



FEBRUARY 25, 2026

## CISO Financial Services NY

► Real conversations from Cloud and DevSecOps to the pressures of the boardroom

If you lead security in Financial Services, this is your room — filled with people who live the same reality you do and talk about it.

When we launched **CISO New York** last September, the response from teams at **HSBC, Wells Fargo, and New York City Council** was: *"This feels built for us."* *"You don't usually hear these conversations on stage."* *"This is a community."*

On **February 25, 2026**, in **Hyatt Jersey City on The Hudson**, we're bringing that same energy, but this time, it's **Financial Services**.

- The new attack patterns targeting financial data right now
- Securing cloud + multi-cloud when nothing is standardized
- AI that cuts SecOps noise instead of adding more
- The fraud and insider threats everyone is feeling but no one is openly talking about

You don't need another event filled with long lectures and generic sessions- you need the community, and the formats that give you answers.

- **Ask-Me-Anything** —unfiltered answers from veteran CISOs
- **Yes / No / Maybe** —fast gut checks on the topics no one agrees on
- **Quick Wins or Just Noise** — tools + tactics that your peers say work
- **Live Poll Debate** — the entire room votes in real time

\*Get in touch with the Conference Producer for this event via [monika.dincheva@coriniumgroup.com](mailto:monika.dincheva@coriniumgroup.com)

### Confirmed Speakers:

- Gharun Lacy, Deputy Assistant Secretary of State for Cyber and Technology Security Bureau of Diplomatic Security -**U.S. Department of State**
- Aaron Katz, *Chief Information Security Officer*-**THE TCW GROUP**
- Scot Miller, *SVP, Chief Information Security Officer* – **Mr. Cooper** (*Advisory board member*)

- Ellis Wong, *Chief Information Security Officer - JST Capital* (Advisory board member)
- Jessica Wilson, *Business Information Security Officer – Bank of America*
- Christopher Russell, *CISO & Head of Tokenization – TZERO GROUP*
- Mo Jamous, *EX Chief Information Officer, Consumer & Business Banking – U.S. Bank*
- Ben Rothke, *Senior Information Security Manager - Experian*
- John Decker, *Chief Technology Officer -Trian Partners*
- Nishit Mehta, Vice President, *Analytics Solutions Manager – JPMorganChase*
- Purna Nayak, *Senior Manager - IT Risk and Control (Data Governance) - Americal Express*
- Paul Pak, *Chief Information Security Officer, Head of Information Governance - Jennison Associates* (Advisory board member)
- Hasan Dimdik, *Senior Workplace Security Engineer – ING*
- Matthew Presson, *CISO for the Americas – Bullish*
- Mahesh Addanki, *Cyber Security Engineer - BlackRock*
- Robert LaRosa, *Information Security Engineer - GELLER*
- Alexander Abramov, *Head of Information Risk -Consultant at Financial Services*
- Julia Cherashore, *Senior Fellow- DATA Foundation*
- Johanthan Sander, *Field CTO - Astrix Security*
- Donovan Stevens, *Principal Sales Engineer - SpyCloud*
- Neil Cohen, *Head of Marketing – Portal26*
- Frank Teruel, *Chief Operating Officer ArkoseLabs*
- Kelly Shortridge, *Chief Product Officer –Fastly*
- Darryl Jones, *VP, Consumer Segment Strategy -Ping Identity*
- Valery Milman - *Sr. Manager, Systems Engineering - ForeScout*

## CISO FS NY

### February 25th, 2026

08:00 – 08:45	<i>Registration &amp; Coffee in the Exhibition Area</i>
8:45 - 8:55	<b>Chair's Opening Remarks</b> Johanthan Sander, <i>Field CTO - Astrix Security</i>
8:55- 9:00	<b>Speed Networking – Making new connections at CISO FS NY!</b> During this 5-minute networking session, the aim of the game is to go and meet two

	people you don't already know.
09:00 - 09:30	<p><b>Opening Panel: Confessions of CISOs: What They Don't Tell You About the Job</b></p> <ul style="list-style-type: none"> <li>• How can sleepless nights, board politics, and regulator heat be managed without burnout?</li> <li>• Which AI-driven threats and hybrid risks are keeping CISOs awake in 2026?</li> <li>• When speed clashes with security and compliance with agility, how can the trade-offs be survived?</li> <li>• What do CISOs wish had been known before stepping into the role?</li> </ul> <p>Moderator: Mo Jamous, <i>EX Chief Information Officer, Consumer &amp; Business Banking – U.S. Bank</i></p> <p>Matthew Presson, <i>CISO for the Americas – Bullish</i></p> <p>Paul Pak, <i>Chief Information Security Officer, Head of Information Governance - Jennison Associates</i></p> <p>Scot Miller, <i>SVP, Chief Information Security Officer – Mr. Cooper (Advisory board member)</i></p> <p>Christopher Russell, <i>CISO &amp; Head of Tokenization – TZERO GROUP</i></p> <p>Gharun Lacy, Deputy Assistant Secretary of State for Cyber and Technology Security Bureau of Diplomatic Security -U.S. Department of State</p>
09:30 - 10:00	<p><b>Presentation: Did you know your firm has a crypto trading platform?</b></p> <p>From ramp and dump schemes (pig butchering) to executive assassinations/executive cyber stalking, why you need to have a Brand and Executive Protection Program in the world of AI and why you need one now.</p> <p>Paul Pak, <i>Chief Information Security Officer, Head of Information Governance - Jennison Associates</i></p>
10:00 - 10:30	<p><b>Expert Ask-Me-Anything: AI, Risk &amp; Regulation</b></p> <p>An informal, interactive session where the audience will ask questions live, on the spot.</p> <p>Speakers respond in real time to questions on AI risk and security, regulatory challenges (SEC, NYDFS, DORA), board-level communication, and building resilient cyber teams.</p> <p><u>Moderator:</u> Alexander Abramov, <i>Head of Information Risk -Financial Services</i> Mo Jamous, <i>EX Chief Information Officer, Consumer &amp; Business Banking – U.S. Bank</i> Robert LaRosa, <i>Information Security Engineer – GELLER</i> Johanthan Sander, <i>Field CTO- Astrix Security</i></p>

10:30- 10:45	<p><b>Malware, Money Laundering &amp; the Markets: Unmasking Hidden Financial Exposures</b></p> <p>Financial services organizations face a uniquely complex attack surface – one where cybercriminals exploit exposed consumer identities, often without detection. At the center of this threat: infostealer malware, silently exfiltrating identity data including authentication cookies, credentials, and session tokens to bypass MFA and expose critical access points.</p> <p>In this session, we'll share our findings on how malware infections are fueling fraud, money laundering, and platform abuse across banks, insurers, and payment service providers. We'll walk through a few real-world examples revealing how security and fraud teams are leveraging recaptured darknet data to detect the intersection of legitimate accounts with criminal marketplaces – surfacing hidden exposures before damage is done.</p> <p>Whether it's a single infected consumer device linked to fraudulent activity and 30+ suspicious accounts, or credentials surfacing on Telegram, these threats are happening now. Join us to better understand the lifecycle of malware-based threats and how leading financial institutions are using identity-centric strategies to prevent attacks using recaptured data.</p> <p>Donovan Stevens, <i>Principal Sales Engineer - SpyCloud</i></p>
10:45- 11:00	<p><b>Fireside chat with Fastly</b></p> <p>Kelly Shortridge, Chief Product Officer -<b>Fastly</b></p>
11:00 11:30	<p><i>Mid-Morning Coffee &amp; Networking in the Exhibition Area</i></p>
	<p>The CISO Boardroom</p> <p>Cloud &amp; DevSecOps Lab</p>

11:30- 12:00	<p><b>Presentation: Agentic AI in Financial Services: Strategic Defense for the Autonomous Threat Era</b></p> <ul style="list-style-type: none"> <li>• How can deepfake fraud, model poisoning, AI-powered phishing, and AI in credit or lending decisions be stopped?</li> <li>• Who owns AI risk, and which frameworks or guardrails keep innovation safe?</li> <li>• Who carries the liability when AI fails in FS?</li> <li>• How is AI risk best reported in board language?</li> <li>• What playbooks work for AI-specific incidents like data leakage or model poisoning?</li> </ul> <p>Frank Teruel, <i>Chief Operating Officer</i> ArkoseLabs</p>	<p><b>Presentation: Lessons from the Trenches: DevSecOps in Regulated Finance</b></p> <ul style="list-style-type: none"> <li>• Which pipeline controls are best enforced through policy-as-code?</li> <li>• How can security checks be safely delegated to dev teams in regulated contexts?</li> <li>• What metrics demonstrate DevSecOps reducing audit findings?</li> <li>• Where does human review still outperform automated tools in Financial Services?</li> </ul> <p>Ellis Wong, <i>Chief Information Security Officer</i> - JST Capital</p>
12:00 – 12:15	<p><b>Live Poll Debate: Would You Trust AI to Act Before Your Team Can?</b></p> <p>Experts go head-to-head, using real incidents and risks from the field. We'll start with a live poll to see where the room stands, then run it again at the end to track if minds have shifted.</p> <p>The debate centers on one tough question: <i>should we ever let technology act on its own during a live cyber incident in financial services?</i></p> <p>The audience is part of it too so ask your questions, share your views, and see how your take stacks up against your peers.</p>	<p><b>A Reality Check for DevSecOps Leaders</b></p> <p>The moderator will share a series of real-world statements, with the audience voting yes / no / maybe before opening the discussion. The focus is on how security, development, and operations actually work together in practice.</p> <p>Topics include managing third-party risk in fast-moving cloud environments, navigating overlapping compliance requirements, measuring what really matters for boards, and whether current resilience and incident-response plans would stand up in a real event.</p> <p>Julia Cherashore, <i>Senior Fellow</i>- DATA</p>

	<p>John Decker, <i>Chief Technology Officer - Trian Partners</i>  Mo Jamous, <i>EX Chief Information Officer, Consumer &amp; Business Banking – U.S. Bank</i></p>	<b>Foundation</b>
12:15 - 13:00	<p><b>Discussion group A: What Happens When Agentic AI Runs Your Security Ops Before You Do?</b></p> <ul style="list-style-type: none"> <li>• What risks come with AI-on-AI escalation between defenders and adversaries?</li> <li>• How can effective oversight frameworks be built for AI-augmented SOCs?</li> <li>• What early wins, and early fails are showing up in adopting agentic AI for security?</li> <li>• How can human analysts stay in the loop when machines move first?</li> </ul> <p>Moderated by Valery Milman - <i>Sr. Manager, Systems Engineering - ForeScout</i></p> <p>Ellis Wong, <i>Chief Information Security Officer - JST Capital</i></p> <p>Scot Miller, <i>SVP, Information Security - Rocket (Advisory board member)</i></p> <p>Mahesh Addanki, <i>Cyber Security Engineer - BlackRock</i></p>	<p><b>Presentation: When Banks Hold the Keys: The New CISO Reality Post-SAB 122</b></p> <ul style="list-style-type: none"> <li>• What SAB 122 changes for CISO accountability and audit scrutiny</li> <li>• How “probable loss” is being interpreted, measured, and defended in practice</li> <li>• The evolving institutional threat landscape once banks hold the keys</li> <li>• How existing security, identity, and governance models must adapt conceptually</li> </ul> <p>Christopher Russell, <i>CISO &amp; Head of Tokenization – TZERO GROUP</i></p>
13:00 – 14:00	<p><i>Lunch &amp; Networking in the Exhibition Area</i></p>	

14:00- 14:20	<p><b>Presentation: The Five Habits of Highly Secure Organizations</b></p> <p>Companies that have developed world-class information security programs have achieved their goals by focusing on security within a risk-mitigation framework.</p> <p>This session will reveal the five main habits shared by the most secure organizations. By focusing on these habits, organizations can spend much less on security while gaining a significant level of security.</p> <p>Ben Rothke, <i>Senior Information Security Manager - Experian</i></p>	<p><b>Presentation: Insider Risk 2.0: When AI Changes the Threat Landscape</b></p> <p>AI is changing the nature of insider risk, amplifying the impact of trusted users and blurring the boundary between productivity and threat. As identities gain more power and controls struggle to keep pace, organisations must rethink insider risk through behaviour, context, and AI-driven defence.</p> <p>Hasan Dimdik, <i>Senior Workplace Security Engineer – ING</i></p>
14:20- 14:40	<p><b>Presentation: Beyond the Breach: What Diplomatic Targets Reveal About Financial Sector Risks</b></p> <p>The U.S. Department of State's Diplomatic Security Service (DSS) protects more than 77,000 personnel across 270+ locations worldwide, often operating inside environments where nation-state cyber actors are active. This places DSS on the front line of advanced threat activity, frequently seeing tactics before they are deployed at scale against financial institutions.</p> <p>Drawing on real-world incidents, including the response to Storm-0558, this session shares how DSS detects and responds to sophisticated attacks in real time, operates under the assumption of breach, and maintains operations during active compromise. Attendees will gain practical insight into reducing response times, managing vendor risk, strengthening human-layer defenses, and applying government-grade intelligence to financial services environments facing the same adversaries.</p> <p>Gharun Lacy, Deputy Assistant Secretary of State for Cyber and Technology Security Bureau of Diplomatic Security -U.S. Department of State</p>	

14:40-	<p><b>Panel Discussion: Who Owns the Fallout around when GenAI use misfires — Security, Risk, or the Board?</b></p>
--------	---

15:10	<ul style="list-style-type: none"> <li>• Who owns AI risk when models impact lending, underwriting, or fraud detection?</li> <li>• How do organisations embed AI monitoring into existing cyber and risk management frameworks?</li> <li>• What guardrails help prevent AI misuse without stifling innovation?</li> <li>• How should firms prepare for AI-specific incidents such as data leakage or model poisoning?</li> </ul> <p>Moderator: Neil Cohen, <i>Head of Marketing</i> - <b>Portal26</b></p> <p>Robert LaRosa, <i>Information Security Engineer</i> – <b>GELLER</b></p> <p>Scot Miller, <i>SVP, Chief Information Security Officer</i> – <b>Mr. Cooper</b> (<i>Advisory board member</i>)</p> <p>Gharun Lacy, Deputy Assistant Secretary of State for Cyber and Technology Security Bureau of Diplomatic Security -<b>U.S. Department of State</b></p>
15:10-15:40	<p><b>Presentation</b> by Darryl Jones, VP, Consumer Segment Strategy -<b>Ping Identity</b></p>
15:40-16:10	<p><i>Afternoon Break &amp; Networking in the Exhibition Area</i></p>
16:10-16:30	<p><b>Panel Discussion: Cloud Security: What's Working and Where We're Over-Engineering</b></p> <ul style="list-style-type: none"> <li>• Where cloud security breaks in real operating environments</li> <li>• Where DevSecOps enables delivery, and where it introduces friction</li> <li>• Which signals drive action versus noise during cloud incidents</li> <li>• What leaders would simplify or remove from today's cloud security stack</li> </ul> <p>Moderator: Julia Cherashore, Senior Fellow – <b>DATA Foundation</b></p> <p>Mahesh Addanki, Cyber Security Engineer - <b>BlackRock</b></p> <p>Aaron Katz, <i>Chief Information Security Officer</i>-<b>THE TCW GROUP</b></p>
16:30-17:00	<p><b>Panel Discussion: How to Stop Compliance Spend Becoming a Black Hole?</b></p> <ul style="list-style-type: none"> <li>• Where do compliance frameworks overlap across borders, and how can the duplication be cut?</li> <li>• What makes a compliance budget credible as resilience spending?</li> <li>• When does compliance move from obligation to competitive advantage?</li> <li>• Which signals of audit readiness build market trust?</li> </ul> <p>Moderator: Alexander Abramov, <i>Head of Information Risk</i> -<b>Financial Services</b></p> <p>Nishit Mehta, <i>Vice President, Analytics Solutions Manager</i> – <b>JPMorganChase</b></p>

	Robert LaRosa, <i>Information Security Engineer - GELLER</i>
17:00 17:05	<b>Chair's Closing Remarks</b> Johanthan Sander, <i>Field CTO - Astrix Security</i>
17:05 - 18:00	<i>Networking drinks and Prize Draw</i>
18:00	<b>END OF CONFERENCE</b>