Monday, March 23

5:45 p.m.	Secure your AI apps before attackers do
6:15 p.m.	2025 cyberthreats wrapped: Cisco Talos' Year in Review

For a list of theater description, please click here.

Tuesday, March 24

10:30 a.m.	Defend faster than AI can exploit
11:00 a.m.	Identity is your new perimeter
11:30 a.m.	Secure your AI apps before attackers do
12:00 p.m.	Go beyond the user: Extend zero trust to agentic AI
12:30 p.m.	See inside your Kubernetes black box
1:00 p.m.	Starting your security operations journey with Cisco XDR
1:30 p.m.	Put firewall management on autopilot
2:00 p.m.	First hop, final stop

For a list of theater description, please click here.

Tuesday, March 24

2:30 p.m.	Go beyond the user: Extend zero trust to agentic AI
3:00 p.m.	AI without anxiety: Effective guardrails for GenAI
3:35 p.m.	2025 cyberthreats wrapped: Cisco Talos' Year in Review
4:00 p.m.	Foundation AI: Building security-specific LLMs
4:30 p.m.	Securing the AI frontier: The power of unified SASE
5:00 p.m.	Secure your AI apps before attackers do
5:30 p.m.	First hop, final stop

For a list of theater description, please click here.

Wednesday, March 25

10:30 a.m.	Securing the AI frontier: The power of unified SASE
11:00 a.m.	Foundation AI: Building security-specific LLMs
11:30 a.m.	Put firewall management on autopilot
12:00 p.m.	AI without anxiety: Effective guardrails for GenAI
12:30 p.m.	See inside your Kubernetes black box
1:00 p.m.	Identity is your new perimeter
1:30 p.m.	Defend faster than AI can exploit
2:00 p.m.	First hop, final stop

For a list of theater description, please click here.

Wednesday, March 25

2:30 p.m.	Go beyond the user: Extend zero trust to agentic AI
3:00 p.m.	Securing the AI frontier: The power of unified SASE
3:30 p.m.	Foundation AI: Building security-specific LLMs
4:00 p.m.	2025 cyberthreats wrapped: Cisco Talos' Year in Review
4:30 p.m.	Go beyond the user: Extend zero trust to agentic Ai
5:00 p.m.	Starting your security operations journey with Cisco XDR
5:30 p.m.	Put firewall management on autopilot

For a list of theater description, please click here.

Thursday, March 26

10:30 a.m.	Starting your security operations journey with Cisco XDR
11:00 a.m.	Identity is your new perimeter
11:30 a.m.	First hop, final stop
12:00 p.m.	Go beyond the user: Extend zero trust to agentic AI
12:30 p.m.	Defend faster than AI can exploit
1:00 p.m.	AI without anxiety: Effective guardrails for GenAI
1:30 p.m.	See inside your Kubernetes black box

For a list of theater description, please click here.

Theater description

2025 cyberthreats wrapped: Cisco Talos' Year in Review	AI has reshaped industries, but cybersecurity adoption has lagged due to models unfit for security tasks, high costs, scarce data, and integration challenges. Foundation AI, a new Cisco initiative, addresses this by delivering open-source, security-tuned models, tools, and datasets that give defenders the control and performance proprietary APIs can't provide. This talk covers why open innovation matters for security workflows, how small, specialized models can outperform far larger LLMs, and what new capabilities Foundation AI is releasing, including a base model, reasoning model, benchmarks, and supply-chain risk intelligence.
AI without anxiety: Effective guardrails for GenAI	GenAI is transforming the workplace, but it's also opening new doors for "Shadow AI" and accidental data exposure. Securing the AI era requires deep prompt inspection and nuanced controls. Learn how Cisco Secure Access provides invisible guardrails that automatically enforce sanctioned app usage and neutralize threats before they can compromise your data. Join us to see how you can scale AI adoption across your workforce with total confidence and zero friction.

Theater description

Defend faster than AI can exploit

Discover how to defend your infrastructure when AI-powered attackers exploit vulnerabilities faster than you can patch them. You'll see practical runtime shielding techniques, East-West traffic controls that block lateral movement, and surgical hardening strategies that protect critical assets before patches exist. Leave with actionable approaches to stay ahead when exploitation timelines collapse from weeks to hours.

First hop, final stop

Contain threats at the first hop—before they become your next incident. Learn how to enforce security at the switch level, turning your network infrastructure into an enforcement point that stops lateral movement in its tracks. You'll see how to collapse network and security functions into a single platform, eliminate hardware sprawl, and enforce segmentation closer to the source—whether at the access layer, core, or cloud edge. Walk away knowing how to give your NetOps and SecOps teams a unified view and shared controls to cut response time when threats emerge.

Theater description

Foundation AI: Building security-specific LLMs

AI has reshaped industries, but cybersecurity adoption has lagged due to models unfit for security tasks, high costs, scarce data, and integration challenges. Foundation AI, a new Cisco initiative, addresses this by delivering open-source, security-tuned models, tools, and datasets that give defenders the control and performance proprietary APIs can't provide. This talk covers why open innovation matters for security workflows, how small, specialized models can outperform far larger LLMs, and what new capabilities Foundation AI is releasing, including a base model, reasoning model, benchmarks, and supply-chain risk intelligence.

Go beyond the user: Extend zero trust to agentic AI

As AI agents begin to navigate networks and handle data autonomously, security strategies must evolve to keep pace. Securing this new landscape requires a SASE architecture that treats agents with the same rigor as human users. Explore how Cisco SASE integrates identity-driven security for users, things, and AI agents alike, ensuring your network remains secure and compliant as you deploy the next generation of AI.

Theater description

Identity is your new perimeter

Make identity your strongest defense. Discover how an identity-first zero trust approach gives you visibility and control over every user, device, and connection—before they access your applications. You'll learn how AI-powered identity intelligence detects risky behavior in real time, how to deploy phishing-resistant authentication that users actually love, and how to unify network and security into a single access solution that scales with your business.

Put firewall management on autopilot

Free your team from endless firewall tickets and alert fatigue. Discover how AI agents can autonomously monitor, detect, and fix firewall issues at machine speed—handling VPN capacity limits, bandwidth spikes, and compliance gaps before they impact your business. You'll see how these agents work like highly skilled admins who never sleep, using deep contextual insights to resolve problems proactively instead of reactively. Walk away with a clear path to reclaim your team's time for strategic work while achieving faster remediation, better compliance, and operational efficiency that manual processes can't match.

Theater description

Secure your AI apps before attackers do

Agents and AI applications are reshaping the way we do business; they also introduce a massive new attack surface to contend with. In this session, we'll explore AI risk in detail, covering topics like AI governance, supply chain vulnerabilities, and agentic threats. Then, we'll look at how to address these risks and secure AI from development through deployment—detecting vulnerabilities, stopping threats like prompt injections and data leakage in real time, and enabling your AI teams to innovate fearlessly.

Securing the AI frontier: The power of unified SASE

As AI redefines the enterprise, traditional siloed security models cannot keep pace with emerging threats. To thrive in the AI era, organizations must transition to a Unified SASE model that integrates Security Services Edge (SSE) with SD-WAN into one cohesive system. See how Cisco's unified approach turns your network into a strategic asset, securing every AI interaction and ensuring seamless, secure connectivity from the edge to the cloud

Theater description

See inside your Kubernetes black box

Stop treating Kubernetes like a black box your NetOps and SecOps teams can't see into. Learn how to gain complete visibility and control across your Kubernetes environments—especially critical for large-scale AI workloads where performance and security can't be compromised. You'll see how to achieve seamless, high-performance connectivity between Kubernetes clusters and traditional infrastructure, protect workloads with micro-segmentation and runtime enforcement, and get the deep observability you need to troubleshoot faster and prevent incidents.

Starting your security operations journey with Cisco XDR

There’s no one-size-fits-all approach to security operations. That’s why Cisco XDR and Splunk meet you where you are on your SOC journey. Cisco XDR provides foundational detection and response that enables lean teams to quickly and easily act on common attacks with out-of-the-box detections, workflows, and responses. As you mature, Splunk extends these capabilities with custom detections, deep investigations, and rich automations. Together, they deliver an agentic AI-driven SOC platform that grows with your team by boosting efficiency, visibility, and outcomes at every stage. Discover how Cisco empowers security teams from day one.