Agenda

Incident Response

Day 1 March 19, 2026

Session 01:

State of Security

Get oriented to the security reality MSPs and IT teams are dealing with right now: how attackers operate, what's changed, and where organizations keep getting caught off guard. Walk away with sharper context for interpreting incidents quickly, setting priorities early, and making security decisions based on today's threat conditions. Not yesterday's assumptions.

Session 02:

Introduction to Incident Response

Build the incident response foundation required to lead, not just participate, when things go sideways. Leave with a clear understanding of the IR lifecycle, what "good" response looks like under pressure, and how to move response efforts from improvisation to a structured, repeatable approach that holds up when the stakes rise.

Session 03:

Assessing Threats to Organizations

Learn how to decide what matters first when everything feels urgent. Take away a practical method for evaluating threats using impact, likelihood, and business risk so response energy goes where it counts—and decisions remain defensible when timelines are tight and information is incomplete.

Session 04:

Initial Analysis and Documentation

Start incidents correctly, because early mistakes become expensive later. Develop the ability to run initial analysis with discipline, capture the details that actually matter, and document actions in a way that supports continuity, accountability, and clean handoffs when incidents stretch beyond a single person or shift.

Session 05:

Targeting Cover Letters

Recover without inviting a repeat incident. Leave with the decision-making framework to eradicate threats thoroughly, validate what "clean" really means, and restore operations safely: balancing speed with confidence so the business comes back online without reopening the same wound.

Session 06:

Using Incident Response Playbooks

Turn playbooks into something teams can actually use when pressure hits. Gain a repeatable approach to applying playbooks without becoming rigid: adapt to real conditions, keeping response consistent across people and clients, and reducing the chaos that slows everything down.

Agenda

Incident Response

Day 2 **March 20, 2026**

Session 07:

Incident Communication

Control the message while the situation is still moving. Walk away with communication patterns that reduce confusion, protect trust, and keep stakeholders aligned—internally and externally—so the response doesn't get derailed by mixed signals, over-sharing, or silence at the wrong time.

Session 08:

Incident Compliance and Risk

Make response decisions with the risk and compliance realities in mind, not as an afterthought. Leave with a stronger understanding of how regulatory requirements, contracts, and liability influence IR actions so technical response stays aligned with obligations and doesn't create avoidable exposure.

Session 09:

Effective Post-Mortems

Convert incidents into measurable improvement instead of a one-time scramble. Take away a structured post-mortem approach that identifies root causes, produces actionable changes, and strengthens readiness—because organizations that "move on" without learning always relive the same incident later.

Session 10:

Gaining Momentum & Building Incident Response Teams

Build an IR capability that works before the next incident tests it. Leave with practical guidance for defining roles, scaling the team, establishing operational readiness, and gaining internal buy-in, so incident response becomes an actual function, not a plan that exists only on paper.

Session 11:

Incident Response & the vCSO

Position incident response as a leadership responsibility and a trust anchor—not just a technical event. Walk away with a clear model for integrating IR into the vCSO role, aligning it to business outcomes, and communicating its value in a way clients and stakeholders understand when pressure is highest.

Session 12:

Wrap-Up

Tie the full IR lifecycle together into a single, usable operating model. Leave with clear next steps, reinforced decision points, and a path to keep maturing response capability, so leadership feels confident and coordinated when the next incident starts, not reactive and scattered.
