SANS DFIR

CYBER THREAT INTELLIGENCE

Summit 2025

AGENDA

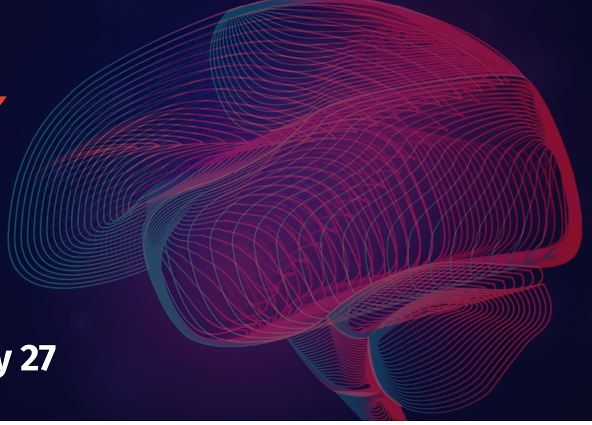
January 27–28

Alexandria, VA

#CTISummit

CYBER THREAT INTELLIGENCE
Summit 2025

SANS DFIR



Sunday, January 26 | Monday, January 27

#CTISummit

View the complete agenda here.

Sunday, January 26

Time	Session
4:30–6:00 PM ET 9:30–11:00 PM UTC	**Event Registration** (Location: Edison Foyer)

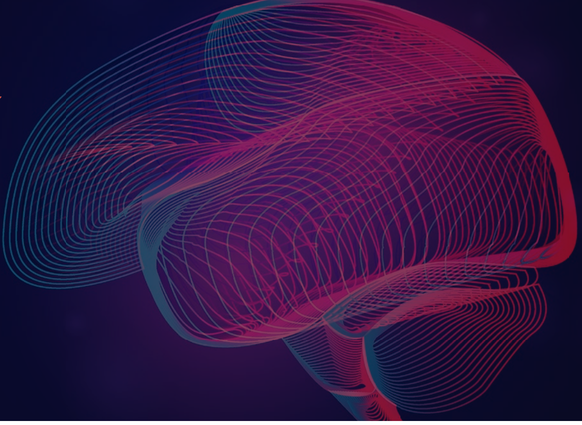
Monday, January 27

Time	Session
7:30–9:00 AM ET 12:30–2:00 PM UTC	**Summit Registration and Solutions Expo** (Location: Edison Foyer) Pick up your badge and join us for a light breakfast before SANS Cyber Threat Intelligence Summit 2025 kicks off!
	Track One – Location: Edison ABCD (In-Person & Streaming Live Online)
9:00–9:15 AM ET 2:00–2:15 PM UTC	***Day 1 Opening Remarks*** Rebekah Brown, Author, SANS Institute Rick Holland, CISO, ReliaQuest Katie Nickels, Certified Instructor, SANS Institute
9:15–10:00 AM ET 2:15–3:00 PM UTC	***Keynote | The Anticipatory Approach: Actionable (not Reactionable) Cyber Threat Intelligence*** Dr. Jeannie Johnson, Founding Director, Center for Anticipatory Intelligence at Utah State University
10:00–10:15 AM ET 3:00–3:15 PM UTC	**Break and Solutions Expo** (Location: Edison Foyer)

Time	Track One	New2CTI – Location: Edison E (Streaming Live Online)	Location: Edison F (In-Person Only)	Location: Edison Foyer (In-Person Only)
10:15–10:50 AM ET 3:15–3:50 PM UTC	***Beyond the FOMO: Expanding Horizons for Cyber Threat Intelligence Analysts*** Sydney Jones, Head of Cyber Threat Intelligence, CLS Group	10:15–10:50 AM ET 3:15–3:50 PM UTC ***Ransomware Syndicates: Cartels or Twisted Tech Unicorns?*** Dr. Ferhat Dikbiyik, Chief Research & Intelligence Officer (CRIO), Black Kite	10:15 AM–12:05 PM ET 3:15–5:15 PM UTC ***Workshop: Threat Hunting and Criminal Infrastructure Analysis – SANS FOR589*** John Doyle, SANS Certified Instructor; Principal Intelligence Enablement Consultant for Mandiant	10:00 AM–12:00 PM ET 3:00–5:00 PM UTC ***Personalized 20-Minute 1:1 and Small-Group Coaching Sessions to Identify Workplace Stressors and How to Address Them*** Daniel Shore and Zac Broomfield
10:55–11:30 AM ET 3:55–4:30 PM UTC	***ONNX Store: The Rise and Fall of a Phishing-as-a-Service Platform Targeting Financial Institutions*** Arda Büyükkaya, Senior Cyber Threat Intelligence Analyst, EclecticIQ	10:55–11:30 AM ET 3:55–4:30 PM UTC ***Dissecting the Cicada: In the Shadow of the Black Cat*** Nicklas Keijser, Threat Research Analyst, Truesec Mattias Wåhlén, Threat Intelligence Expert, Truesec		
11:35 AM–12:05 PM ET 4:35–5:05 PM UTC	***Making CTI Cool!: Methods for Teaching Cyber Threat Intelligence Through Gaming*** Bryan Quillen, Cybersecurity Instructor, Fairdale High School Jibby Saetang, Security Researcher, Microsoft (GHOST) & KC7Cyber	11:35 AM–12:05 PM ET 4:35–5:05 PM UTC ***But Mom, I Need To Spend More Time on Social Media! (Bridging CTI and Fraud: Understanding Social Media Cyber Threat Landscape and Beyond)*** Daniel Widya Suryanata, Incident Response Senior Manager, GoTo Group Jurgen Visser, Head of Cyber Defense and Enterprise Security, GoTo Group		

Time	Session
12:05–1:30 PM ET 5:05–6:30 PM UTC	**Lunch and Solutions Expo** (Location: Edison Foyer)

CYBER THREAT INTELLIGENCE
Summit 2025



SANS DFIR

Monday, January 27 *(Continued)*

#CTISummit

View the complete agenda **here**.

Track One – Location: Edison ABCD (In-Person & Streaming Live Online)

1:30–2:05 PM ET
6:30–7:05 PM UTC

From Threat Intelligence to Detection Engineering: A Case Study on Identifying Gaps in Detection and Enhancing CTI Value for the Organization

Pedro Barros, Security Analyst II, CODE

2:10–2:45 PM ET
7:10–7:45 PM UTC

Advanced Threat Research Methodologies: Unraveling a Triple-APT Intrusion

Tom Fakterman, Threat Researcher, Palo Alto Networks

Lior Rochberger, Senior Threat Researcher, Palo Alto Networks

New2CTI – Location: Edison E (Streaming Live Online)

1:30–2:05 PM ET
6:30–7:05 PM UTC

Everybody Wants to Rule the World (of Data)

John Stoner, (Army) Senior Security Consultant, Google Cloud – Public Sector

John Stoner, (Civ) Global Principal Security Strategist, Google Cloud

2:10–2:45 PM ET
7:10–7:45 PM UTC

The Secret Life of Forgotten Malware C2

Eli Woodward, Cyber Threat Intelligence Analyst, Early Warning Services

Location: Edison Foyer (In-Person Only)

1:30–2:30 PM ET
6:30–7:30 PM UTC

Personalized 20-Minute 1:1 and Small-Group Coaching Sessions to Identify Workplace Stressors and How to Address Them

Daniel Shore and Zac Broomfield

2:45–3:10 PM ET
7:45–8:10 PM UTC

Afternoon Break and Solutions Expo (Location: Edison Foyer)

3:10–3:45 PM ET
8:10–8:45 PM UTC

Building Cyber Threat Resilience with STRAT: A New Methodology for CTI

Scott Roberts, Head of Threat Research, Interpres Security

Chandler McClellan, Student, Intrusion Analyst Intern, Utah State University, CrowdStrike

3:10–3:45 PM ET
8:10–8:45 PM UTC

Building the CTI Brand: A Path to Success

Matt Brady, Director CTI, Target

Location: Edison Foyer (In-Person Only)

3:10–4:10 PM ET
8:10–9:10 PM UTC

Personalized 20-Minute 1:1 and Small-Group Coaching Sessions to Identify Workplace Stressors and How to Address Them

Daniel Shore and Zac Broomfield

3:50–4:25 PM ET
8:50–9:25 PM UTC

Immaturity Can Be Fun: Just Not in a CTI Program

John Holland, CTI Operations Consultant, IntL8

Alexander Perez Palma, Threat Intelligence, Workday

4:30–4:40 PM ET
9:30–9:40 PM UTC

Day One Wrap-Up & Day Two Preview

Rebekah Brown, Author, SANS Institute

Rick Holland, CISO, ReliaQuest

Katie Nickels, Certified Instructor, SANS Institute

5:30–7:30 PM ET
10:30 PM–12:30 AM UTC

Summit Night In | Minute 2 Win It (Location: Edison Foyer)
Get your game faces on! Join us after the summit for a series of different challenges, food, drinks, networking, and a chance to win prizes. One lucky player will walk away with an Apple Watch!

Summit CPEs & Certificate of Completion
You will receive 12 CPEs for attending SANS Cyber Threat Intelligence Summit 2025 live, 6 for each day you attend. Currently, we are not able to issue CPEs to those that view the Summit recordings. A Certificate of Completion will be available in your account on Tuesday, February 4 (after the conclusion of the Summit & course training) and can be found under the *My Orders* section of your SANS Dashboard Account. SANS will automatically submit your Summit CPEs to GIAC within 7–10 business days after the event's end date, no action is required on your part.

Slack

CYBER THREAT INTELLIGENCE

Summit 2025

SANS DFIR

Monday, January 27

#CTISummit

SOLUTIONS TRACK

View the complete agenda **here**.

10:30–10:40 AM ET 3:30–3:40 PM UTC	***Event Kickoff & Introduction*** Doug McKee, Event Chairperson & SANS Certified Instructor Candidate	
10:40–11:15 AM ET 3:40–4:15 PM UTC	***So You Need a Threat Profile... Now What?*** Taylor Long, Sr. Analyst for Custom Intelligence Solutions and Research, Mandiant Intelligence at Google Cloud Security Steven Savoldelli, Sr. Intelligence Consultant, Mandiant Intelligence at Google Cloud Security	Google Cloud Security
11:15–11:50 AM ET 4:15–4:50 PM UTC	***Optimizing Suspicious File Triage*** Aaron Hoffman, SOAR Architect at Reversing Labs Stuart Phillips, Sr. Cybersecurity Marketing Strategist at Reversing Labs	ReversingLabs
11:50 AM**–12:25** PM ET 4:50–5:25 PM UTC	***Exposing Triad Nexus: How FUNNULL CDN Facilitates Widespread Cyber Threats*** Noah Plotkin, Solutions Engineer at Silent Push	SILENT PUSH
12:25–12:40 PM ET 5:25–5:40 PM UTC	**Break**	
12:40–1:15 PM ET 5:40–6:15 PM UTC	***How the Rebels Beat the Empire: Cyber Threat Intelligence Lessons from Star Wars*** Dan Cole, VP of Product Marketing at ThreatConnect	ThreatConnect.
1:15–1:50 PM ET 6:15–6:50 PM UTC	***Unlocking Cyber Resilience: Censys ASM + Search Solutions for Modern Threat Intelligence*** Paul Lambert, Sr. Solutions Engineer at Censys	censys
1:50–2:25 PM ET 6:50–7:25 PM UTC	***Using Customizable Vulnerability Intelligence to See Threats Faster and Act Smarter*** Kasimir Schulz, Co-Founder at Rapid Risk Radar	RAPID RISK RADAR DEFEND FASTER. DEFEND SMARTER.
2:25–3:00 PM ET 7:25–7:30 PM UTC	***Event Recap & Closing Remarks*** Doug McKee, Event Chairperson & SANS Certified Instructor Candidate	

THANK TO OUR SUMMIT SPONSORS

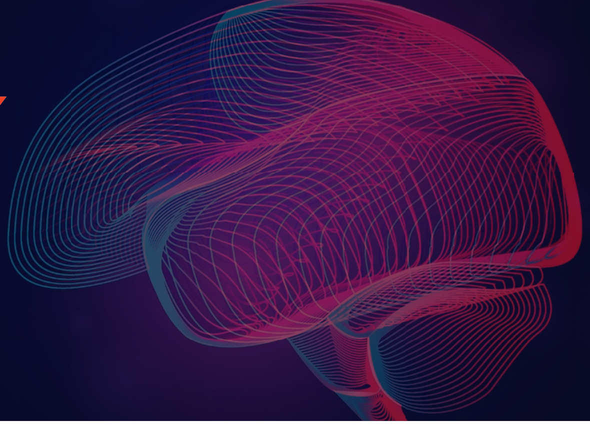
CARDINALOPS Detection Posture Management · censys · CROWDSTRIKE · feedly · Filigran

flare · Google Cloud Security · GREYNOISE INTELLIGENCE · INTEL471 · Microsoft

RAPID RISK RADAR DEFEND FASTER. DEFEND SMARTER. · Recorded Future® · ReversingLabs · SILENT PUSH · Silobreaker

SOPHOS Cybersecurity evolved. · ThreatConnect. · THREATLOCKER · TIDAL CYBER THREAT-INFORMED DEFENSE · VMRAY

CYBER THREAT INTELLIGENCE
Summit 2025



SANS DFIR

Tuesday, January 28

#CTISummit

View the complete agenda **here**.

7:30–9:00 AM ET
12:30–2:00 PM UTC
Summit Registration and Solutions Expo (Location: Edison Foyer)

Track One – Location: Edison ABCD (In-Person & Streaming Live Online)

9:00–9:15 AM ET
2:00–2:15 PM UTC

Day 2 Opening Remarks

Rebekah Brown, Author, SANS Institute

Rick Holland, CISO, ReliaQuest

Katie Nickels, Certified Instructor, SANS Institute

9:15–10:00 AM ET
2:15–3:00 PM UTC

Keynote | Your Mental Health & Well-Being: Combating the Adversaries of Stress and Burnout in Cybersecurity

Dr. Daniel Shore, Co-Founder, Multiteam Solutions

10:00–10:15 AM ET
3:00–3:15 PM UTC
Break and Solutions Expo (Location: Edison Foyer)

10:15–10:50 AM ET
3:15–3:50 PM UTC

What a Cluster: A Case Study in Threat Actor Collaboration and Framework for Comparative Attribution

Jono Davis, Senior Analyst, PwC Global Threat Intelligence Team

10:55–11:30 AM ET
3:55–4:30 PM UTC

Iterate and Innovate: Applying the Startup Mindset to CTI

Josh Darby MacLellan, Staff Threat Intelligence Advisor, Feedly

11:35 AM–12:10 PM ET
4:35–5:10 PM UTC

Navigating the Fog of War: A Programmatic Approach to Capturing and Communicating Relevant Insights from Rising Geopolitical Tensions

John Doyle, Certified Instructor

Simone Kraus, Senior CSIRT, Orange Cyberdefense

Workshops – Location: Edison F (In-Person Only)

10:15 AM–12:10 PM ET
3:15–5:10 PM UTC

SAT for CTI: Structured Analytic Techniques for Cyber Threat Intelligence

Rebekah Brown, Author, SANS Institute

Scott Roberts, Head of Threat Research, Interpres Security

Location: Edison Foyer

10:15 AM–12:15 PM ET
3:15–5:15 PM UTC

Personalized 20-Minute 1:1 and Small-Group Coaching Sessions to Identify Workplace Stressors and How to Address Them

Daniel Shore and Zac Broomfield

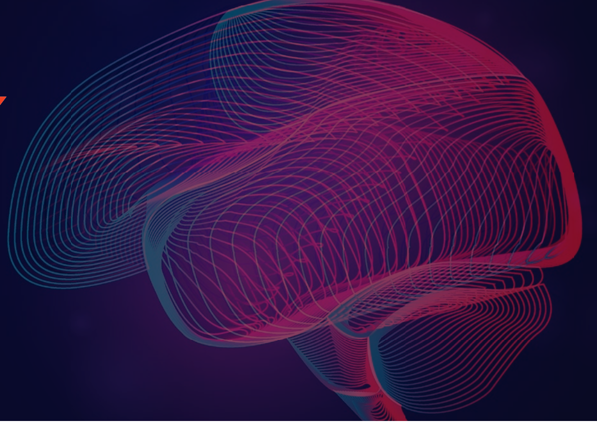
12:10–1:30 PM ET
5:10–6:30 PM UTC
Lunch and Solutions Expo (Location: Edison Foyer)

Summit CPEs & Certificate of Completion
You will receive 12 CPEs for attending SANS Cyber Threat Intelligence Summit 2025 live, 6 for each day you attend. Currently, we are not able to issue CPEs to those that view the Summit recordings. A Certificate of Completion will be available in your account on Tuesday, February 4 (after the conclusion of the Summit & course training) and can be found under the *My Orders* section of your SANS Dashboard Account. SANS will automatically submit your Summit CPEs to GIAC within 7–10 business days after the event's end date, no action is required on your part.

Slack

CYBER THREAT INTELLIGENCE

Summit 2025



SANS DFIR

Tuesday, January 28 *(Continued)*

#CTISummit

View the complete agenda **here**.

	Track One – Location: Edison ABCD (In-Person & Streaming Live Online)	Workshops – Location: Edison F (In-Person Only)
1:30–2:05 PM ET 6:30–7:05 PM UTC	***Sales And Marketing Are Threat Actors, Too*** Erica Peterson, Director of Sales and Marketing, Digital Project Masters and The Vertex Project Michael Graven, Director	1:30–3:30 PM ET 6:30–8:30 PM UTC ***Leadership Workshop: Tools and Strategies to Motivate Yourself and Others in Cybersecurity*** Daniel Shore, Co-Founder, Multiteam Solutions Zac Broomfield
2:10–2:45 PM ET 7:10–7:45 PM UTC	***Decoding Cyber Threats: A Practical Guide to Using Attack Trees*** Gert-Jan Bruggink, Founder & CEO, Venation Sherman Chu, Cyber Threat Intelligence Lead, BlackRock	
2:45–3:00 PM ET 7:45–8:00 PM UTC	**Break and Solutions Expo** (Location: Edison Foyer)	
3:00–3:35 PM ET 8:00–8:35 PM UTC	***It's So Overt its Covert: Leveraging Classic HUMINT Tactics in CTI Investigations*** Eliska Puckova, Cyber Threat Intelligence Specialist, Ubisoft Julien Mascaro, Security & Forensic Investigator, Ubisoft	
3:40–4:00 PM ET 8:40–9:00 PM UTC	***Day Two Wrap-Up and Event Close*** Rebekah Brown, Author, SANS Institute Rick Holland, CISO, ReliaQuest Katie Nickels, Certified Instructor, SANS Institute	

Summit CPEs & Certificate of Completion

You will receive 12 CPEs for attending SANS Cyber Threat Intelligence Summit 2025 live, 6 for each day you attend. Currently, we are not able to issue CPEs to those that view the Summit recordings. A Certificate of Completion will be available in your account on Tuesday, February 4 (after the conclusion of the Summit & course training) and can be found under the *My Orders* section of your SANS Dashboard Account. SANS will automatically submit your Summit CPEs to GIAC within 7–10 business days after the event's end date, no action is required on your part.

Slack

CYBER THREAT INTELLIGENCE

Summit 2025

SANS DFIR

Tuesday, January 18

#CTISummit

SOLUTIONS TRACK

View the complete agenda **here**.

10:30–10:40 AM ET 3:30–3:40 PM UTC	***Event Kickoff & Introduction*** Doug McKee, Event Chairperson & SANS Certified Instructor Candidate	
10:40–11:15 AM ET 3:40–4:15 PM UTC	***Building Effective Threat-Driven Security Posture Validation Programs*** Samuel Hassine, CEO & Co-Founder at Filigran	Filigran
11:15–11:50 AM ET 4:15–4:50 PM UTC	***Threat Intelligence Research: Navigating the Threat Landscapes*** Sherrod DeGrippo, Director of Threat Intelligence Strategy at Microsoft	Microsoft
11:50 AM**–12:25** PM ET 4:50–5:25 PM UTC	***Using Infostealer Logs for Advanced Threat Intelligence Work*** Nick Ascoli, Director of Product Strategy at Flare	flare
12:25–12:40 PM ET 5:25–5:40 PM UTC	**Break**	
12:40–1:15 PM ET 5:40–6:15 PM UTC	***Who's Afraid of Little Old Me? Tracking Ransomware Groups Targeting Your Third Parties*** Kathleen Kuczma, Technical Marketing Manager at Recorded Future	Recorded Future®
1:15–1:50 PM ET 6:15–6:50 PM UTC	***Beyond Detection: Using Malware Analysis to Enhance CTI and Proactive Defense*** Shyam Pema, Enterprise Senior Security Sales Engineer at VMRay	VMRAY
1:50–2:25 PM ET 6:50–7:25 PM UTC	***Navigating the NVD Slowdown: AI and OSINT Strategies for Vulnerability Prioritization*** Josh Darby MacLellan, Staff Threat Intelligence Advisor at Feedly	feedly
2:25–2:40 PM ET 7:25–7:40 PM UTC	**Break**	
2:40–3:15 PM ET 7:40–8:15 PM UTC	***Your Threat Intelligence Called...It Wants to be Actionable*** Jay Lillie, VP of Customer Success at CardinalOps	CARDINALOPS Detection Posture Management
3:15–3:50 PM ET 8:15–8:50 PM UTC	***Separating Phish from the Chaff: Searching for Phishing Page Infrastructure*** Jordon Olness, Threat Intelligence Analyst at Sophos	SOPHOS Cybersecurity evolved.
3:50–4:25 PM ET 8:50–9:25 PM UTC	***Improving Ransomware Threat Assessment with Structured Prioritization*** Scott Small, Director of Cyber Threat Intelligence at Tidal Cyber	TIDAL CYBER THREAT-INFORMED DEFENSE
4:25–4:30 PM ET 9:25–9:30 PM UTC	***Event Recap & Closing Remarks*** Doug McKee, Event Chairperson & SANS Certified Instructor Candidate	

Solutions Track CPEs & Certificate of Completion

You will receive 10 CPEs for attending SANS Cyber Threat Intelligence Solutions Track 2025 live, 4 on Monday, January 27th & 6 on Tuesday, January 28th. You will need to submit your certificate of completion to GIAC to receive your CPEs.

Slack

Upcoming SANS Summits

2025

OSINT

Arlington, VA & Virtual
SUMMIT: February 24–25
TRAINING: February 26–March 3

New2Cyber

Virtual (ET)
SUMMIT: March 13

AI Cybersecurity

Denver, CO & Virtual
SUMMIT: March 31–April 1
TRAINING: April 2–7

Cybersecurity Leadership

Virtual (CT)
SUMMIT: April 24

Emerging Threats

Arlington, VA & Virtual
SUMMIT: May 13–14

Ransomware

Virtual (ET)
SUMMIT: May 30

ICS

Orlando, FL & Virtual
SUMMIT: June 15–17
TRAINING: June 18–23

DFIR

Salt Lake City, UT & Virtual
SUMMIT: July 24–25
TRAINING: July 26–31

Security Awareness

Chicago, IL & Virtual
TRAINING: August 11–13
SUMMIT: August 14–15

CloudSecNext

Denver, CO & Virtual
TRAINING: October 2–3
SUMMIT: October 4–9

All North American Virtual Summits in 2025 are free.
For more info on upcoming Summit events, visit: sans.org/summits

SANS