CYBER THEORY

2025 CISO Engagement and Decision Drivers Study

AI Dominates Security Content

In partnership with Cyentia Institute

Contents

Introduction

In B2B cybersecurity marketing, precision wins. This report digs into exclusive content consumption patterns, intent data, and topic engagement insights from ISMG's media network to reveal where cybersecurity buyers actually devote their attention.

From the topics that pull in CISOs to the content formats gaining traction around the world, this data-backed report breaks down what's working, what's fading, and where savvy marketers see the most impactful outcomes.

Intent data — behavioral signals that reveal what buyers are researching, when, and why — gives marketers the power to engage earlier and more effectively. It brings clarity to audience needs, campaign timing, and content strategy at every stage of the funnel.

For a more custom analysis, talk with CyberTheory. Our exclusive access to ISMG's intent and engagement data can be leveraged into more effective marketing and content strategies, delivering the results you seek.

Key findings include:

1. **AI topics drive the broadest interest.** Security audiences continue to seek out AI-themed content, especially when paired with clear use cases, industry context, and practical value.
2. **OT cybersecurity content is under-supplied.** Interaction with OT topics is high, but sponsored coverage remains limited. Vendors who move early can claim attention in a growing space.
3. **Buyers cast a wide net when researching solutions.** Most buyers are actively consuming both sponsored and non-sponsored content, including sponsored content from multiple vendors. Intent data shows what's happening behind the scenes.
4. **Webinars outperform other formats for CISOs.** When executive attention is the goal, webinars deliver. On-demand access and substantive insights drive performance across funnel stages.
5. **Podcasts and video assets build mid-funnel momentum.** Trust-building formats like expert-led videos and recurring podcast series fill a critical gap between awareness and conversion.
6. **Original research earns repeat attention, yet is underutilized.** Survey-based content remains a powerful driver of engagement. Unique data and industry insights build authority and create room for surround assets.
7. **Whitepapers remain essential for executive decision-makers.** Long-form content still plays a vital role. When positioned strategically, whitepapers support evaluation and purchase-stage decision-making.

Research Methodology

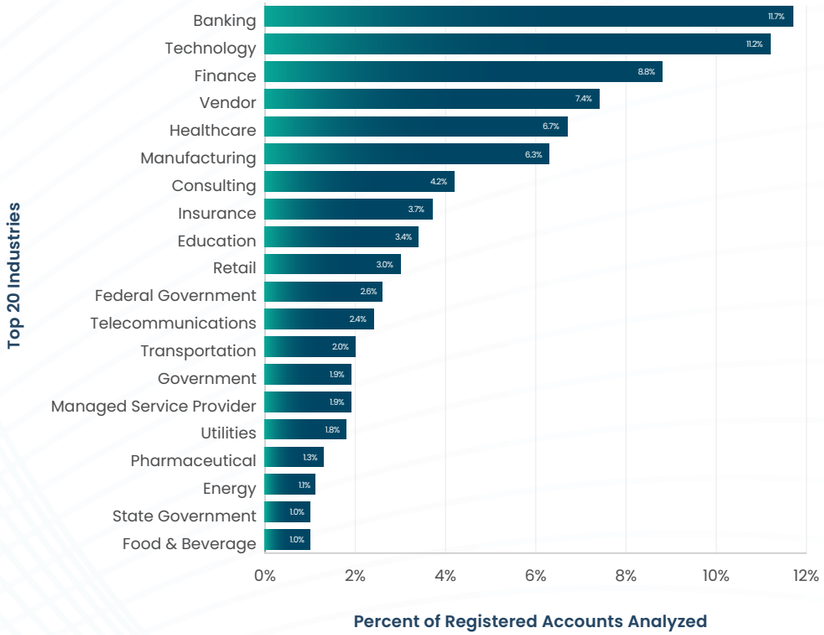
This report is based on an extensive analysis of content consumption and engagement signals from ISMG, the world's largest B2B cybersecurity media network. The dataset spans gigabytes of behavioral data and includes interactions tied to more than 300 distinct cybersecurity topics.

The insights presented here draw from five core data sources:

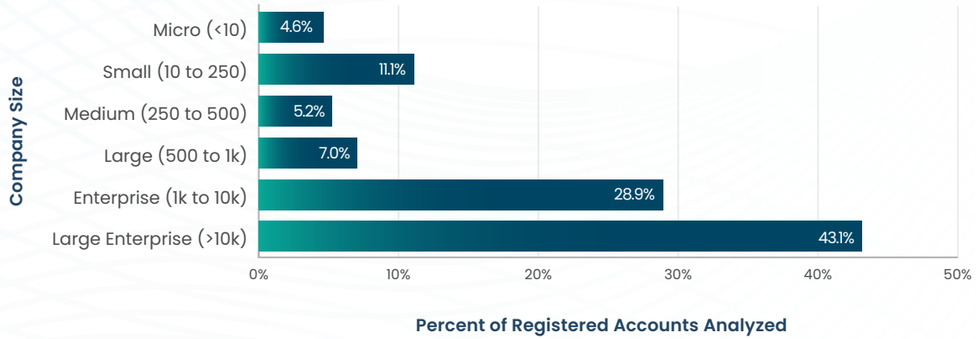
- **ISMG's Editorial Network** — Our portfolio of 38 online publications serving over 2 million cybersecurity professionals worldwide. The network averages over 50,000 unique daily visitors and hosts more than 500,000 user interactions each day.
- **ISMG Global Events** — In-person and virtual events held throughout the year, including regional summits, executive roundtables, and editorial interviews conducted live at industry events such as RSAC, InfoSec Europe, and Black Hat. Engagement data also includes OT-focused ManuSec programming.
- **CyberEdBoard Community** — A closed community of CISOs and executive-level cybersecurity leaders from more than 1,800 organizations. This group provides peer-driven insight on top-of-mind challenges and trends.
- **CyberEd.io Platform** — An education platform offering structured cybersecurity learning paths, executive training, hands-on labs, and certifications. Platform usage informs content interest trends by role and experience level.
- **CyberTheory Marketing Intelligence** — Strategic marketing insights developed by CyberTheory, informed by the same ISMG datasets used in this report. These include advisory programs focused on campaign design, demand generation, and content performance analysis.

Audience data is further analyzed by organization size, industry, region, and role. See the charts on this page reflecting the distribution of registered accounts by company size and vertical.

Industry Breakdown



Organization Size Breakdown



Section I

Content Creation & Format Trends

This section dives into evolving cybersecurity content trends, providing actionable insights for marketers by unpacking a decade's worth of asset production data. We spotlight growth in articles and video content, along with strategic opportunities emerging from our in-depth analysis of ISMG intent data. The surge in sponsored digital content, for example, underscores the importance of targeted, timely, and purposeful messaging in a saturated market.

You'll gain an understanding of seasonal patterns that drive sponsored content activity, enabling smarter planning and execution. We also highlight an untapped area of growth in operational technology (OT) cybersecurity, where editorial interest outpaces sponsored content production. Marketers positioned to fill this gap with relevant, high-value assets can secure early leadership in an increasingly critical field.

How are content asset formats changing over time?

Figure 1 shows a 235% increase in total content asset production over the past 10 years. Articles and whitepapers remain the most commonly produced formats, but video has steadily grown in volume, especially in the last three years. Podcast output, by contrast, has declined both in absolute terms and relative share. A small dip at the start of 2025 aligns with typical seasonal slowdowns seen in prior years.

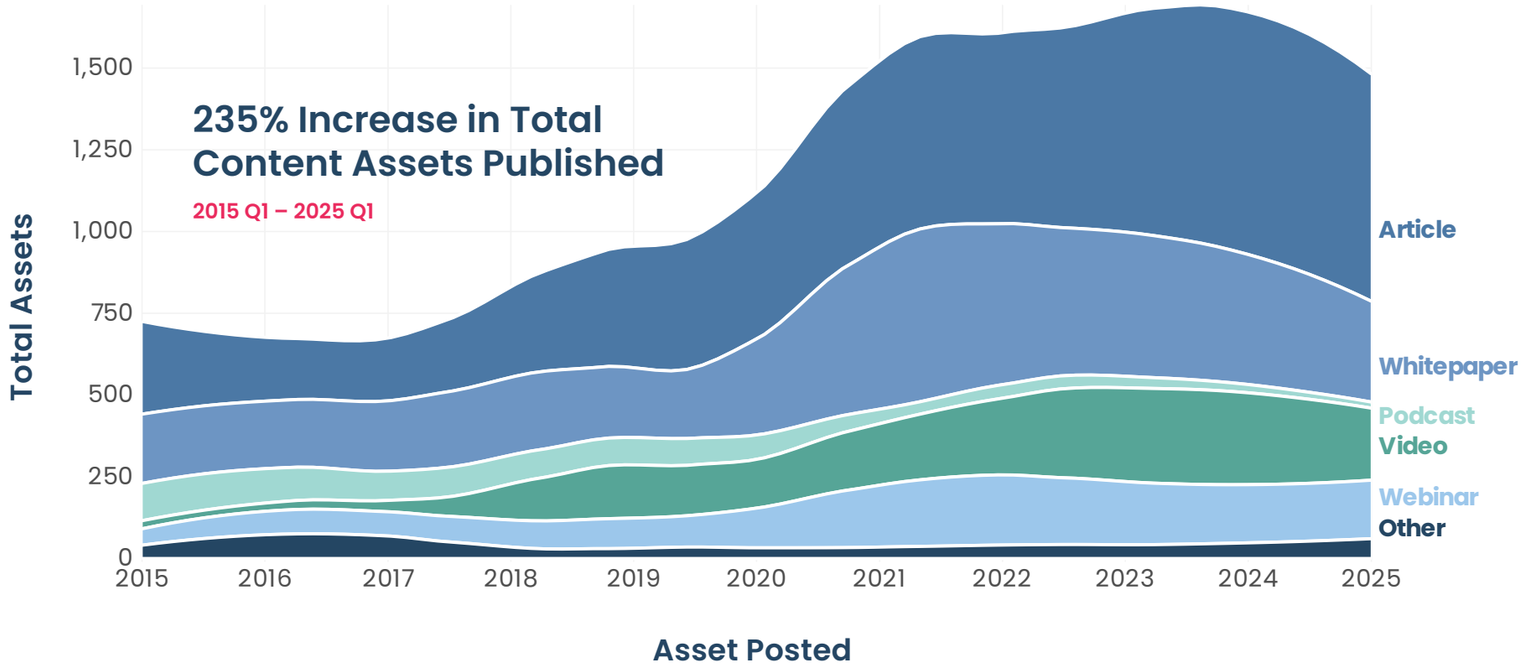


Figure 1: Asset formats by quarter (10-year view)

CyberTheory Takeaways

1. **Build content volume with purpose.** The 235% growth in asset output over 10 years reflects our now hyper-competitive content backdrop. To stay visible, cybersecurity vendors must maintain a steady cadence of new, high-quality assets that align to buyer information needs across the funnel.

2. **Reinvest in podcast strategy.** Despite strong strategic value, podcast production has declined — leaving an opening. CISOs and senior leaders value recurring formats with expert voices. A well-positioned series can fill this whitespace and establish durable thought leadership.

3. **Use video to break through early-stage noise.** Video assets have gained significant traction in recent years. Short, expert-led videos are ideal for explaining complex topics quickly and helping your brand stand out in crowded digital channels.

4. **Anchor awareness with editorial-style articles.** Articles continue to drive top-of-funnel performance. Invest in paid placement articles on trusted media properties and align article themes with high-interest intent signals to earn early-stage attention.

5. **Repurpose whitepapers for depth and reach.** While still widely used, whitepapers now compete with more flexible formats. Break long-form reports into serialized assets, combine them with webinars, or pair with interactive tools to gain additional value.

What asset formats are being produced vs. a year ago?

Figure 2 compares asset formats from Q4 2024 and Q1 2025 with the same period a year earlier. Article production continues to climb, extending a multi-year growth trend. Whitepapers declined modestly, showing a gradual shift away from traditional long-form formats. Video content showed a notable gain, while webinar volume appears to have stabilized following a pandemic-driven expansion. The broad “Other” category, including blog posts, surveys, and reports grew modestly, reflecting incremental diversification rather than breakout adoption. These trends suggest that while content mix is evolving, format preferences are not shifting dramatically.

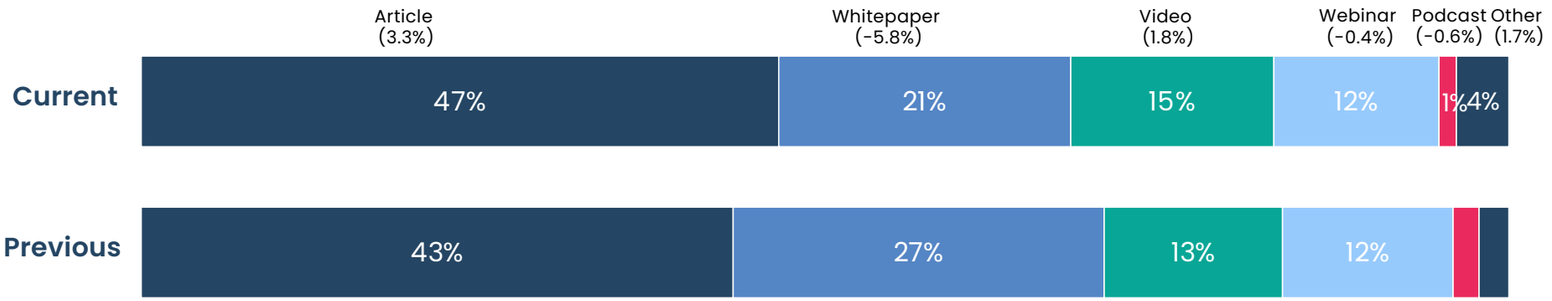


Figure 2: Asset formats Q4 2024 vs. 1 year ago

CyberTheory Takeaways

1. **Keep investing in articles, but sharpen your edge.** Rising article output makes early-stage visibility harder to earn. Strong headlines and trusted placements are now table stakes.
2. **Whitepapers remain relevant.** Once front-line lead drivers, they now work best as supporting content within multi-asset campaigns.
3. **Video is on the rise for a reason.** Buyers want quick, high-credibility content that showcases expertise. Video fills that need and drives stronger mid-funnel traction.

How popular is digital content with sponsors?

Figure 3 tracks the volume of sponsored content assets published each quarter over the past decade. The data reveals a sharp acceleration beginning in 2020, followed by a sustained high-volume phase through early 2025. While some seasonal variation is visible, quarterly production levels have not returned to pre-2020 (pre-COVID) norms, suggesting that elevated levels of sponsored content production have become the new norm.

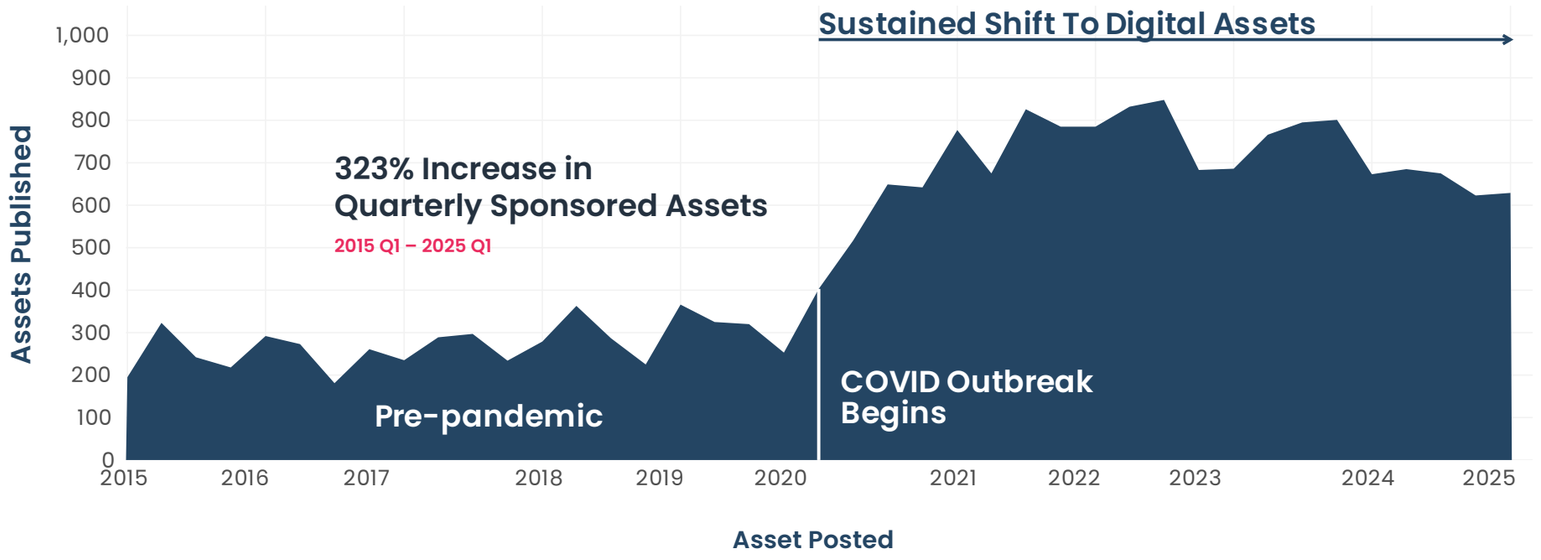


Figure 3: Sponsored assets by quarter (10-year view)

CyberTheory Takeaways

1. **Sponsored content has surged, and so has the need for better content execution.** The 10-year rise in sponsored content means standing out requires more than being present. Lead with a clear point of view that speaks to specific buyer concerns and stages.

2. **Avoid contributing to content fatigue.** With so many assets now in circulation, marketers must prioritize clarity, specificity, and usefulness. Generic messaging disappears fast — relevance and utility are now essential for engagement.

3. **Treat digital content and in-person events as complementary, not competing.** Figure 3 shows that digital output didn't drop when events returned. Plan campaigns that bridge both to drive touchpoint density and cross-channel momentum.

4. **Maximize ROI by extending the life of top-performing assets.** With production volume at record highs, it's wasteful to create one-and-done content. Repackage standout assets into new formats, gate them differently, or syndicate with fresh messaging.

5. **Challenger brands can punch above their weight.** Use differentiated formats, bold positioning, and audience egmentation, such as by industry or use case, to cut through the sponsored content volume driven by dominant players.

What proportion of assets were sponsored?

Figure 4 displays the percentage of total assets that were sponsored in Q4 2024 and Q1 2025. Sponsorship levels dipped in late Q4, reflecting a typical seasonal slowdown in sponsored assets, but users still show strong engagement with non-sponsored assets throughout December. The overall Q4 increase aligns with the end-of-year push to discharge annual budgets and meet key objectives, while a second peak in March suggests a possible tie to budget resets or new-year coordinated campaign launches. The data also reveals a pattern of irregular spikes rather than a consistent trend, highlighting the campaign-driven nature of sponsored content activity during this period. While the volume of sponsored content varies throughout the year, additional data shows the overall number of sponsors publishing remains roughly consistent. That indicates many vendors cluster their campaigns around key seasonal windows.

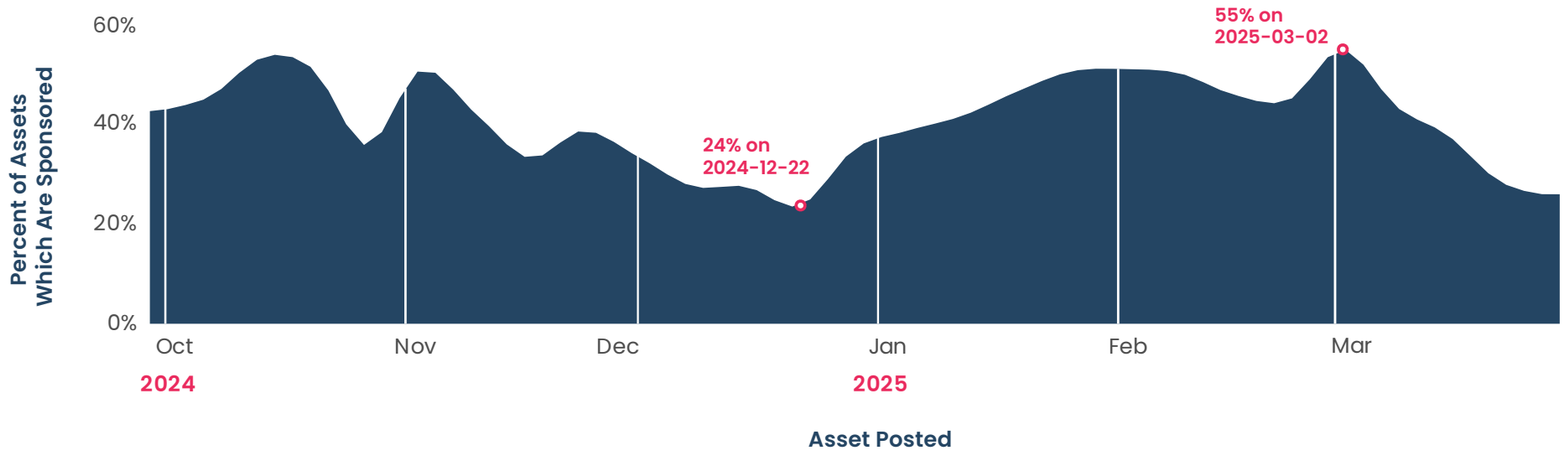


Figure 4: Percentage of assets sponsored, Q4 2024 – Q1 2025

CyberTheory Takeaways

1. **March is a prime launch window for high-priority content.** The spike in sponsored content suggests this period aligns with refreshed budgets and campaign resets, which is a smart time to release flagship assets and drive visibility.

2. **Plan ahead for October's crowded attention cycle.** Q4 consistently draws high sponsor activity as vendors leverage Cybersecurity Awareness Month in October as well as end-of-year budget cycles. To get your share, finalize assets early, secure placements, and consider high-performing topics with broad appeal.

3. **Use January for low-noise experimentation.** With fewer sponsored assets in circulation post-holidays, early Q1 offers a clean slate to test new formats, creative angles, or bolder positioning without as much competition for attention.

4. **Build for peaks, but plan for lulls.** The quarterly rhythm in Figure 4 suggests an opportunity to repurpose or resurface high-performing content during periods with less sponsored content activity, extending value while keeping interaction steady.

5. **Sustain visibility through consistent cadence.** Top-performing sponsors don't just show up during peak seasons — they publish with discipline. A steady calendar builds recognition, relevance, and reach.

How many OT cybersecurity assets are being produced?

Figure 5 compares sponsored and non-sponsored OT cybersecurity content from 2022 through Q1 2025. Non-sponsored coverage increased by 51% in 2024, with further growth in early 2025, reflecting rising editorial attention to industrial cybersecurity and critical infrastructure protection, as well as an increase in OT cybersecurity incident news. In contrast, sponsored OT content declined during the same period, marking a reversal of its prior growth trend. This divergence suggests that while public and regulatory interest in OT security is accelerating, vendor response through sponsored content has slowed, creating a gap between coverage and commercial engagement.

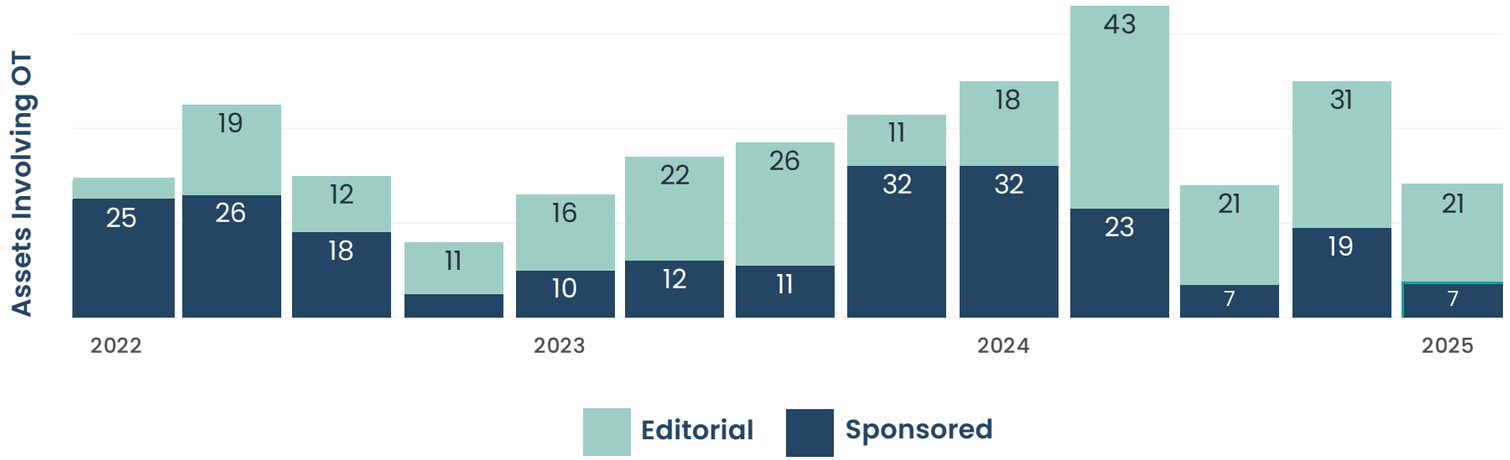


Figure 5: Sponsored and non-sponsored OT content by quarter, 2022 – Q1 2025

CyberTheory Takeaways

1. **OT cybersecurity is gaining traction in editorial channels.** Marketers should respond with content that speaks directly to this rising interest and and leverages the market opportunity to gain visibility among OT cybersecurity buyers.

2. **Regulations are raising the stakes.** Recent mandates like NIS2, SOCI, and OTCC make OT security a priority. Position your content around risk, operational continuity, and compliance.

3. **Tie OT messaging to real-world threats.** Target industries like energy, transportation, and manufacturing with tailored language and use cases.

4. **Capitalize on breaking news to promote OT content.** Editorial spikes signal audience attention. Use syndication and ads to surface your OT assets during high-interest moments, and consider deploying a rapid response content capability to publish good, related content closely timed with incidents appearing in the news.

Section II

Topic Trends & Industry Signals

This section delivers critical insights on sponsored content trends, highlighting those that are quickly gaining traction and those poised for sustained growth. Through detailed analysis of ISMG intent data, we identify sponsored cybersecurity themes that resonate with audiences and spotlight the fastest-moving topics marketers need to watch closely.

You'll discover which topics command the highest levels of audience engagement and learn how preferred asset formats differ by global regions, which can be used to inform more targeted, effective campaigns. We also explore topic preferences by industry, emphasizing the strategic importance of addressing unique concerns within each vertical.

Finally, we differentiate between today's hot topics and those with proven staying power, enabling marketers to invest strategically in content that consistently attracts audience attention and drives lasting impact.

Which sponsored topics are gaining ground?

Figure 6 compares the top sponsored content topics from two six-month periods: Q4 2024 to Q1 2025 vs. the same period one year ago. Several topics appear consistently across both periods, including cloud security and artificial intelligence. Notably, OT cybersecurity and identity and access management emerged as top-tier sponsored topics in the more recent period after ranking outside the top 15 in the prior year. Ransomware also rose significantly in rank, indicating increased sponsor attention. The all-time popularity shading shows that while some topics are consistently prominent, others are gaining momentum more recently.

One Year Ago	Rank	Past Six Months
Cloud Security	1	Cloud Security
AI-Driven Security Operations	2	Ransomware
Artificial Intelligence & Machine Learning	3	Threat Detection
Threat Intelligence	4	Artificial Intelligence & Machine Learning
Cloud Data Security & Resilience	5	Identity & Access Management
Ransomware	6	Operational Technology (OT)
Threat Detection	7	Microsoft Copilot for Security
Zero Trust	8	Threat Intelligence
Enterprise Browser Security	9	Zero Trust
Securing SaaS & Web App Workflows	10	Cloud Data Security & Resilience
IT Risk Management	11	DevSecOps
Application Security	12	Enterprise Browser Security
Network Detection & Response	13	Application Security
Security Operations Center (SOC)	14	IT Risk Management
Network Firewalls, Network Access Control	15	Remote Workforce

New top-15 topic in Q4 2024 to Q1 2025

Figure 6: Top sponsored asset topics, Q4 2024 – Q1 2025 vs. Q4 2023 – Q1 2024

CyberTheory Takeaways

1. **AI remains a top theme.** Sponsors can anchor AI messaging in defined use cases, relevant industry applications, and real-world outcomes to gain AI credibility and meet rising buyer expectations.
2. **Ransomware is gaining more attention.** A four-spot climb shows sponsors are re-engaging with this urgent topic. It pairs well with OT, cloud, or identity storylines that highlight critical risk.
3. **OT security broke into the top tier for the first time.** This marks a clear shift in sponsor awareness of industrial cybersecurity, a signal for vendors in this space to act while competition is still thin.
4. **Cloud and identity remain reliable anchor topics.** Their presence in both periods and strong all-time rankings confirm their role as go-to content themes. Refresh with new insights or formats to keep them relevant.
5. **Track topic momentum to guide content planning.** Surging topics like OT and ransomware show how fast sponsor priorities shift. Aligning campaigns with these trends can boost visibility and timing precision, so be sure to incorporate the latest topic trend intelligence into your content campaigns.

Which sponsored content topics are fastest moving?

Figure 7 highlights the fastest-rising sponsored content topics between Q4 2024 and Q1 2025 and the same period a year prior. AI-related topics remain dominant, with two ranking among the top ten movers. Other notable increases include Secure Service Edge (SSE), insider threats, and API security — reflecting sponsor interest in both emerging solutions and resurging risk areas. Several topics tied to infrastructure and tooling, such as observability and AI-based attacks, also appear among the top risers. This suggests that sponsor strategies are expanding beyond headline trends to include the supporting technologies required to implement and defend them.

Topic	Rank	Change
AI-Powered Cloud Next-Generation Firewalls	109 → 20	89
Security Service Edge (SSE)	91 → 19	72
Insider Threat	121 → 65	56
API Security	105 → 53	52
Observability	111 → 62	49
Data Privacy	85 → 44	41
AI-Based Attacks	60 → 21	39
Government	68 → 29	39
Global Compliance	70 → 33	37
Social Engineering	74 → 38	36

Figure 7: Top 10 fastest-rising sponsored topics, Q4 2024 – Q1 2025

CyberTheory Takeaways

1. **AI is on the move, but it's not alone.** Two AI topics topped the list of fastest movers, but SSE, insider threats, and API security also gained ground. Expand campaign coverage to reflect how buyers are thinking beyond AI headlines.
2. **Fast-moving topics are early indicators of sponsors' market expectations.** Monitoring topic velocity helps marketers stay one step ahead. Use this insight to align editorial calendars and thought leadership before the space becomes saturated.
3. **Insider threats and API security are having a resurgence.** These longstanding risks are regaining attention. Refresh old messaging with new context, such as AI defenses, hybrid work, third-party exposure, or identity sprawl.
4. **Observability is rising — for good reason.** It supports cloud and network resilience, application security, compliance, and more. Sponsors should lead with real-world implementation stories and use case examples to reach technical buyers and connect to broader leadership goals.
5. **Offense and defense are converging.** AI-based attacks ranked just behind AI-powered defenses. Marketers should build narratives that address both capabilities and threats to reflect how security teams actually evaluate solutions.

What topics are audiences consuming?

Figure 8 ranks the top 25 content topics by the percentage of users who interacted with them during Q4 2024 and Q1 2025, reflecting which topics resonated most widely with audiences across the reporting period. AI and machine learning had by far the highest user reach, and cloud security topics appear twice in the top six spots.

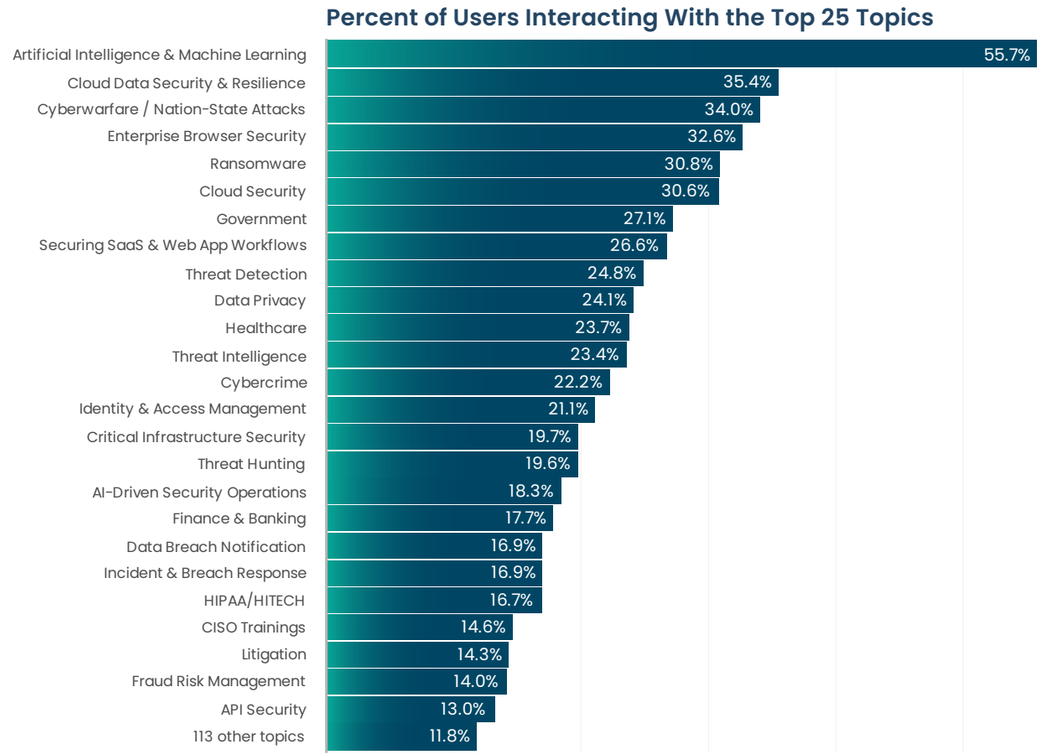


Figure 8: Percentage of audience interacting with the top 25 topics

CyberTheory Takeaways

1. **Anchor campaigns with topics reaching a high percentage of buyers.** AI and machine learning themes are safe bets for front-line messaging when reach is the goal.

2. **Classic threats still command attention.** Ransomware, cloud security, and identity remain among the most-viewed topics. Their staying power makes them ideal for reinforcing risk narratives or opening buyer conversations.

3. **Buyers are tracking both offense and defense.** AI-based threats and AI-powered protections both rank high. Don't silo your story — combine both perspectives to reflect how buyers assess risk holistically.

4. **Evergreen topics act as a perpetual traffic magnet.** Several top themes, like IAM and threat detection, have ranked highly for years. This signals that timely, high-utility content still performs.

5. **Plan for reach, then build depth.** High-reach topics pull buyers in. Use them to drive clicks, then transition to deeper mid-funnel content that educates, qualifies, and moves them forward.

What asset formats perform best in each region?

Figure 9 shows engagement with content formats across North, Central and South America, as well as EMEA and Asia-Pacific. While there are many similarities across the regions, these differences reflect some distinct format preferences which can help inform strategy. To standardize the data, the relative number of engagements for each region is scaled against North America, which has the highest engagement volume.

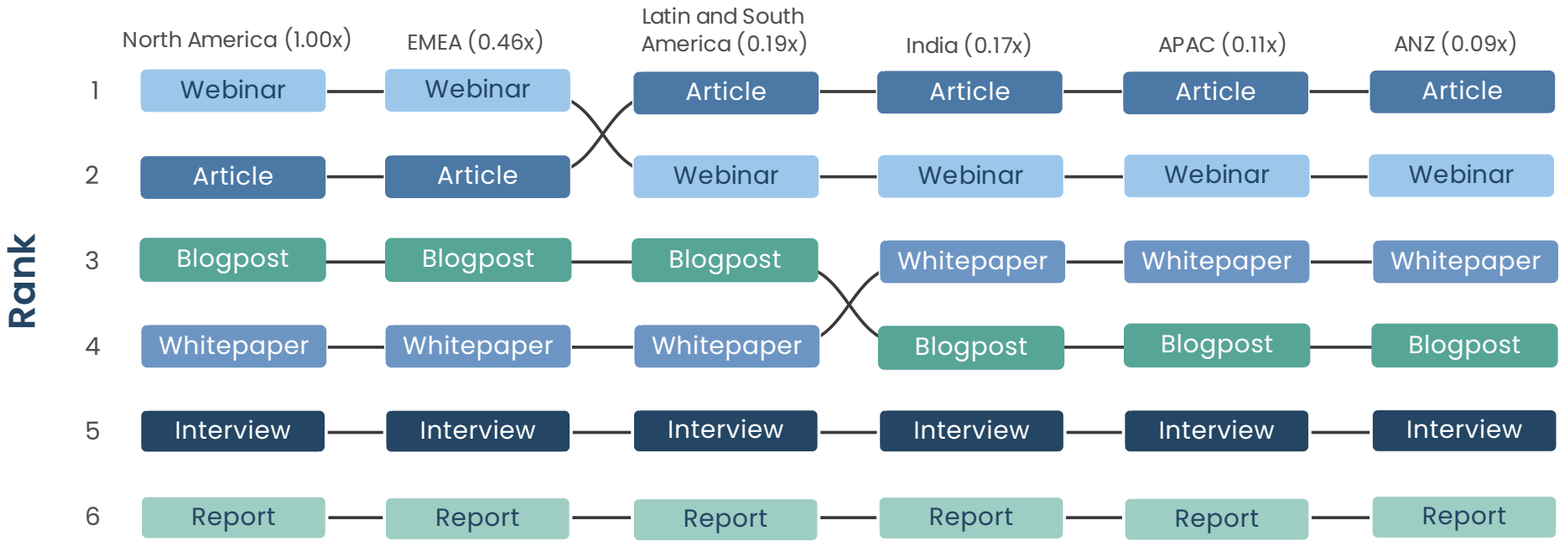


Figure 9: Top asset formats by region

CyberTheory Takeaways

1. **Top format preferences vary by region.** Those in North America and EMEA favor webinars, while articles draw the highest engagement in LATAM and Asia-Pacific regions. Users across India, APAC, and ANZ also engage more often with longer-form whitepapers, in contrast to a preference for blogs in the Americas and EMEA. Adjust global campaigns accordingly.

2. **Avoid a one-size-fits-all format strategy.** Releasing the same asset mix across all regions risks wasting effort. Instead, customize regional content by format, not just by language, to match how each region consumes information.

3. **Tailor asset reuse by region to increase efficiency and impact.** High-performing formats in one region, such as webinars in North America, can be reimagined as short videos or infographics for APAC, where mobile-friendly, digestible formats see strong uptake.

Which topics are hot in each industry?

Figure 10 shows the most frequently sponsored topics across major industry sectors. AI, cloud security, cyberwarfare, and ransomware rank highly across nearly all verticals. The chart highlights both cross-industry themes and industry-specific content focus areas.

In some cases, one industry has particularly high engagement on a topic compared to others, indicating a focus area to target with content, such as federal government users on AI-driven security operations. The insurance industry also shows high engagement across a range of topics, illustrating how those users need to monitor and understand a wide range of cyber threats and solutions for their customers.

	Industry									
	Banking	Consulting	Education	Fed Gov't	Finance	Healthcare	Insurance	Manufacturing	Retail	Technology
Artificial Intelligence & Machine Learning	65.8%	65.9%	59.5%	49.4%	60.4%	48.9%	66.8%	60.8%	57.8%	58.5%
Cloud Data Security & Resilience	36.1%	44.5%	39.3%	39.9%	38.8%	38.1%	50.2%	34.8%	41.6%	32.3%
Cyberwarfare / Nation-State Attacks	46.6%	40.4%	41.0%	28.6%	41.1%	31.7%	41.9%	40.9%	38.9%	40.2%
Ransomware	36.3%	40.0%	38.0%	27.0%	38.3%	42.1%	45.8%	29.3%	31.2%	32.6%
Cloud Security	34.8%	42.8%	35.4%	31.0%	40.1%	32.2%	46.9%	28.2%	29.0%	30.7%
Enterprise Browser Security	41.4%	35.8%	33.1%	22.8%	36.8%	30.1%	43.4%	34.7%	34.8%	30.6%
Government	29.3%	33.4%	30.6%	36.6%	30.8%	35.5%	39.1%	23.8%	24.3%	26.3%
Securing SaaS & Web App Workflows	28.2%	29.6%	30.8%	26.6%	31.9%	31.0%	42.6%	23.3%	28.3%	23.9%
Data Privacy	30.0%	31.8%	28.0%	24.6%	30.3%	31.3%	36.1%	20.7%	23.3%	25.1%
Cybercrime	26.8%	30.2%	31.9%	21.4%	27.2%	30.8%	33.0%	22.7%	24.6%	28.5%
Healthcare	28.8%	31.1%	25.8%	25.4%	30.9%	39.7%	39.3%	18.0%	20.3%	21.9%
Threat Detection	24.2%	27.5%	29.8%	26.1%	30.0%	30.1%	40.9%	22.2%	26.0%	22.5%
Threat Intelligence	25.9%	26.6%	27.8%	23.0%	30.4%	25.6%	41.4%	20.2%	23.6%	22.8%
Identity & Access Management	25.7%	27.1%	27.7%	19.5%	26.2%	24.2%	32.2%	18.8%	20.9%	20.6%
Critical Infrastructure Security	23.7%	24.4%	23.8%	21.1%	23.7%	23.9%	30.8%	18.4%	18.6%	20.9%
Threat Hunting	19.9%	21.0%	24.3%	22.4%	24.8%	20.7%	35.8%	18.2%	20.3%	18.5%
AI-Driven Security Operations	18.5%	23.9%	18.8%	29.3%	20.3%	18.4%	30.8%	14.7%	15.0%	14.8%
HIPAA/HITECH	20.4%	21.0%	20.0%	18.8%	21.2%	28.9%	25.8%	14.0%	15.1%	17.2%
Incident & Breach Response	19.4%	23.5%	25.0%	13.2%	19.9%	19.5%	23.8%	18.0%	19.6%	21.7%
Finance & Banking	30.3%	23.7%	22.8%	7.6%	27.6%	12.4%	28.2%	17.1%	18.7%	20.0%
Fraud Risk Management	24.4%	17.4%	17.4%	9.8%	24.8%	12.9%	25.2%	12.4%	13.7%	15.7%

Figure 10: Hot topics by industry

CyberTheory Takeaways

1. **AI leads in all industries.** The imperative for marketers is clear: create content that provides value to cybersecurity buyers around the topic of AI.
2. **Leverage other high-performing industry / topic combinations.** While AI, identity, and ransomware have wide appeal, industries also reward content that reflects their use cases, specific risks, and organizational priorities.
3. **Use identity as a bridge theme.** It performs across all industries and connects easily to cloud, Zero Trust, fraud, and compliance. Shape identity-focused content around role-specific pain points to deepen impact.
4. **Verticalized messaging beats broad positioning.** A topic like AI takes on different meaning in healthcare vs. financial services. Anchor messaging in industry-specific use cases, risks, and regulatory concerns to earn buyer trust.

What topics matter to critical infrastructure industries?

Figure 11 shows topics with the highest user engagement among the top 10 critical infrastructure industries over a six-month period. Once again, the AI/ML topic leads the way overall, as organizations seek efficiencies and AI-backed defensive capabilities while guarding against AI-driven threats. Cyberwarfare, ransomware, and cybercrime also ranked in the top 10 topics, underlining the importance for critical infrastructure organizations to address those persistent threats that can lead to costly operational disruption.

Some industries also showed outsized engagement on specific topic clusters compared to other sectors. For example, financial services companies (banking and finance) operate in a highly regulated industry, and they engaged more often than others with content on fraud risk management and identity & access management, indicating unique pain points to address.

Top 10 Critical Infrastructure Sectors

	Overall	Banking	Education	Energy	Fed Gov't	Finance	Healthcare	Manufactoring	Telecomunications	Transportation	Utilities
Artificial Intelligence & Machine Learning	59.6%	65.8%	59.5%	66.1%	49.4%	60.4%	48.9%	60.8%	61.2%	64.5%	64.7%
Cyberwarfare / Nation-State Attacks	41.0%	46.6%	41.0%	45.5%	28.6%	41.1%	31.7%	40.9%	42.9%	47.9%	44.6%
Cloud Data Security & Resilience	36.6%	36.1%	39.3%	39.2%	39.9%	38.8%	38.1%	34.8%	25.0%	32.0%	41.2%
Ransomware	35.1%	36.3%	38.0%	34.7%	27.0%	38.3%	42.1%	29.3%	22.8%	30.6%	36.8%
Cloud Security	33.0%	34.8%	35.4%	27.2%	31.0%	40.1%	32.2%	28.2%	22.7%	27.9%	32.5%
Enterprise Browser Security	35.2%	41.4%	33.1%	41.5%	22.8%	36.8%	30.1%	34.7%	33.4%	40.9%	36.3%
Government	29.6%	29.3%	30.6%	27.4%	36.6%	30.8%	35.5%	23.8%	18.5%	22.3%	30.2%
Securing SaaS & Web App Workflows	27.5%	28.2%	30.8%	23.7%	26.6%	31.9%	31.0%	23.3%	15.2%	21.6%	27.9%
Cybercrime	26.7%	26.8%	31.9%	25.4%	21.4%	27.2%	30.8%	22.7%	19.0%	22.8%	28.9%
Data Privacy	27.0%	30.0%	28.0%	24.4%	24.6%	30.3%	31.3%	20.7%	17.0%	20.1%	26.6%
Threat Detection	26.0%	24.2%	29.8%	24.0%	26.1%	30.0%	30.1%	22.2%	17.8%	21.1%	27.8%
Threat Intelligence	25.1%	25.9%	27.8%	23.1%	23.0%	30.4%	25.6%	20.2%	16.6%	20.7%	29.1%
Healthcare	27.0%	28.8%	25.8%	22.4%	25.4%	30.9%	39.7%	18.0%	12.3%	17.8%	23.3%
Identity & Access Management	23.3%	25.7%	27.7%	23.9%	19.5%	26.2%	24.2%	18.8%	14.6%	19.3%	25.2%
Critical Infrastructure Security	22.2%	23.7%	23.8%	23.1%	21.1%	23.7%	23.9%	18.4%	13.9%	18.2%	24.6%
Threat Hunting	20.8%	19.9%	24.3%	19.9%	22.4%	24.8%	20.7%	18.2%	13.8%	17.6%	23.7%
Incident & Breach Response	19.7%	19.4%	25.0%	21.9%	13.2%	19.9%	19.5%	18.0%	15.2%	19.5%	24.2%
HIPAA/HITECH	19.4%	20.4%	20.0%	16.1%	18.8%	21.2%	28.9%	14.0%	8.6%	12.3%	17.4%
Finance & Banking	21.0%	30.3%	22.8%	20.3%	7.6%	27.6%	12.4%	17.1%	13.3%	17.6%	20.0%
AI-Driven Security Operations	17.8%	18.5%	18.8%	14.0%	29.3%	20.3%	18.4%	14.7%	8.4%	14.5%	15.3%
Fraud Risk Management	17.8%	24.4%	17.4%	14.7%	9.8%	24.8%	12.9%	12.4%	9.9%	13.2%	16.8%

Figure 11: Hot topics among selected critical infrastructure industries

CyberTheory Takeaways

1. **AI and cyberwarfare/nation-state attacks lead critical infrastructure concerns.** Content creators in these industries should show how their solutions address these issues to boost visibility and engagement.

2. **Ransomware is getting added interest in healthcare.** Sponsors can differentiate their solutions by tying ransomware prevention, identity, access, and detection strategies directly to patient safety and operational continuity.

3. **Tailor threat narratives to each industry's blind spots.** The same risk — like ransomware — carries different stakes in healthcare vs. transportation. Reframing familiar threats for sector-specific impact creates relevance buyers can't ignore.

4. **Highly-regulated industries present ready content opportunities.** Tie critical infrastructure compliance mandates such as NIS2, OTCC, SOCI, and NERC CIP, to the broader, high-interest topics to increase relevance.

5. **Speak to cybersecurity buyer needs around IT/OT convergence.** As topic rankings show, today's critical infrastructure CISOs need integrated security across both IT and OT environments. Help guide the conversation through supporting content.

What topics are hot today and which ones have staying power?

Figure 12 compares topic popularity in Q4 2024 and Q1 2025 against all-time activity, using a quadrant view. The top left highlights newly popular topics, such as AI-driven security operations and cloud security, which surged recently but have lower historical presence. The top right quadrant includes evergreen topics like ransomware and cybercrime that perform consistently well over time as well as in recent quarters. Topics lower on the chart rank lower in recent engagement. It's important to watch topic trends over time, as new topic entrants may take 12 months or more to demonstrate their performance.

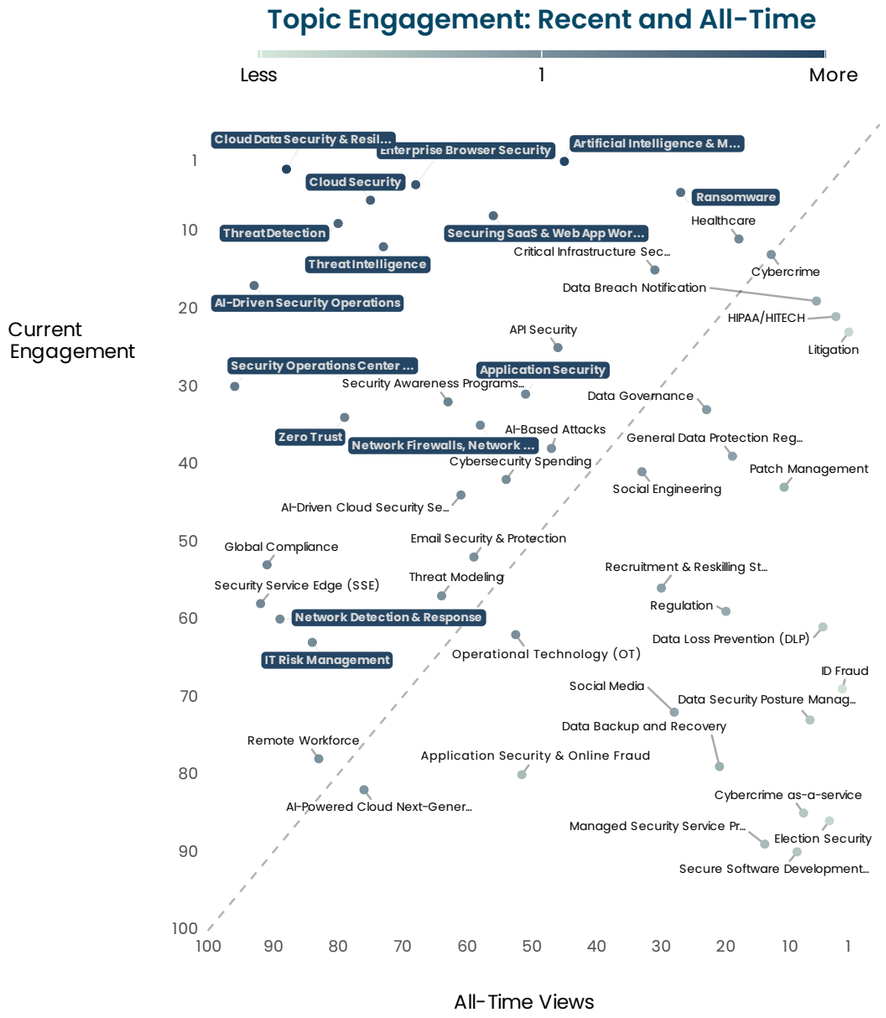


Figure 12: Hot topics in Q4 2024 – Q1 2025 vs. all-time

CyberTheory Takeaways

1. **Watch the top-left quadrant for rising opportunities.** Topics like AI-driven SecOps and cloud data security are gaining traction now but haven't yet saturated the field. Acting early here allows proactive sponsors to shape the narrative.

2. **Don't drop your evergreen winners.** Cybercrime and ransomware remain top performers over time. Use them to drive traffic and tie in newer themes without sacrificing reach.

3. **Declining interest doesn't mean no value.** Risk, governance, and fraud topics have slipped in ranking. That creates space to reposition them with fresh angles tied to AI, regulation, or operational resilience.

4. **Balance your content assets by topic maturity.** Pair hot, emergent themes with tried-and-true performers. This blend draws attention while supporting different buyer stages and messaging objectives.

5. **Quadrant-based planning beats guesswork.** This chart can guide asset strategy. Build momentum in the "newly hot" space, sustain volume in the top-right, and re-evaluate spend on themes falling off the radar.

What asset titles resonate most?

Figure 13 highlights the sponsored content assets with the highest engagement during the reporting period, ranked by title. High-performing assets often referenced timely topics, such as AI-powered security and synthetic (AI-created) media. Several titles included practical framing or audience-specific targeting, such as “threat detection” or insights for a specific industry or region. The data reflects patterns in topic urgency and headline structure that drive interaction.

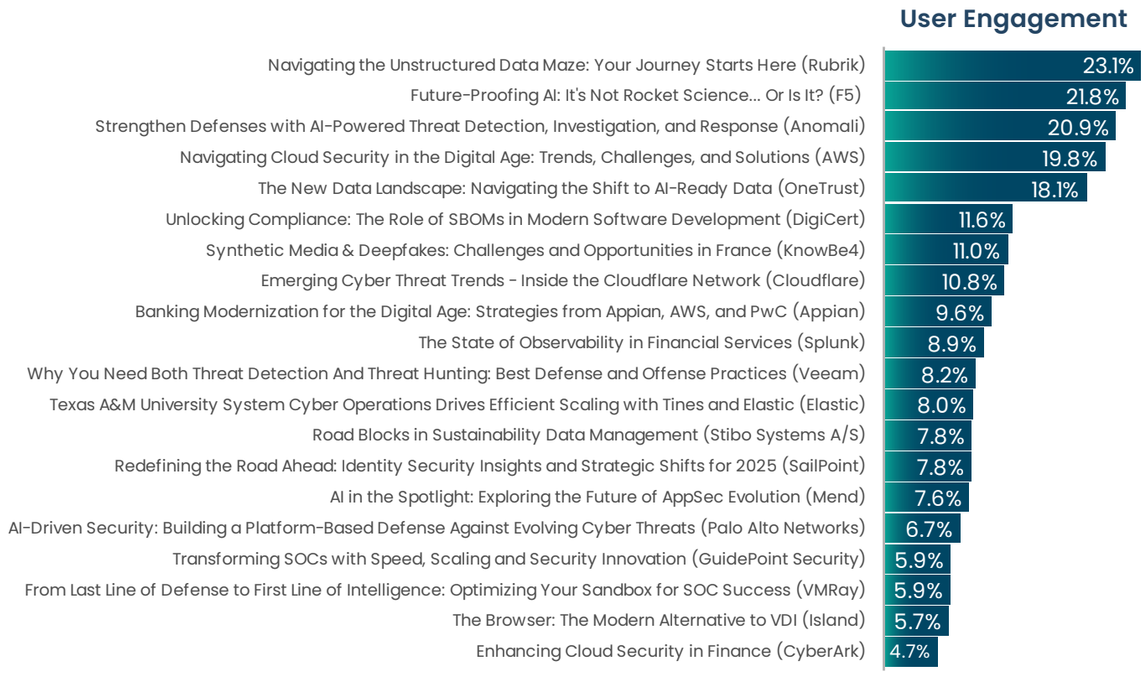


Figure 13: Top sponsored asset titles by engagement

CyberTheory Takeaways

1. **AI sells.** The best-performing titles often include terms about AI and related considerations, like “AI-powered threat detection,” “AI-driven security,” and “AI-ready data.”

2. **Titles with clear audience targeting outperform.** Assets that reference topics of known interest to security leaders earned more interest. Call out the topics of interest and personas of your intended readers to increase connection and credibility.

3. **Data-driven framing adds weight.** Buyers trust content that signals evidence — not just opinion. Anchor high-level themes about threats and trends using real-world data.

4. **Use practical formats to earn clicks.** Lists, frameworks, and how-to phrases (e.g., “5 ways to improve...”) drive curiosity and show value fast. Use this structure in both educational and mid-funnel content.

5. **Position content with clarity, not cleverness.** Top titles favor clarity over wordplay. Avoid vague or branded phrasing. Instead, focus on buyer priorities, pressing threats, and the direct value of what’s inside.

Section III

CISO Preferences & Persona Engagement

In this section, we zero in on what resonates with CISOs and other key personas. By analyzing their engagement levels with various sponsored asset titles, we uncover the language and themes most effective at capturing executive attention.

We also pinpoint which content formats drive the greatest engagement among CISOs compared to broader audiences, enabling marketers to better align asset creation with executive preferences. Separately, we identify the top-performing individual assets among CISOs, offering tangible examples of successful content strategies.

Finally, we present an account-based marketing (ABM) view, illustrating how different roles within a single organization engage distinctly with various content formats, providing invaluable data for tailoring outreach and maximizing content effectiveness across buying groups.

Which asset formats are preferred by CISOs?

Figure 14 compares average engagement by asset format between CISOs vs. the broader cybersecurity audience. Webinars and whitepapers show higher traction among CISOs compared to the broader audience, while webinars and articles performed highest with CISOs overall. The data suggests that senior executives favor content formats that offer depth, structure, and context over brevity.

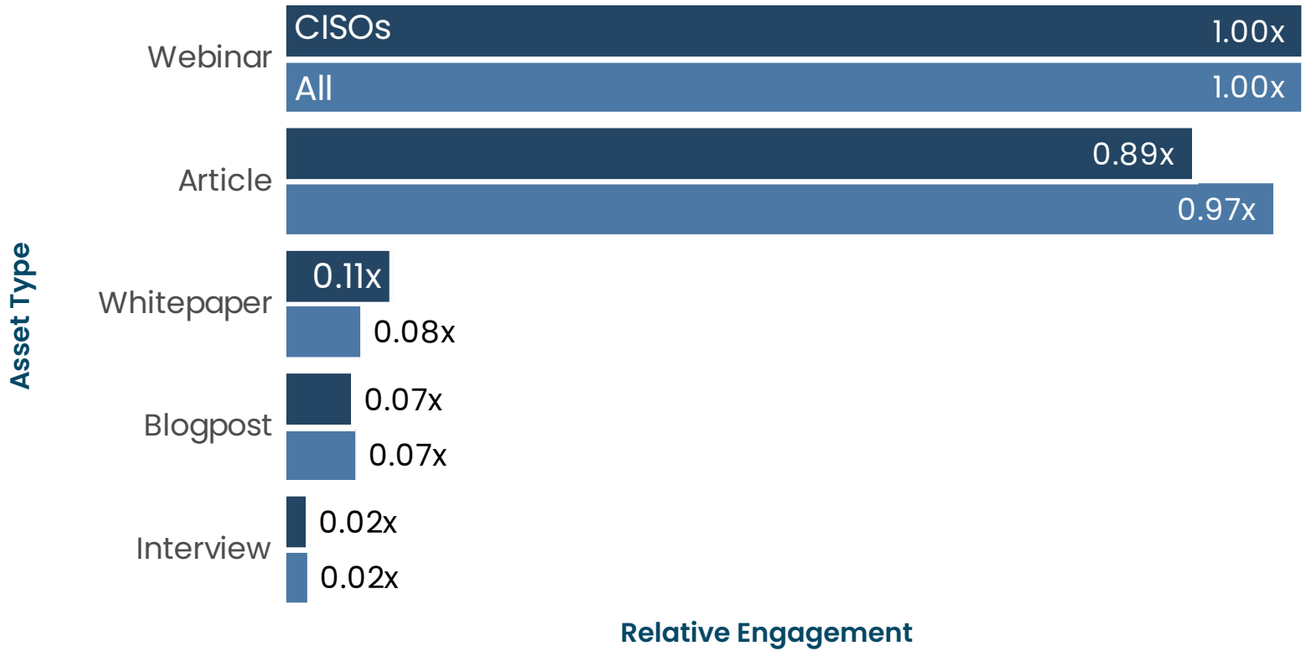


Figure 14: Engagement by asset format, CISO vs. all

CyberTheory Takeaways

1. **Webinars and articles win with CISOs.** These formats earned the highest executive interaction. Use them to deliver in-depth insights, clear solutions to pain points, and other strategic messaging.

2. **Use short-form assets to drive CISOs to long-form content.** Infographics, checklists, and short articles work best as entry points in social media, email and ungated website content. Use them to capture top-of-funnel attention and lead to higher performing long-form content.

3. **Apply persona insights to asset format strategies.** When planning content campaigns and deciding which types of assets to build, use asset-type engagement data by role, not just by buyer journey stage, to gain a competitive edge.

Which specific asset titles are getting the most CISO attention?

Figure 15 ranks the top 25 content assets by engagement among CISOs. The highest-performing titles frequently reference executive priorities, frameworks, and high-impact threats. AI-driven security themes are also well represented. The data highlights which topics and title structures are most effective at capturing senior-level attention.

1.	Securing the Digital Core by Activating Strategic Levers
2.	Navigating the Evolving SIEM Landscape: Key Insights and Strategic Integrations
3.	Banking Modernization for the Digital Age: Strategies from Appian, AWS, and PwC
4.	Navigating the Unstructured Data Maze: Your Journey Starts Here
5.	OnDemand: Road Blocks in Sustainability Data Management
6.	The CISO's Guide to a Strong Security Culture
7.	The State of Observability in Financial Services
8.	The New Data Landscape: Navigating the Shift to AI-Ready Data
9.	Cyber Incident Response: Recovery and Review
10.	Redefining the Road Ahead: Identity Security Insights and Strategic Shifts for 2025
11.	Unlocking Compliance: The Role of SBOMs in Modern Software Development
12.	Runtime and Punishment: AI Models vs. Emerging Threats
13.	AI-Driven Security: Building a Platform-Based Defense Against Evolving Cyber Threats
14.	Transforming SOCs with Speed, Scaling and Security Innovation
15.	From Risky to Resilient: Proactive Strategies for Program De-Risking and Audit Readiness
16.	AI in the Spotlight: Exploring the Future of AppSec Evolution
17.	Future-Proofing AI: It's Not Rocket Science... Or Is It?
18.	Synthetic Media & Deepfakes: Challenges and Opportunities in France
19.	Strengthen Defenses with AI-Powered Threat Detection, Investigation, and Response
20.	Why You Need Both Threat Detection And Threat Hunting: Best Defense and Offense Practices
21.	SaaS Data Protection: Are You Covered?
22.	API Security Matters: The Risks of Turning a Blind Eye
23.	Texas A&M University System Cyber Operations Drives Efficient Scaling with Tines and Elastic
24.	Emerging Cyber Threat Trends - Inside the Cloudflare Network
25.	Navigating Cloud Security in the Digital Age: Trends, Challenges, and Solutions

Figure 15: Top 25 assets popular with CISOs

CyberTheory Takeaways

1. **Lead with strategic language.** Titles referencing frameworks, executive priorities, or board-level concerns performed best. For CISO audiences, framing matters as much as the topic.

2. **AI topics appear repeatedly on the list.** These themes earned the highest engagement. Use them to introduce broader narratives around resilience, modernization, or incident response.

3. **Avoid tactical or feature-focused titles.** CISOs engage with content that supports big-picture thinking. Position assets as decision-making tools — not product explainers.

4. **Use proven title styles to inform headline strategy, then refine for your brand.** The highest-performing CISO-facing assets follow recognizable headline patterns. Model your content on those structures, then sharpen messaging with your unique POV and buyer focus.

What roles engage with various asset formats in a single account?

Figure 16 examines content engagement patterns by role and format in a single top-10 global financial institution over a 12-month period, from mid-2024 to mid-2025. The analysis is based on activity from 186 subscribers in this account, and it highlights how different organizational roles engage with sponsored versus non-sponsored content. Senior-level roles, including VPs and C-level executives, show distinct preferences, particularly favoring non-sponsored (editorial) articles. The overall data reveals a much higher level of interaction with non-sponsored content, which accounts for 580 views compared to 43 views for sponsored assets. This disparity underscores the importance of measuring target account engagement across all content consumption when the focus is on reaching key accounts, such as in ABM strategies.

	C-Level	Director	Manager	Staff	VP	Total
Sponsored						
Whitepaper Downloads	3	0	0	5	12	20
Webinar Attendance	10	2	0	1	10	23
Total	13	2	0	6	22	43
Non-Sponsored						
Articles Views	181	107	55	10	170	523
Roundtable Registration	1	2	5	0	0	8
Interview Access	0	0	0	1	1	2
Custom Event Registration	0	0	5	0	1	6
Blog Views	12	11	2	0	10	35
Summit Registration	1	0	1	0	4	6
Total	195	120	68	11	186	580

Figure 16: ABM view of asset format engagement by role

CyberTheory Takeaways

1. **Prioritize contact-level insights over account-level intent data.** Account activity alone can be misleading. Tracking individual interaction — across sponsored, editorial, and event formats — reveals who's active, what they care about, and when to act.

2. **Don't overlook non-sponsored content.** In this account, non-sponsored assets earned more than 13 times the engagement of sponsored ones. Editorial behavior provides early-stage signals that can shape messaging, targeting, and outreach strategy. Invest in a solid PR program to grow visibility and uptake in editorial channels.

3. **Tailor content and outreach by role.** C-level and VP contacts consistently engaged with editorial articles. These roles track industry developments and scan headlines, making them highly responsive to native content and adjacent ad placements.

Section IV

Intent Data, AI Trends & Buyer Behavior

This section explores the impact of AI on cybersecurity content trends, offering strategic marketing insights derived from detailed intent data analysis. We look at how AI-related content production has surged since 2022, with recent engagement trends signaling areas of peak interest and evolving priorities among buyers.

We also spotlight content topics driving the highest engagement in small and medium-sized businesses (SMBs), helping marketers tailor campaigns to resonate with this critical audience segment.

In addition, we examine the correlation between event attendance and content engagement within organizations, highlighting how targeted event strategies can amplify marketing outcomes. Engagement patterns across IT and operational technology (OT) topics are also compared to identify nuanced differences in buyer behavior.

Lastly, we assess user engagement with sponsored versus editorial content, revealing opportunities for marketers to leverage intent signals for more effective outreach and lead nurturing.

How has AI-related content performed since 2022?

Figure 17 tracks the volume of AI-related sponsored and non-sponsored content assets published quarterly from 2022 through early 2025. The chart shows three distinct phases of growth: steady adoption in 2022, a sharp acceleration beginning in Q2 2023, and a sustained high-volume plateau through 2024 and into 2025. This pattern indicates long-term investment in AI-themed content and, based on engagement trends observed in earlier figures, continued opportunity for strategic expansion.

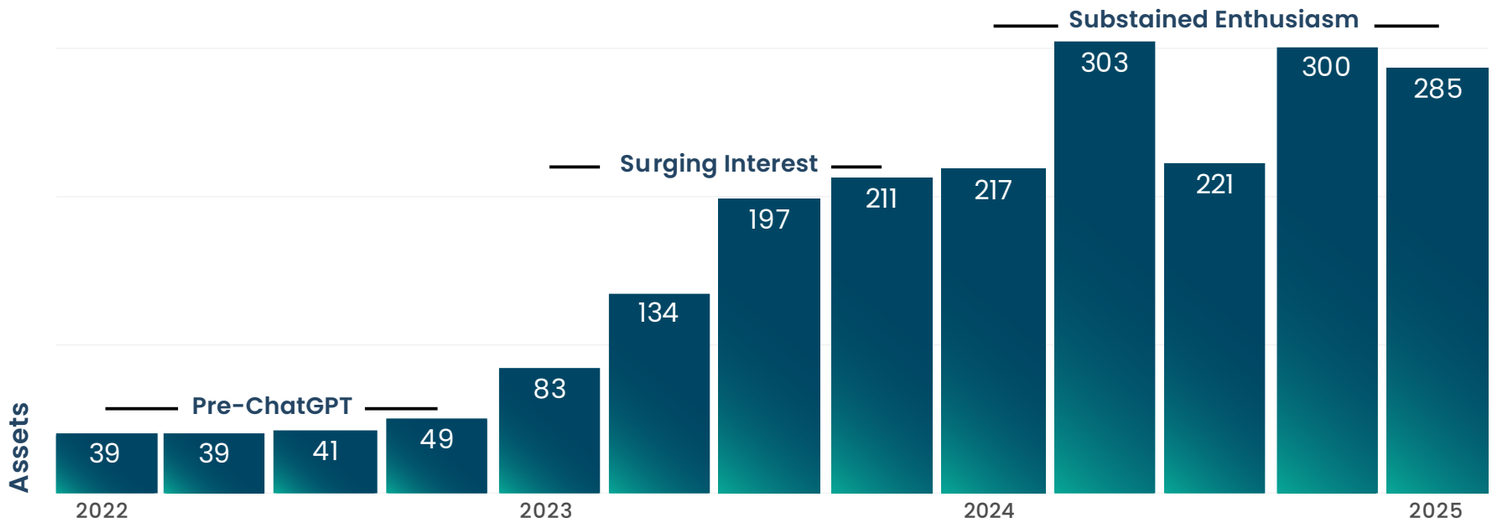


Figure 17: AI content assets by quarter, 2022–25

CyberTheory Takeaways

1. **AI is the backbone of security marketing today.** AI content volume increased more than sixfold from 2022 to 2024. Every major vendor now plays in this space, whether through AI solutions directly or adjacent capabilities. Producing AI content is ‘cybersecurity marketing 101’ in 2025.

2. **Ensure new AI content stands out.** With production at an all-time high, sponsors need a sharper point of view that includes vertical industry relevance, specific use cases, or other credible differentiation.

3. **Missed the initial AI wave?** If you’re entering the AI conversation now, go specific. Focus on secure AI pipelines, SOC automation, next-generation firewalls, or other use cases becoming more standardized. Develop original research and analyses tied to real-world outcomes. Associate AI with other high performing topics that offer a unique point of view.

How has engagement with AI-related content changed recently?

Figure 18 tracks weekly engagement with AI-related content from Q4 2024 through Q1 2025. Engagement went through peaks and valleys throughout the period, with a pronounced spike in February. This surge coincides with notable AI product launches and market events, indicating that timely developments can sharply elevate user interest. Interaction with AI content peaked mid-quarter, with weekly variation suggesting interest is cyclical. Overall, the data reflects sustained demand for AI-themed content.

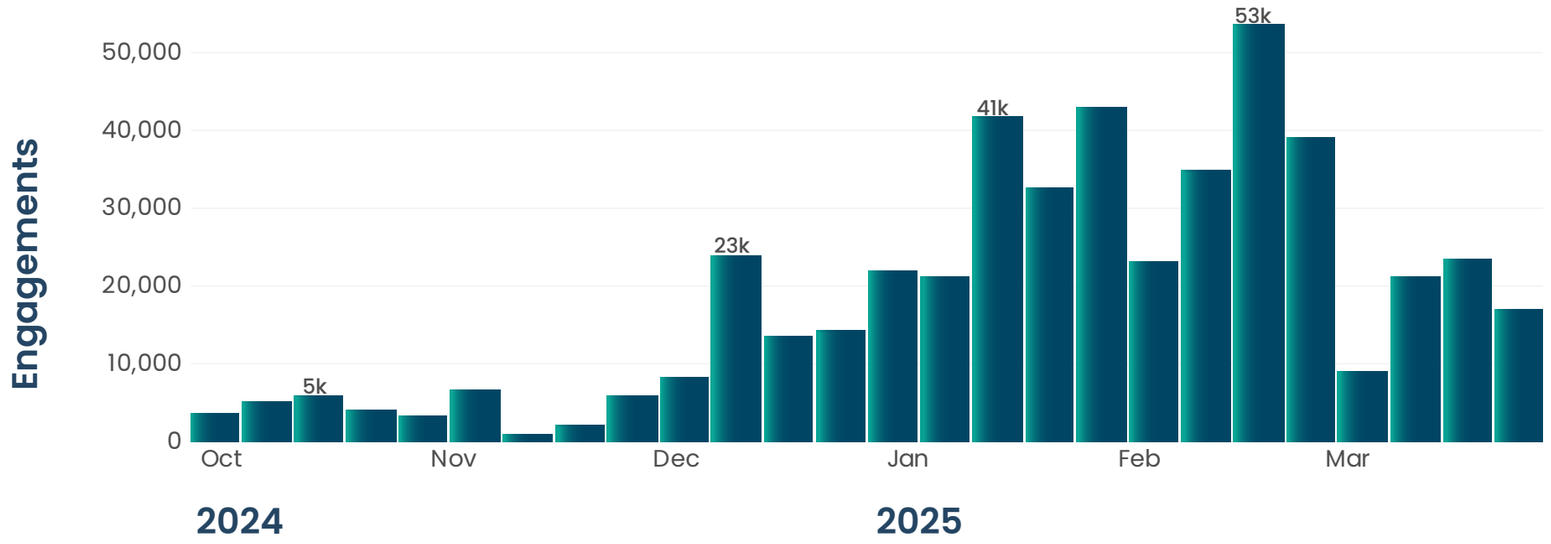


Figure 18: AI content engagement by week, Q4 2024 – Q1 2025

CyberTheory Takeaways

1. **Capitalize on event-driven momentum.** February's spike followed DeepSeek's R1 chatbot launch and ISMG's virtual summit on AI and cybersecurity. Time your campaigns around industry moments — and be ready to move fast when new catalysts emerge.

2. **Don't have an AI product?** Lead with insight. Use thought leadership surveys to uncover your audience's AI priorities and pain points. This data can power high-value content that drives engagement and positions your brand as a trusted voice in the space.

3. **Map your AI content to buyer needs.** Generic narratives fall flat. Explore how AI applies to detection, automation, compliance, or operational outcomes, and use that framing to engage buyers with clear problems to solve.

What topics see the highest engagement from small and medium-sized businesses?

Figure 19 ranks the top 25 content topics by engagement among small and mid-sized business users, defined here as organizations with 500 or fewer employees. AI-related topics lead the list, signaling that SMBs are actively exploring how AI can impact their operations and defenses. Other topics of high SMB engagement include ransomware and threat detection, underscoring strong interest in practical, operational security themes. While the report focuses on the top 25 topics, more than 100 others fall below the 3% engagement threshold, highlighting how concentrated SMB attention is on this core set.

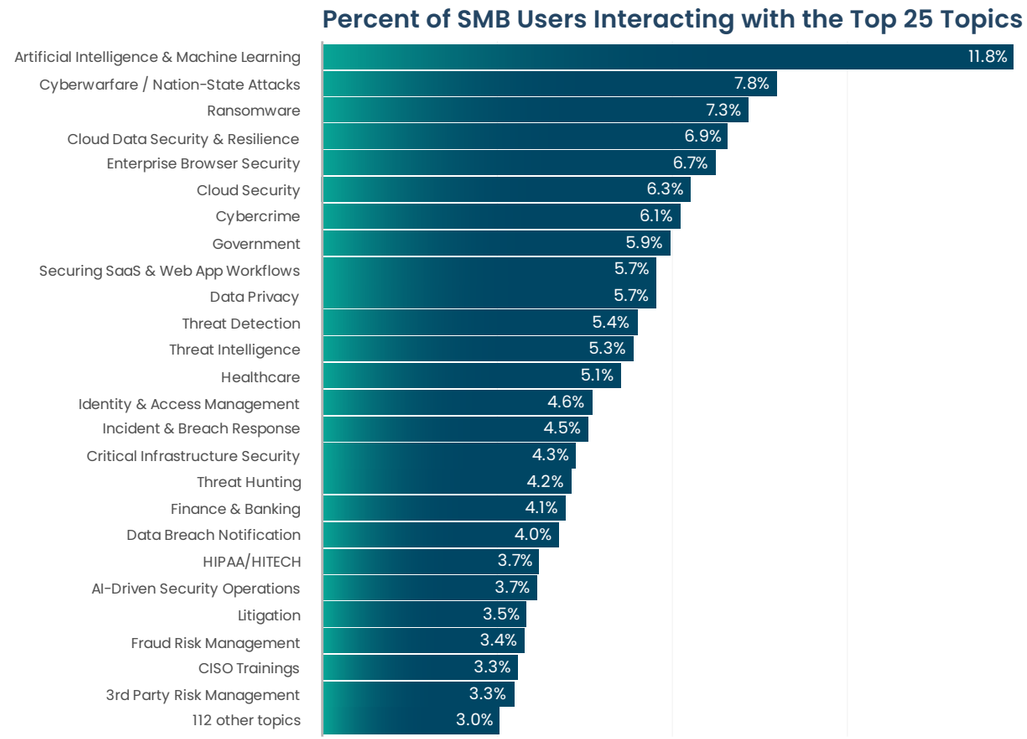


Figure 19: Top 25 topics by SMB user engagement

CyberTheory Takeaways

1. **SMBs are highly engaged in AI but need relatable use cases.** Position AI through scenarios SMBs face daily: phishing detection, endpoint automation, and risk alerts. Practicality drives interaction in this segment.
2. **SMBs engage with content that solves immediate problems.** Focus messaging on risks that directly affect daily operations.
3. **Ransomware is a universal entry point.** It has high engagement among SMBs and across companies of all sizes. Use it to open conversations with SMBs — then extend into practical mitigation guidance.
4. **Make content easy to act on.** SMB teams are often lean and resource-constrained. Assets that offer simple checklists, tools, or tactical advice perform better than conceptual whitepapers.
5. **Avoid abstract frameworks and boardroom strategy.** SMB buyers show low interest in governance and strategic planning content. Save those topics for enterprise audiences and keep SMB assets practical.

How does event attendance impact content engagement in an organization?

Figure 20 examines patterns in event attendance and engagement at the organizational level. Many sponsored events are attended by multiple users from the same company. When one or more individuals from an organization participate, average engagement across the organization increases significantly. This pattern suggests that attendance correlates with deeper or more sustained interaction.

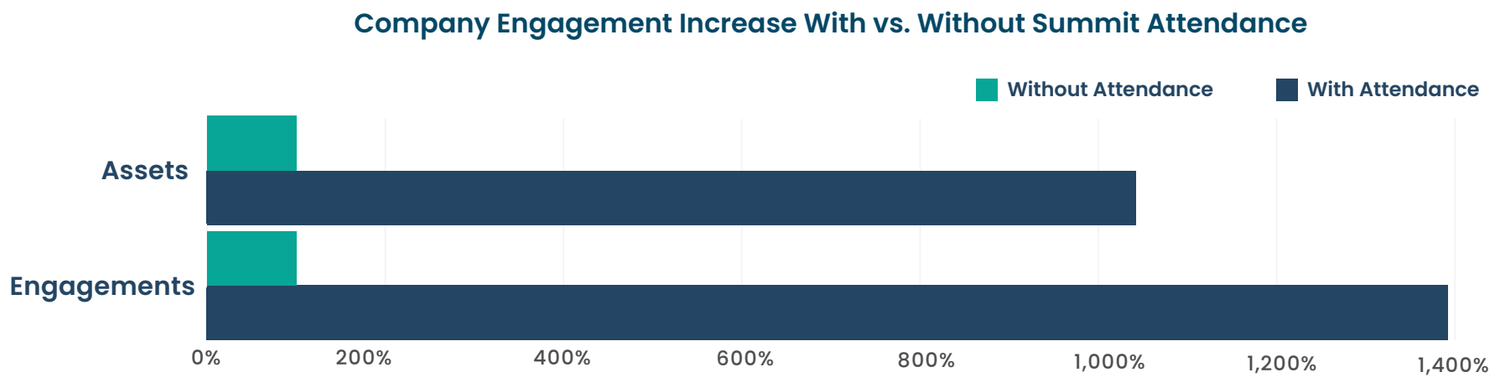


Figure 20: Comparing companies with at least 1 event attendee vs. those with no event attendees

CyberTheory Takeaways

1. **Asset and overall engagement increase impressively with event attendance.** This is an "ABM strategy in a box:" sponsor events, drive key account targets to attend (with VIP travel packages if needed), then double down on promoting relevant content across those organizations' buying committees afterward.

2. **Coordinate follow-up across titles.** If a security architect and an executive both attend, tailor your outreach accordingly. Multi-role participation is enhanced by tailoring content to role levels.

3. **Design events with team value in mind.** If multiple attendees improve outcomes, create experiences worth sharing internally — such as executive Q&As, practical downloads, or post-event toolkits.

How does engagement with IT and OT topics compare?

Figure 21 compares audience engagement across content focused on IT versus OT security topics. This view is limited to users who have engaged with four or more OT assets, helping to isolate those with sustained interest in operational technology. Despite representing a smaller share of total asset volume, OT-related content generates significantly higher average engagement. These users also show strong interest in adjacent topics such as AI/ML, ransomware, cloud security and cybercrime. The data suggests that OT-focused users, while having distinct priorities, respond to content that bridges both technical and regulatory dimensions.

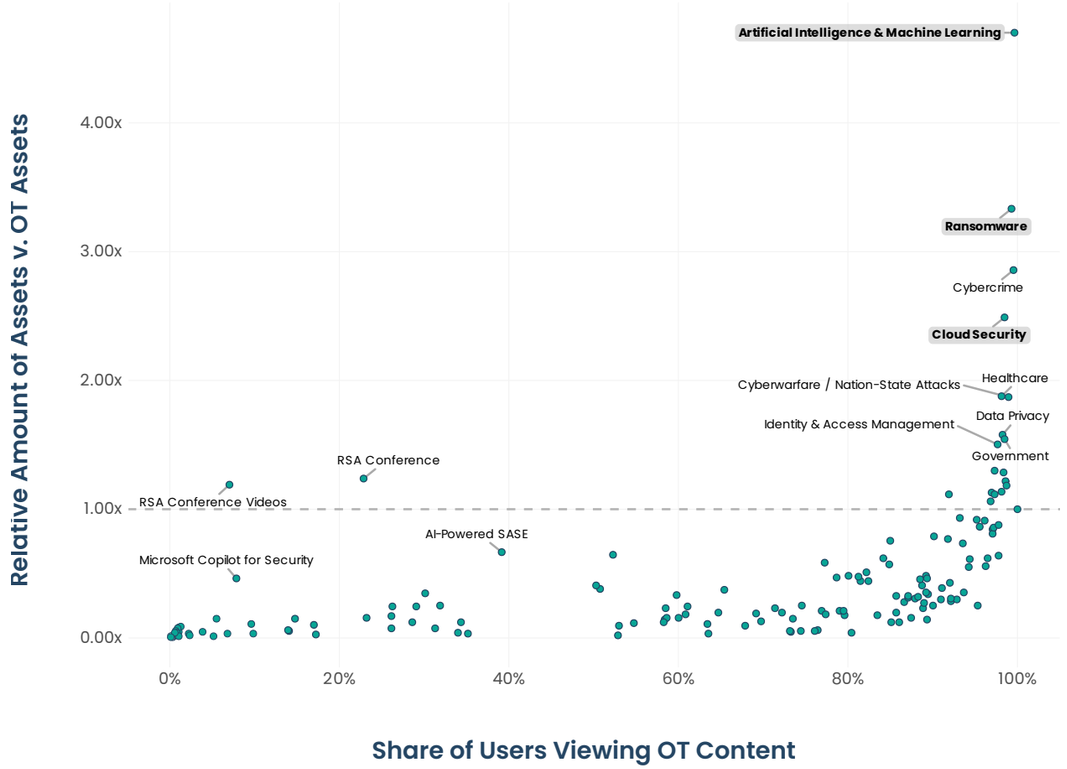


Figure 21: Engagement with IT and OT content topics

CyberTheory Takeaways

1. **AI is a gateway topic.** OT users heavily engage with AI/ML themes. Content that explores AI's impact on OT security, from anomaly detection to automation, can lift engagement and signal forward-thinking strategy.

2. **Unify your messaging across IT and OT.** OT-engaged users also consume non-OT content topics, such as privacy and healthcare. Bridging silos can increase relevance and reflect the way security teams evaluate threats across environments.

3. **OT content earns more attention per asset.** Despite a lower volume of content, OT topics generate higher interest than their IT counterparts. The demand is there — the content coverage isn't.

4. **Anchor OT content in real-world risks.** High-performing OT assets focus on specific threats like asset visibility, ransomware, and control system vulnerabilities. Leave behind vague positioning in favor of operational relevance.

Does daily user engagement differ for sponsored vs. non-sponsored editorial content?

Figure 22 shows an example of how a sponsor sees engagement activity on their own sponsored assets, as represented above the line. However, they don't see engagement with all other assets on that topic across the ISMG network, shown below the line. In this case, that unseen activity comprised 73% of engagement on the "security operations" topic during Q4 2024. Without leveraging intent data, three out of four user engagements on that topic would remain invisible to the company in this example.

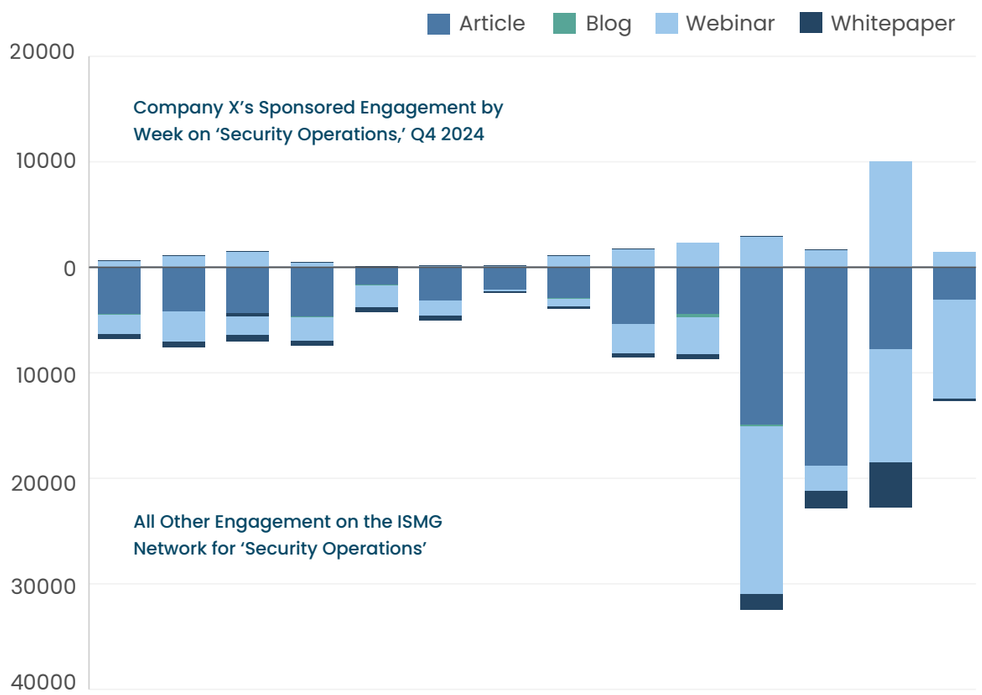


Figure 22: Engagement with sponsored vs. non-sponsored assets

CyberTheory Takeaways

1. **Use intent data to spot unseen opportunities.** Non-sponsored content drives significant interaction and reveals what buyers are engaging with beyond your brand. Shape smarter go-to-market strategies by leveraging these intent signals to identify high-performing content strategies and to find buyers currently shopping for your solution category.

2. **Turn intent signals into tailored outreach.** Use contact-level intent data from editorial articles and other non-sponsored content to personalize nurture streams, guide follow-up messaging, and map emerging buying groups.

3. **Make your sponsored content count.** Your sponsored marketing assets, while seen less often than the rest, are your chance to convert topic interest into excitement about your particular solution. Ensure your assets deliver unique value, offer useful and prescriptive insight, and stand out through smart creative and buyer-centric messaging.

Looking Ahead

To stay competitive, cybersecurity vendors must act on real buyer behavior — not outdated assumptions. This report highlights where attention flows, but success depends on what you do next.

The most effective marketing teams use contact-level signals to tailor campaigns, fine-tune timing, and sharpen messaging. These insights drive impact because they reflect what buyers are actually doing now.

CyberTheory works with cybersecurity marketers to turn this intelligence into action. From shaping strategy to amplifying execution, we partner with teams to close the gap between buyer signals and business outcomes.

Takeaways To Apply Immediately

1. **Use intent data to drive decisions.** Target topics, formats, and prospects based on real buyer behavior.
2. **Anchor content to high-performing themes.** Focus on AI, OT, ransomware, cloud security, and other topics already earning attention.
3. **Tailor format to role and funnel stage.** Match format strategy to decision-maker needs — not just content length or cost.
4. **Add context buyers care about.** Use customer stories, timely incidents, or real-world outcomes to improve relevance.
5. **Invest in formats that build trust.** Video, podcast, and survey-based assets help brands educate and differentiate.
6. **Use credible platforms to build trust.** Editorial context and expert voices help content stand out and stick.
7. **Make the most of what you already have.** Break up large assets, repurpose content, and build series to stretch your investment.
8. **Extend campaign impact after events.** Promote content to engaged attendees and their teams once the event ends.

To request a private briefing or talk strategy with our team, reach out at info@cybertheory.io.

About CyberTheory

CyberTheory is a marketing advisory firm built for cybersecurity. We help vendors turn market signals into strategy, campaigns into results, and content into conversations that matter. We support some of the world's largest cybersecurity and IT solution providers with end-to-end strategy, content, media planning, tactical execution, and more. Visit CyberTheory.io today.

About Cyentia Institute

Cyentia Institute delivers high-integrity, high-quality, data-driven research which provides meaningful marketing content for clients to drive sales and attain greater visibility in competitive markets. Cyentia's partnership with ISMG provides robust, data-based research and analysis to help the cybersecurity community reduce risks and confront the latest threats.