robert McLean**, Senior Manager, Cyber Threat Intelligence, Capital One
4:25–5:00 pm EST 21:25–22:00 UTC	**Hosted in Track 1** ***Day 1 Wrap-Up Panel***	

You will receive 12 CPEs for attending SANS Cyber Threat Intelligence Summit live (6 for each day). Your Certificate of Completion and CPEs will be issued within a week of the Summit's conclusion. At this time, we are not able to issue CPEs to those that view the Summit recording.

SANS DFIR

CYBER THREAT INTELLIGENCE

Agenda | Friday, January 22

#CTISummit

View the complete agenda **here**. Add all of the CTI Summit presentations to your schedule by subscribing to the **CTI Summit Calendar**.

	TRACK 1
9:00–9:15 am EST 14:00–14:15 UTC	***Welcome & Opening Remarks*** **Rebekah Brown**, @PDXBek, Summit Co-Chair **Rick Holland**, @rickhholland, Summit Co-Chair **Robert M. Lee**, @RobertMLee, Summit Co-Chair **Katie Nickels**, @likethecoins, Summit Co-Chair
9:15–10:00 am EST 14:15–15:00 UTC	***Keynote: SolarWinds of Change: A New Era of Supply Chain Attacks and its Impact on Analysis and Attribution*** **Stephen Eckels**, @stevemk14ebr, FLARE Reverse Engineer, Mandiant **Isif Ibrahima**, @isifmobile , FLARE-AP Principal Threat Analyst, Mandiant **Jacqueline O'Leary**, Manager, Advanced Analysis, Mandiant
10:05–10:40 am EST 15:05–15:40 UTC	***Pivoting from Art to Science*** **Joe Slowik**, @jfslowik, Senior Security Researcher, DomainTools
10:40–10:50 am EST 15:40–15:50 UTC	**Break**
10:50–11:25 am EST 15:50–16:25 UTC	***VERISIZE Your Way into CTI*** **David Thejl-Clayton**, Cyber Defence Center Department Manager, JN Data
11:30 am – 12:05 pm EST 16:30–17:05 UTC	***Six CTI Challenges and Their Solutions – Reaching CTI's Full Potential*** **Dr. Christian Doerr**, Chair of Cyber Security and Enterprise Security, Hasso Plattner Institute **Kris Oosthoek**, @f00th0ld, Senior CTI Analyst, Rijkswaterstaat (Dutch Public Works/Critical Infrastructure Agency)
12:05–1:00 pm EST 17:05–18:00 UTC	**Lunch**
12:30–12:50 pm EST 17:30–17:50 UTC	**BONUS SESSION: SANS Technology Institute Graduate Program: An Insider's View** **Kim Kafka**, Admissions Specialist, SANS Technology Institute **Megan Roddie**, Cyber Threat Researcher, IBM

You will receive 12 CPEs for attending SANS Cyber Threat Intelligence Summit live (6 for each day). Your Certificate of Completion and CPEs will be issued within a week of the Summit's conclusion. At this time, we are not able to issue CPEs to those that view the Summit recording.

SANS DFIR

CYBER THREAT INTELLIGENCE

Agenda | Friday, January 22 (Continued)

#CTISummit

View the complete agenda **here**. Add all of the CTI Summit presentations to your schedule by subscribing to the **CTI Summit Calendar**.

1:05–1:40 pm EST 18:05–18:40 UTC	***Still Thinking About Your Ex(cel)? Here are Some TIPs*** **Andreas Sfakianakis**, @asfakian, Cyber Threat Intelligence Analyst
1:45–2:20 pm EST 18:45–19:20 UTC	***Analyzing Chinese Information Operations with Threat Intelligence*** **Che Chang**, Cyber Threat Analyst, TeamT5 **Silvia Yeh**, @silvia_yeh, Cyber Threat Analyst, TeamT5
2:25–3:00 pm EST 19:25–20:00 UTC	***Quantifying Intelligence: Increasing Executives IQ*** **Colin Connor**, Global Threat Intelligence Analyst, IBM
3:05–3:15 pm EST 20:05–20:15 UTC	**Break**
3:15–3:50 pm EST 20:15–20:50 UTC	***Will They Read My Reports? Creating Value Driven Reports*** **Christopher Lopez**, @l0psec, Tanium
3:55–4:30 pm EST 20:55–21:30 UTC	***Day 2 Wrap-Up Panel***
5:00–6:00 pm EST 22:00–23:00 UTC	**Happy Hour: CTI Career Success**

You will receive 12 CPEs for attending SANS Cyber Threat Intelligence Summit live (6 for each day). Your Certificate of Completion and CPEs will be issued within a week of the Summit's conclusion. At this time, we are not able to issue CPEs to those that view the Summit recording.

SANS DFIR

CYBER THREAT INTELLIGENCE

Solutions Track

Agenda | Friday, January 22

The Cyber Threat Intelligence Solutions Track showcases case-studies and thought leadership to provide security practitioners with the latest industry leading products and services they can use to improve their threat intelligence capabilities.

Register to attend the CTI Summit Solutions Track **here**.

	SOLUTION TRACK
10:05–10:15 am EST 15:05–15:15 UTC	***FOR578: Cyber Threat Intelligence Update and Move to Six Days*** **Rob M. Lee**, @RobertMLee, Summit Co-Chair, SANS Institute
10:15–10:50 am EST 15:15–15:50 UTC	***Cisco*** **Ben Greenbaum**, @secintsight, Technical Leader, Cisco
10:50–11:25 am EST 15:50–16:25 UTC	***A Product Approach to Your Threat Intelligence Practice: Increase Investment and Outcomes*** **Chris Jacob**, Vice President of Threat Intelligence Engineering, ThreatQuotient
11:25 am – 12:00 pm EST 16:25–17:00 UTC	***From the Front Lines Incident Response at Scale*** **James Perry**, Senior Director and Global Head of Incident Response, CrowdStrike
12:00–12:15 pm EST 17:00–17:15 UTC	**Break**
12:15–12:50 pm EST 17:15–17:50 UTC	***Cisco Umbrella – Correlating Threat Intelligence with CTIM*** **Daniel Bates**, Technical Solutions Architect, Cisco Umbrella
12:50–1:25 pm EST 17:50–18:25 UTC	***Turning Data into Actionable Threat Intelligence*** **Fayyaz Rajpari**, Sr. Director of Product, SOC/IR, Recorded Future **Dragos Gavrilut**, Director, Cyber Threat Intelligence Lab, Bitdefender
1:25–2:00 pm EST 18:25–19:00 UTC	***Post Mortem: The First 72 Hours of SUNBURST Threat Intelligence Research*** **Tanner Payne**, Senior Sales Engineer, ExtraHop
2:00–2:10 pm EST 19:00–19:10 UTC	**Break**
2:10–2:45 pm EST 19:10–19:45 UTC	***Are You Ready for Intelligent SOC?*** **Brandon Hoffman**, CISO, Head of Security Strategy, NetEnrich
2:45–3:20 pm EST 19:45–20:20 UTC	***Key Functionalities of a Modern Cyber Threat Intelligence Program*** **Jerry Caponera**, Vice President of Cyber Risk Strategy, ThreatConnect
3:20–3:30 pm EST 20:20–20:30 UTC	**Break**
3:30–4:05 pm EST 20:30–21:05 UTC	***SUNBURST: DGA or DNS Tunneling?*** **Peter Rydzynski**, Threat Analysis Lead, IronNet
4:05–4:40 pm EST 21:05–21:40 UTC	***Agile Threat Intelligence for the Modern Threatscape*** **Sumukh Tendulkar**, Product Marketing, Sixgill, Sixgill **Michael-Angelo Zummo**, Cyber Threat Intelligence Analyst, Sixgill
4:40–5:15 pm EST 21:40–22:15 UTC	***Going from Open Source Intelligence to Threat Intelligence with DomainTools Iris*** **Taylor Wilkes-Pierce**, @tw_pierce, Sr. Sales Engineer, DomainTools,
5:15–5:30 pm EST 22:15–22:30 UTC	***Wrap-Up***

You will earn 4 CPE credits for attending the Cyber Threat Intelligence Solutions Track.
Your Certificate of Completion and CPEs will be issued within a week of the event's conclusion.

SANS DFIR

CYBER THREAT INTELLIGENCE

Summit

Event Time Zones

#CTISummit

Time Zone	Day 1	Day 2
Pacific Standard Time (PST) UTC –8	6:00 am (Thu) – 2:00 pm (Thu)	6:00 am (Fri) – 3:00 pm (Fri)
Central Standard Time (CST) UTC –6	8:00 am (Thu) – 4:00 pm (Thu)	8:00 am (Fri) – 5:00 pm (Fri)
Eastern Standard Time (EST) UTC –5	**9:00 am (Thu) – 5:00 pm (Thu)**	**9:00 am (Fri) – 6:00 pm (Fri)**
Greenwich Mean Time (GMT) UTC +0	2:00 pm (Thu) – 10:00 pm (Thu)	2:00 pm (Fri) – 11:00 pm (Fri)
Central European Time (CET) UTC +1	3:00 pm (Thu) – 11:00 pm (Thu)	3:00 pm (Fri) – 12:00 am (Sat)
India Standard Time (IST) UTC +5:30	7:30 pm (Thu) – 3:30 am (Fri)	7:30 pm (Fri) – 4:30 am (Sat)
Singapore Time (SGT) UTC +8	10:00 pm (Thu) – 6:00 am (Fri)	10:00 pm (Fri) – 7:00 am (Sat)
Japan Standard Time (JST) UTC +9	11:00 pm (Thu) – 7:00 am (Fri)	11:00 pm (Fri) – 8:00 am (Sat)
Australian Eastern Daylight Time (AEDT) UTC +11	1:00 am (Fri) – 9:00 am (Fri)	1:00 am (Sat) – 10:00 am (Sat)