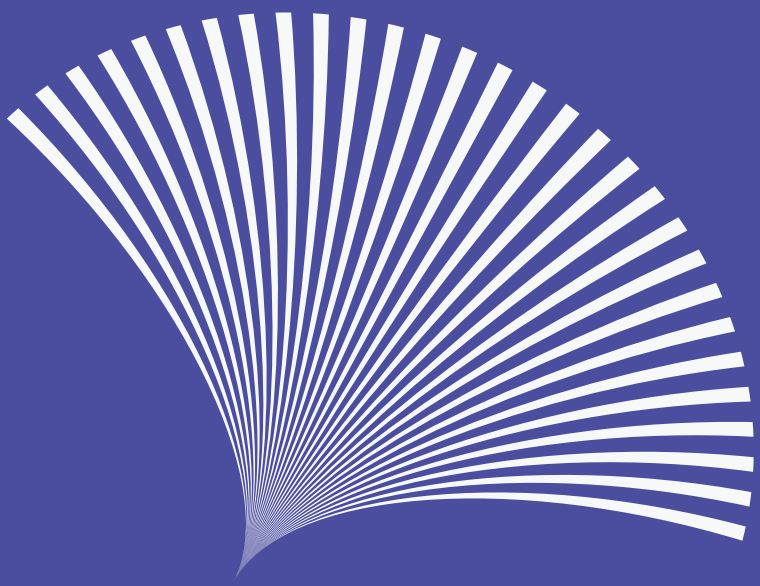
The Cybersecurity Observatory Journal

Inaugural Issue
Volume 1, Issue 1 (June 2026)



Publisher : THE Cybersecurity Observatory Institute
Editor-in-Chief: Bruce ZHANG
Advisory Board: Xiaosheng TAN, Jon XU
Editorial Team: Erin Li

Contact
Email: info@the-coi.org
Website: www.the-coi.org

Publication Policies

Ethics Statement
This journal adheres to recognized standards of publication ethics and integrity.

Disclaimer
The views expressed in this publication are those of the authors and do not necessarily reflect those of the publisher.

Contents


THE
COI
Cybersecurity
Observatory
Institute

About THE COI

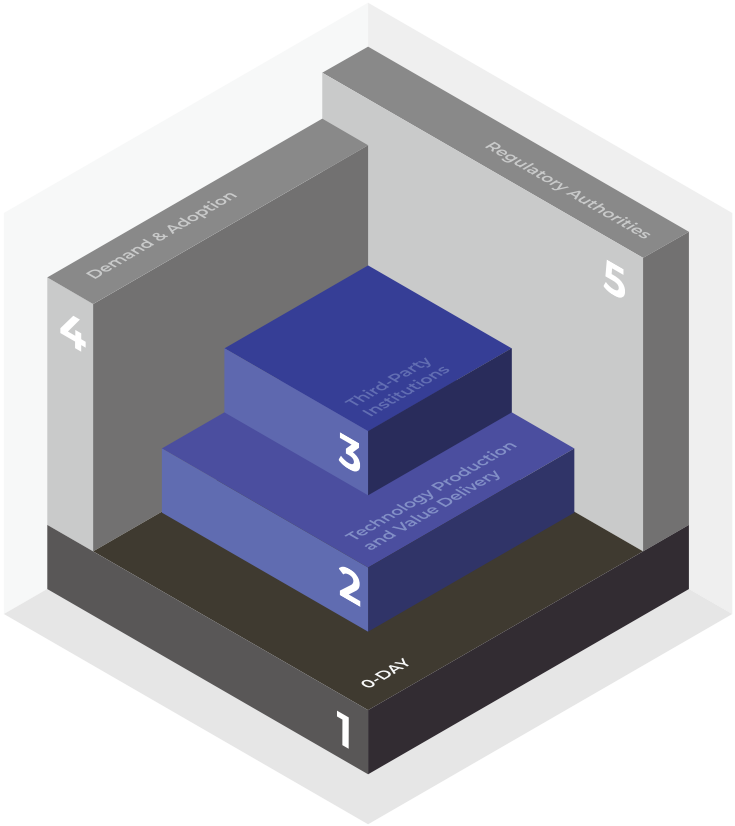
THE COI (Cybersecurity Observatory Institute) is an independent, non-profit research institute dedicated to the sustained observation and systematic epistemic study of the global cybersecurity ecosystem as a structured, multi-layered industry.

Established for academic and public-interest purposes, THE COI does not engage in vulnerability trading, technology production, commercial services, or compliance enforcement. Instead, it operates as a neutral observatory—examining how cybersecurity capabilities are generated, commercialized, institutionalized, and governed across different sectors and jurisdictions.

By systematically mapping actors, roles, and interactions across the sectors of cybersecurity, THE COI develops analytical frameworks, ecosystem models, and research outputs intended to support informed decision-making by users, institutions, and policymakers.

THE COI is independent by structure.

Its role is not to participate, but to observe, study, and clarify the complexities of an evolving global cybersecurity landscape.


Demand & Adoption
4
Regulatory Authorities
5
Third-Party Institutions
3
Technology Production and Value Delivery
2
0-DAY
1

THE COI
Cybersecurity Industry Observation Framework

01 Framework Rationale

Cybersecurity is not a singular technical domain, but a complex ecosystem jointly shaped by resources, technologies, institutions, demand, and governance. As cybersecurity capabilities continue to be produced, traded, deployed, and governed on a global scale, the field has increasingly evolved into an industry characterized by differentiated roles, functional specialization, and cross-domain interaction.

THE COI develops this Cybersecurity Industry Observation Framework not to impose a normative definition or value judgment on the industry, but to offer a structured approach to observation and analysis—one that enables a clearer understanding of how different roles emerge, operate, and relate to one another within the cybersecurity ecosystem. We hold that meaningful understanding of complex systems requires explicit role differentiation; such differentiation is not intended to freeze reality, but to make relationships visible, differences comparable, and evolution intelligible.

Within this framework, THE COI abstracts the cybersecurity industry into a set of core categories, which serve as foundational reference points for observing how the ecosystem functions. These categories are not meant to represent the singular or essential identity of real-world organizations. Rather, they describe the functional roles that entities assume in specific contexts. A single actor may span multiple categories across different phases or situations, and its actions may therefore carry layered meanings.

At the same time, THE COI recognizes that relationships within the cybersecurity industry are inherently multidimensional. Technical, commercial, institutional, cultural, and political dynamics are often interwoven, and their expressions vary across time, geography, and analytical perspective. This framework does not seek to reduce such complexity, but instead aims to provide a basis upon which complexity can be examined, compared, and discussed.

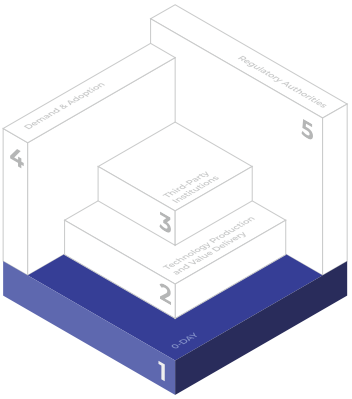
Based on this rationale, THE COI proposes a cybersecurity industry observation framework composed of five core categories. The following sections define each category, clarify their analytical boundaries, and outline the perspectives through which they are examined.

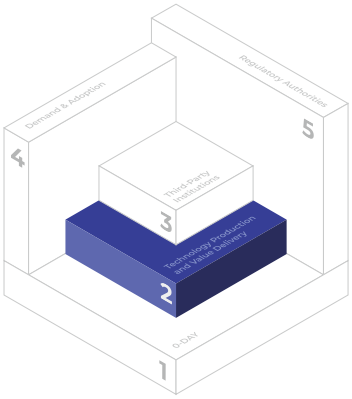
02 Definition of the Research Object

Category 1:
Zero-Day (Primary Sector)

Following the economic system analogy, the primary category corresponds to raw resources of the original world, such as coal or oil in the physical economy. In the cybersecurity industry, “Category 1: Zero-Day,” as defined in this report, refers to vulnerabilities that remain in their primordial state, yet uninstrumentalized and outside institutionalized management.

Any further evolution or intervention applied to these raw resources—whether through validation, trading, tooling, defensive deployment, or regulatory, governance, and other forms of institutional counteraction—marks their transition from a primordial state into other dimensions of the industrial ecosystem, gradually becoming operable, institutionally manageable, and governable resource elements.





Category 2:
Technology Production and Value Delivery (Secondary Sector)

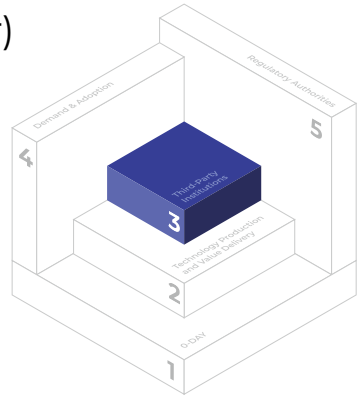
In the cybersecurity industry, the secondary category refers to the industrial system that transforms technological capabilities into products, tools, services, or financial instruments, and delivers them commercially to end users. The ecosystem includes not only technology developers and manufacturers, but also all derivative actors who convey value to clients—such as sales, integration and system assembly, delivery and implementation, and all supporting structures that facilitate value realization.

Technology itself is morally neutral, yet it empowers its users. The ultimate purpose of the secondary sector is to enable end users to realize the full value of technological capabilities. However, as user needs and objectives vary, the selection and application of specific technologies likewise differ—whether commercial or political, whether just or malicious, the realization of value ultimately depends on the intent of the user.

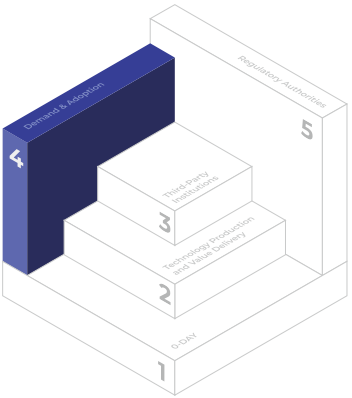
Category 3:
Third-Party Institutions (Tertiary Sector)

In the global cybersecurity market, there is no singular ultimate arbiter. Countless third-party institutions continuously emit judgment signals through their own symbolic systems. These signals are repeatedly referenced and cross-validated within the market, gradually coalescing into a distributed expert trust system, which ultimately converges into actual commercial choices and decisions.

“Third-party institutions,” as defined in this report, are independent organizations or systems that do not directly provide products or services, but through institutionalized mechanisms actively articulate knowledge, judgments, and opinions, producing outputs that are recognized, referenced, and materially influence vendor assessment, trust formation, and business decisions.

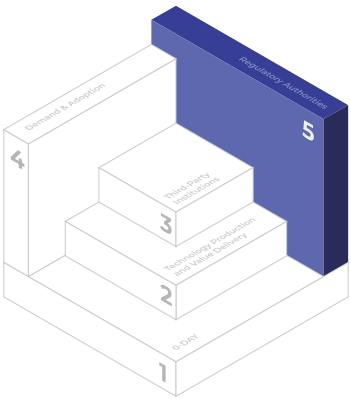


Category 4:
Demand & Adoption



Within the cybersecurity ecosystem, the fourth category refers to technology demanders and end users, understood as a macro-level user collective, with a highly diverse global distribution. Users can be categorized by country or region, or by industry characteristics; they may also be classified as critical infrastructure based on their socio-economic impact. Moreover, depending on their political or commercial objectives, as well as lawful or illicit intentions, demanders exhibit diverse characteristics.

Not all technological demands are met. The choices of demanders drive technological iteration and industrial development, while their usage simultaneously validates the advancement, maturity, and practical value of technologies, serving as an indispensable feedback and value assessment mechanism within the technological ecosystem, and representing the value pathway through which cybersecurity technologies reintegrate into the mainstream social system.



Category 5:
Regulatory Authorities

Within the cybersecurity ecosystem, the fifth category refers to regulatory institutions with clearly defined jurisdictional authority and enforcement capability across national, regional, or industry dimensions. Globally, these institutions coordinate through mechanisms of collaboration and interaction to continuously monitor development trends and challenges across the industry, implementing governance and regulatory measures to maintain ecosystem order and systemic stability.

Regulatory institutions not only establish rules but also, through supervision, coordination, and guidance, influence technological application, industrial behavior, and societal value realization, serving as an indispensable institutional pillar within the cybersecurity ecosystem, while also driving the development and evolution of both industry and ecosystem.

03 Notes

1. Role Multiplicity and Analytical Perspective

It should be noted that certain institutions exhibit role multiplicity within the cybersecurity ecosystem, with their functions and behaviors often spanning multiple categories. For example, regulatory authorities classified under Category Five frequently also act as government demand-side entities under Category Four. Similarly, telecommunications operators may function both as direct users of cybersecurity technologies and as Category Two actors involved in system integration and solution delivery.

Within this framework, classification is not intended to define an institution's singular or essential identity, but to distinguish the functional roles it assumes in specific contexts. Accordingly, analysis assigns institutions to different categories based on their situational roles, rather than imposing a static or exclusive classification.

2. The Non-Attribution of Individuals

This framework does not assign categorical attribution to individuals themselves. The underlying rationale is that individuals constitute highly fluid variables rather than stable industrial roles. A person's skills, identities, and behaviors may fall into different categories depending on time, context, and mode of engagement.

For instance, a highly skilled security researcher may, during working hours, operate as part of an enterprise or government demand-side organization under Category Four, or as an employee of a technology vendor under Category Two, conducting compliant research and development. Outside formal work contexts, the same individual's technical activities may fall within Category One, involving the discovery and analysis of Zero-Day vulnerabilities, and in some cases, their circulation

Rethinking The Secondary Sector Of Cybersecurity Industry

01 About Secondary Sector

Category 2: **Technology Production and Value Delivery** (Secondary Sector)

In the cybersecurity industry, the secondary category refers to the industrial system that transforms technological capabilities into products, tools, services, or financial instruments, and delivers them commercially to end users. The ecosystem includes not only technology developers and manufacturers, but also all derivative actors who convey value to clients—such as sales, integration and system assembly, delivery and implementation, and all supporting structures that facilitate value realization.

Technology itself is morally neutral, yet it empowers its users. The ultimate purpose of the secondary sector is to enable end users to realize the full value of technological capabilities. However, as user needs and objectives vary, the selection and application of specific technologies likewise differ—whether commercial or political, whether just or malicious, the realization of value ultimately depends on the intent of the user.

THE COI
Cybersecurity Observatory Institute

Category 2
SECONDARY SECTOR

TECHNOLOGY PRODUCTION and VALUE DELIVERY

2.1 Tech Products

2.1A By Tech Scenarios

- 2.1A.1 Risk & Compliance
- 2.1A.2 Application Security
- 2.1A.3 AI Security
- 2.1A.4 Data & Privacy
- 2.1A.5 Security Ops & Incident Response
- 2.1A.6 Cloud Security
- 2.1A.7 Identity Security
- 2.1A.8 Endpoint Security
- 2.1A.9 Network Security
- 2.1A.10 Cryptography
- 2.1A.11 Vulnerability Management
- 2.1A.12 Threat Intelligence
- 2.1A.13 Infrastructure Security

2.1B By Business Scenarios

- 2.1B.1 ICS/OT Security
- 2.1B.2 IOT Security
- 2.1B.3 Defense Tech
- 2.1B.4 Railway/Traffic Security
- 2.1B.5 Water Security
- 2.1B.6 Vessel/Maritime Security
- 2.1B.7 Healthcare/IoMT Security
- 2.1B.8 Aerospace/Aviation Security
- 2.1B.9 Satellite/Space Security
- 2.1B.10 Media Security
- 2.1B.11 Industry 4.0 Security
- 2.1B.12 Video Surveillance/Network Security
- 2.1B.13 Automotive Security
- 2.1B.14 Power/Grid/Electricity Security
- 2.1B.15 Petrochemical Security
- 2.1B.16 Business-Critical Application Security
- 2.1B.17 Web3/Metaverse Security

2.1C By Threat Scenarios

- 2.1C.1 Anti-Virus
- 2.1C.2 Anti-Malware
- 2.1C.3 Anti-Web Defacement
- 2.1C.4 Anti-Phishing
- 2.1C.5 Anti-Fraud
- 2.1C.6 Anti-DDoS
- 2.1C.7 Anti-Money Laundering
- 2.1C.8 Anti-Ransomware
- 2.1C.9 Anti-Bot
- 2.1C.10 Anti-DeepFake
- 2.1C.11 TSCM

2.2 Professional Services

2.2.1 Readiness & Preparedness

- 2.2.1.1 Tabletop Exercise
- 2.2.1.2 Security Awareness Training
- 2.2.1.3 Executive Cyber Workshop
- 2.2.1.4 Crisis Simulation

2.2.2 Offensive & Defensive Testing

- 2.2.2.1 Penetration Testing
- 2.2.2.2 Red/Blue Team
- 2.2.2.3 CTF

2.2.3 Incident Response & Recovery

- 2.2.3.1 Incident Response
- 2.2.3.2 Digital Forensics
- 2.2.3.3 Ransomware Negotiation Support

2.2.4 Security Operation

- 2.2.4.1 SOC
- 2.2.4.2 MSSP
- 2.2.4.3 MDR

2.3 Financial Services

2.3.1 Insurance & Risk Transfer

- 2.3.1.1 Cyber Insurance
- 2.3.1.2 Reinsurance
- 2.3.1.3 ILS / Cat Bonds

2.3.2 Risk Financing & Liquidity

- 2.3.2.1 Contingent Credit
- 2.3.2.2 Captive Insurance
- 2.3.2.3 Parametric Financing

2.3.3 Loss Recovery & Compensation

- 2.3.3.1 Asset Recovery
- 2.3.3.2 Claims & Subrogation
- 2.3.3.3 Guarantees & Bonds

2.3.4 Operational & Embedded Finance

- 2.3.4.1 Leasing
- 2.3.4.2 Vendor Financing

2.4 Consulting & Design

- 2.4.1 Security Strategy Consulting
- 2.4.2 Governance & Compliance Advisory

2.5 Go-to-Market Partners

- 2.5.1 Distributor / Reseller / VAR
- 2.5.2 SI
- 2.5.3 ISV
- 2.5.4 Broker
- 2.5.5 Cloud Service Provider
- 2.5.6 Implementation Partner
- 2.5.7 Support / Maintenance Partner

2.6 Independent Evaluation / Assessment

2.7 Technology Alliance

2.8 Assurance & Fiduciary Services

- 2.8.1 Legal Services
- 2.8.2 Audit & Assurance

Category 2: Technology Production and Value Delivery (Secondary Sector)

In the cybersecurity industry, the secondary category refers to the industrial system that transforms technological capabilities into products, tools, services, or financial instruments, and delivers them commercially to end users. The ecosystem includes not only technology developers and manufacturers, but also all definitive actors who convey value to clients—such as sales, integration and system assembly, delivery and implementation, and all supporting structures that facilitate value realization.

Technology itself is morally neutral, yet it empowers its users. The ultimate purpose of the secondary sector is to enable end users to realize the full value of technological capabilities. However, as user needs and objectives vary, the selection and application of specific technologies likewise differ—whether commercial or political, whether just or malicious, the realization of value ultimately depends on the intent of the user.

Framework Usage Notes

1. Representative, not exhaustive: Institutions are selected for representativeness only and do not constitute a comprehensive list.
2. Multiple roles: Some institutions perform multiple functions and may appear in more than one category, reflecting practical influence rather than a single classification.
3. Time and context-bound: This framework reflects institutional influence at the time of research. Roles and market impact may evolve with policy, market, or strategic changes.
4. Information sources and neutrality: All content is based on publicly available information. Inclusion does not imply endorsement of past outputs, nor recommendation of future applicability.
5. Disclaimer: This framework represents COI's professional judgment at the time of publication. Users should conduct independent evaluation based on their own business, regulatory, and compliance requirements.

About THE COI

THE COI (Cybersecurity Observatory Institute) is an independent, non-profit research institute dedicated to the sustained observation and systematic epistemic study of the global cybersecurity ecosystem as a structured, multi-layered industry.

Established for academic and public-interest purposes, THE COI does not engage in vulnerability testing, technology production, commercial services, or compliance enforcement. Instead, it operates as a neutral observatory—examining how cybersecurity capabilities are generated, commercialized, institutionalized, and governed across different sectors and jurisdictions.

By systematically mapping actors, roles, and interactions across the sectors of cybersecurity, THE COI develops analytical frameworks, ecosystem models, and research outputs intended to support informed decision-making by users, institutions, and policymakers.

THE COI is independent by structure.

Its role is not to participate, but to observe, study, and clarify the complexities of an evolving global cybersecurity landscape.

02 Clarifying Key Relationships

1. Protagonists and Supporting Roles

In most technological narratives, solution providers—particularly technology vendors—are placed at the centre of the stage and portrayed as the protagonists of technological evolution, industrial transformation, and capital-driven wealth creation. Technological breakthroughs, product innovation, and capital success form the main storyline, while other participants in the industry are naturally relegated to supporting roles.

Underlying this narrative structure is a deeper assumption: technology is treated as the ultimate purpose of industrial development, and the significance of other actors lies primarily in enabling the realization of that purpose.

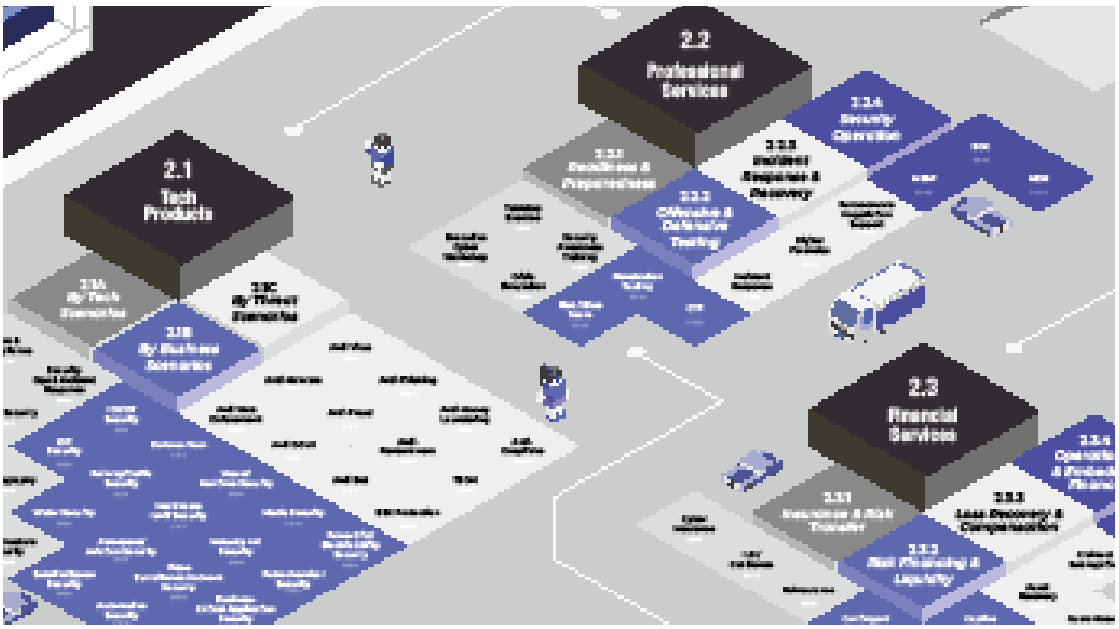
The cybersecurity industry, however, does not fully conform to this technology-centred, one-dimensional narrative. Rather than a linear progression driven solely by technological advancement, it more closely resembles an organic ecosystem of strategic interaction among multiple actors. Within this ecosystem, each participant exists according to its own logic, value, and objectives, rather than as a mere extension or instrumental tool of another.

For this reason, within our analytical framework of the cybersecurity secondary sector, THE COI do not presuppose a hierarchy of protagonists and supporting roles. Technology vendors and the surrounding ecosystem—including service providers, channel networks, consulting institutions, and other industry participants—are situated on the same analytical plane. Industrial evolution, in this view, is not the result of unilateral propulsion by a single type of actor, but rather the outcome of continuous interaction among multiple roles that collectively shape the trajectory of the industry.

Likewise, the existence of the secondary sector should neither be understood as the sole purpose of the cybersecurity industry, nor reduced to an instrumental function serving other dimensions of the industry. It constitutes an essential component of the broader industrial ecosystem—one that coexists with and depends upon other structural dimensions, together forming the integrated system through which the cybersecurity industry operates and evolves.

2. Logical Exclusivity and Practical Integration

In conventional commercial settings, the objectives of the various solutions within the secondary industry are largely aligned: to



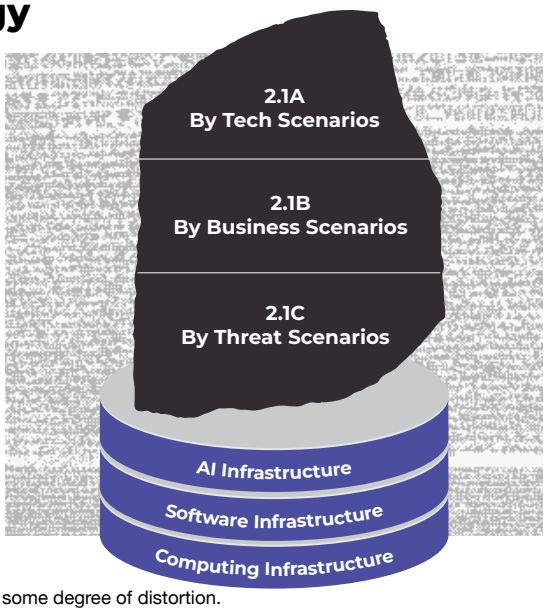
address clients' problems and create tangible value.

Yet the different paths through which these objectives are pursued remain distinct in their essential attributes. Within the analytical framework of the secondary industry, we therefore distinguish among three categories—2.1 Technology Products, 2.2 Professional Services, and 2.3 Financial Services—each of which evolves into different forms under its respective attributes.

Conceptually, a client may adopt any one of these instruments as the primary means of addressing its needs. An enterprise, for example, may allocate the majority of its security budget to technology products, or combine the three through different arrangements in order to construct a security architecture better suited to its circumstances. Correspondingly, companies may specialize in a single technical or service capability, or assemble integrated offerings composed of multiple instruments.

However, the combination of tools in concrete commercial practice does not imply that their industrial attributes can be blurred. Technology, services, and finance represent fundamentally different forms of value. These distinctions of attribute shape not only their internal logic of value creation but also their external modes of application, and to a considerable extent define the structural relationships through which other actors in the industry collaborate and integrate with them.

3. Three Lenses of Technology



The technology industry communicates meaning largely through systems of terminology, concepts, and symbols. Such symbolic systems do not merely provide different forms of description; they embody distinct logics and value orientations.

Within the field of cybersecurity, three commonly used descriptive frameworks can be observed: technology-based, threat-based, and business-scenario-based. In practice, these symbolic systems are frequently used interchangeably or in combination, depending on the context. One may think of them as viewing the same object through different faces of a triangular prism, or as analogous to the Rosetta Stone—where multiple languages converge in their effort to describe a single underlying reality.

Yet language and symbols possess inherent limits. No symbolic system can fully escape this constraint. Consequently, technological narratives constructed from different dimensions each contain elements of precision, while also inevitably introducing some degree of distortion.

Structurally, these three lenses do not stand in a hierarchical relationship to one another. Rather, they represent different perspectives through which the same technological reality may be articulated. When examined more closely, each of these frameworks can in turn reveal deeper layers of internal logic.

Nor is there any inherent superiority among them. They simply constitute different pathways for understanding and describing technological reality.

THE COI
Cybersecurity Observatory Institute

2.1 Three Lenses of Technology

2.1A By Tech Scenarios

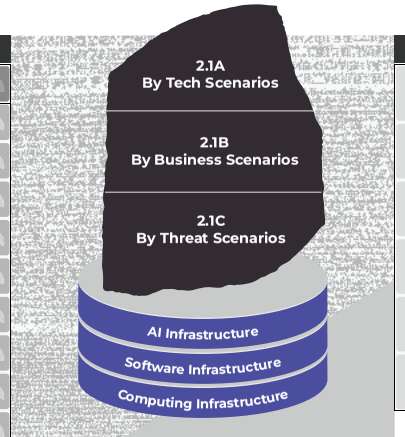
			GRC Automation	SRS	TPRM	IRM	2.1A.1 Risk & Compliance						DRP	CRQ	Social Listening	STC					
DDM	SDM	DSPM	DAG	CDM	DDR	APM Observability	WAF	WAAP	API Security	SWG	DAST	IAST	SAST	RASP								
DAP	2.1A.4 Data & Privacy				DLP	SBG	Fuzzing	2.1A.2 Application Security					Reverse Engineering/ Decompile	SCA								
DRM	SMPC	Differential Privacy	Personal Privacy Protection	Confidential Computing	TEE	CDR	Sandbox	ASOC	ASTO	ADR	ASPM	Application Shielding	MFT	RBI								
	Homomorphic Encryption	PMT	Privacy Computing	PIAs					SSL Certificate Management	Code Signing	Secure Instant Communications											
	SIEM	SOAR	XDR	Honeypot/ Deception	2.1A.5 Security Ops & Incident Response							UEBA	DFIR	Threat Hunting								
CNAPP	CSPM	KSPM	SSPM	IAM	PAM	Bastion Host/ Jumpbox	MIM	CIAM							IP Intelligence							
CWPP	CASB	CIEM	CDR	IEAM	ITDR	IDaaS	DaaS	IGA	HSM	KMaaS	EKM		Dark Web Intelligence	Vulnerability Intelligence	CEM		2.1A.3 AI Security					
2.1A.6 Cloud Security				AD Security	2.1A.7 Identity Security			IDV	2.1A.10 Cryptography				2.1A.12 Threat Intelligence									
Secure Workspace	Secure Browser	Microsegmentation	Container Security	RBIA	CA	MFA/FIDO/ OTP/PKI Token	Passwordless	UA	PQC	QKD	FPE		TI Lookup	TI Feed	TIP							
						CAPTCHA								TIG								
SASE	SSE	ZTNA	NGFW	NSPM	EDR	HIDS	UEM	CSSTPs	Cyber Range	VA	VPT			SG Network Security								
NDR/NTA	2.1A.9 Network Security			APT Protection	2.1A.8 Endpoint Security			2.1A.11 Vulnerability Management					2.1A.13 Infrastructure Security									
	ETA	Network Visibility and Observability	NIPM Observability		UES	EAIC	Host Hardening	RBVM	CTEM	EASM	Cyberspace Surveying and Mapping		DNS Security	IPv6 Security	SCA							
	Data Diode		NAC			MTD			CAASM	BAS				Firmware Security								

2.1B By Business Scenarios

2.1B.1 ICS/OT Security	2.1B.2 IOT Security	2.1B.3 Defense Tech
2.1B.4 Railway/Traffic Security	2.1B.5 Water Security	2.1B.6 Vessel/Maritime Security
2.1B.7 Healthcare IoMT Security	2.1B.8 Aerospace/Aviation Security	2.1B.9 Satellite/Space Security
2.1B.10 Media Security	2.1B.11 Industry 4.0 Security	2.1B.12 Video Surveillance Network Security
2.1B.13 Automotive Security	2.1B.14 PowerGrid/Electric Utility Security	2.1B.15 Petrochemical Security
2.1B.16 Business-Critical Application Security		2.1B.17 Web3 Security

2.1C By Threat Scenarios

2.1C.1 Anti-Virus	2.1C.2 Anti-Malware	2.1C.3 Anti-Web Defacement	2.1C.4 Anti-Phishing
2.1C.5 Anti-Fraud	2.1C.6 Anti-DDoS	2.1C.7 Anti-Money Laundering	2.1C.8 Anti-Ransomware
2.1C.9 Anti-Bot	2.1C.10 Anti-DeepFake	2.1C.11 TSCM	2.1C.12 BEC Protection



2.1A By Tech Scenarios

2.1A.1 Risk & Compliance
- 2.1A.11 Governance/Risk/Compliance Automation
- 2.1A.12 Security Rating Service
- 2.1A.13 Third-party Risk Management
- 2.1A.14 Insider Risk Management
- 2.1A.15 Digital Risk Protection
- 2.1A.16 Cyber Risk Quantification
- 2.1A.17 Social Listening
- 2.1A.18 Sensitive Terminology Compliance

2.1A.2 Application Security
- 2.1A.21 Application Performance Monitoring and Observability
- 2.1A.22 Web Application Firewall
- 2.1A.23 Web Application API Protection
- 2.1A.24 API Security
- 2.1A.25 Secure Web Gateway
- 2.1A.26 Dynamic Application Security Testing
- 2.1A.27 Interactive Application Security Testing
- 2.1A.28 Static Application Security Testing
- 2.1A.29 Runtime Application Self-protection
- 2.1A.210 Secure Email Gateway
- 2.1A.211 Fuzz Testing
- 2.1A.212 Reverse Engineering/Decompile
- 2.1A.213 Software Composition Analysis
- 2.1A.214 Content Disarm and Reconstruction
- 2.1A.215 Sandbox
- 2.1A.216 Application Security Orchestration Correlation
- 2.1A.217 Application Security Testing Orchestration
- 2.1A.218 Application Detection Response
- 2.1A.219 Application Security Posture Management
- 2.1A.220 Application Shielding
- 2.1A.221 Managed File Transfer
- 2.1A.222 Remote Browser Isolation
- 2.1A.223 SSL Certificate Management
- 2.1A.224 Code Signing
- 2.1A.225 Secure Instant Communications

2.1A.3 AI Security

2.1A.4 Data & Privacy
- 2.1A.41 Dynamic Data Masking
- 2.1A.42 Static Data Masking
- 2.1A.43 Data Security Posture Management
- 2.1A.44 Data Access Governance
- 2.1A.45 Copy Data Management
- 2.1A.46 Data Detection Response
- 2.1A.47 Database Audit Protection
- 2.1A.48 Data Loss Prevention
- 2.1A.49 Digital Right Management
- 2.1A.410 Secure Multi-Party Computation
- 2.1A.411 Differential Privacy
- 2.1A.412 Personal Privacy Protection
- 2.1A.413 Confidential Computing
- 2.1A.414 Trusted Execution Environment
- 2.1A.415 Homomorphic Encryption
- 2.1A.416 Privacy Management Tools
- 2.1A.417 Privacy Computing
- 2.1A.418 Privacy Impact Assessments

2.1A.5 Security Ops & Incident Response
- 2.1A.51 Security Information Event Management
- 2.1A.52 Security Orchestration, Automation Response
- 2.1A.53 Extended Detection Response
- 2.1A.54 Honeypot/Deception
- 2.1A.55 Users Entity Behavior Analytics
- 2.1A.56 Digital Forensics and Incident Response
- 2.1A.57 Threat Hunting

2.1A.6 Cloud Security
- 2.1A.61 Cloud Native Application Protection Platforms
- 2.1A.62 Cloud Security Posture Management
- 2.1A.63 Kubernetes Security Posture Management
- 2.1A.64 SaaS Security Posture Management
- 2.1A.65 Cloud Workload Protection Platform
- 2.1A.66 Cloud Access Security Broker
- 2.1A.67 Cloud Infrastructure Entitlement Management
- 2.1A.68 Cloud Detection and Response
- 2.1A.69 Secure Workspace
- 2.1A.610 Secure Browser
- 2.1A.611 Microsegmentation
- 2.1A.612 Container Security

2.1A.7 Identity Security
- 2.1A.71 Identity Access Management
- 2.1A.72 Privileged Access Management
- 2.1A.73 Bastion Host/Jumpbox
- 2.1A.74 Machine Identity Management/ Non-human Identity
- 2.1A.75 Customer Identity Access Management
- 2.1A.76 Employee Identity Access Management
- 2.1A.77 Identity Threat Detection Response
- 2.1A.78 Identity as a Service
- 2.1A.79 Directory as a Service
- 2.1A.710 Identity Governance Administration
- 2.1A.711 Active Directory Security
- 2.1A.712 Identity Verification
- 2.1A.713 Risk-Based Authentication
- 2.1A.714 Certificate Authority
- 2.1A.715 MFA/FIDO/OTP/PKI Token
- 2.1A.716 Passwordless
- 2.1A.717 User Authentication
- 2.1A.718 CAPTCHA

2.1A.8 Endpoint Security
- 2.1A.81 Endpoint Detection Response
- 2.1A.82 Host-based Intrusion Detection System
- 2.1A.83 Unified Endpoint Management
- 2.1A.84 Unified Endpoint Security
- 2.1A.85 Endpoint Application Isolation Containment
- 2.1A.86 Host Hardening
- 2.1A.87 Mobile Threat Defense

2.1A.9 Network Security
- 2.1A.91 Secure Access Service Edge
- 2.1A.92 Security Service Edge
- 2.1A.93 Zero-Trust Network Access
- 2.1A.94 Next Generation Firewalls
- 2.1A.95 Network Security Policy Management
- 2.1A.96 Network Detection Response/Network Traffic Analysis
- 2.1A.97 Advanced Persistent Threat Protection
- 2.1A.98 Encrypted Traffic Analysis
- 2.1A.99 Network Visibility and Observability
- 2.1A.910 Network Performance Monitoring and Observability
- 2.1A.911 Data Diode
- 2.1A.912 Network Access Control

2.1A.10 Cryptography
- 2.1A.101 Hardware Security Module
- 2.1A.102 Key Management as a Service
- 2.1A.103 Enterprise Key Management
- 2.1A.104 Post-Quantum Cryptography
- 2.1A.105 Quantum Key Distribution
- 2.1A.106 Format-Preserving Encryption

2.1A.11 Vulnerability Management
- 2.1A.111 Crowdsourced Software Security Testing Platforms
- 2.1A.112 Cyber Range
- 2.1A.113 Vulnerability Assessment
- 2.1A.114 Vulnerability Prioritization Technology
- 2.1A.115 Risk-Based Vulnerability Management
- 2.1A.116 Continuous Threat Exposure Management
- 2.1A.117 External Attack Surface Management
- 2.1A.118 Cyberspace Surveying and Mapping
- 2.1A.119 Cyberasset Attack Surface Management
- 2.1A.1110 Breach Attack Simulation

2.1A.12 Threat Intelligence
- 2.1A.121 IP Intelligence
- 2.1A.122 Dark Web Intelligence
- 2.1A.123 Vulnerability Intelligence
- 2.1A.124 Critical Event Management
- 2.1A.125 Threat Intelligence Lookup
- 2.1A.126 Threat Intelligence Feed
- 2.1A.127 Threat Intelligence Platform
- 2.1A.128 Threat Intelligence Gateway

2.1A.13 Infrastructure Security
- 2.1A.131 5G Network Security
- 2.1A.132 DNS Security
- 2.1A.133 IPv6 Security
- 2.1A.134 Side-Channel Analysis
- 2.1A.135 Firmware Security

2.1B By Business Scenarios

- 2.1B.1 ICS/OT Security
- 2.1B.2 IOT Security
- 2.1B.3 Defense Tech
- 2.1B.4 Railway/Traffic Security
- 2.1B.5 Water Security
- 2.1B.6 Vessel/Maritime Security
- 2.1B.7 Healthcare IoMT Security
- 2.1B.8 Aerospace/Aviation Security
- 2.1B.9 Satellite/Space Security
- 2.1B.10 Media Security
- 2.1B.11 Industry 4.0 Security
- 2.1B.12 Video Surveillance Network Security
- 2.1B.13 Automotive Security
- 2.1B.14 PowerGrid/Electric Utility Security
- 2.1B.15 Petrochemical Security
- 2.1B.16 Business-Critical Application Security
- 2.1B.17 Web3 Security

2.1C By Threat Scenarios

- 2.1C.1 Anti-Virus
- 2.1C.2 Anti-Malware
- 2.1C.3 Anti-Web Defacement
- 2.1C.4 Anti-Phishing
- 2.1C.5 Anti-Fraud
- 2.1C.6 Anti-DDoS
- 2.1C.7 Anti-Money Laundering
- 2.1C.8 Anti-Ransomware
- 2.1C.9 Anti-Bot
- 2.1C.10 Anti-DeepFake
- 2.1C.11 TSCM
- 2.1C.12 BEC Protection

Category 2 **Technology Production and Value Delivery (Secondary Sector)**

In the cybersecurity industry, the secondary category refers to the industrial system that transforms technological capabilities into products, tools, services, or financial instruments, and delivers them commercially to end users. The ecosystem includes not only technology developers and manufacturers, but also distributors and sales actors who convey value to clients—such as sales, integration and system assembly, delivery and implementation, and all supporting structures that facilitate value realization.

Technology itself is morally neutral, yet it empowers its users. The ultimate purpose of the secondary sector is to enable end users to realize the full value of technological capabilities. However, as user needs and objectives vary, the selection and application of specific technological levers differ—whether commercial or political, whether just or malicious, the realization of value ultimately depends on the intent of the user.

2.1 Three Lenses of Technology

The technology industry communicates meaning largely through systems of terminology, concepts, and symbols. Such symbolic systems do not merely provide different forms of description; they embody distinct logics and value orientations.

Within the field of cybersecurity, three commonly used descriptive frameworks can be observed: technology-based, threat-based, and business-scenario-based. In practice, these symbolic systems are frequently used interchangeably or in combination, depending on the context. One may think of them as viewing the same object through different faces of a triangular prism, or as analogous to the Rosetta Stone—where multiple languages converge in their effort to describe a single underlying reality.

Yet language and symbol possess inherent limits. No symbolic system can fully escape this constraint. Consequently, technological narratives constructed from different dimensions each contain elements of precision, while also inevitably introducing some degree of distortion.

Structurally, these three lenses do not stand in a hierarchical relationship to one another. Rather, they represent different perspectives through which the same technological reality may be articulated. When examined more closely, each of these frameworks can in turn reveal deeper layers of internal logic.

Nor is there any inherent superiority among them. They simply constitute different pathways for understanding and describing technological reality.

About THE COI

THE COI (Cybersecurity Observatory Institute) is an independent, non-profit research institute dedicated to the sustained observation and systematic epistemic study of the global cybersecurity ecosystem as a structured, multi-layered industry.

Established for academic and public interest purposes, THE COI does not engage in vulnerability testing, technology production, commercial services, or compliance enforcement. Instead, it operates as a neutral observatory—examining how cybersecurity capabilities are generated, commercialized, institutionalized, and governed across different sectors and jurisdictions.

By systematically mapping actors, roles, and interactions across the sectors of cybersecurity, THE COI develops an analytical framework, ecosystem models, and research outputs intended to support informed decision-making by users, institutions, and policymakers.

THE COI is independent by structure

Its role is not to participate, but to observe, study, and clarify the complexities of an evolving global cybersecurity landscape.

4. Market Pathways and the End User

Within the secondary industry, a diversity of roles can be observed. In concrete commercial cases, multiple roles may appear in conjunction; yet this does not imply that every role must necessarily be present within the practical pathway of the market, nor that they invariably form a complete sequential chain.

Across different countries and regions, variations in cultural traditions, commercial conventions, and institutional environments give rise to different configurations of market pathways. Some chains remain relatively concise, while others develop into more layered structures; the forms through which value is distributed—and the scale at which it is realized—accordingly vary.

Value ultimately converges upon the user. Users may take the form of corporate organizations or individual consumers. Under different stages of development and contextual conditions within the cybersecurity industry, these categories of users assume distinct positions within the broader industrial structure. In constructing the THE COI Model, no restriction is imposed upon any particular type of user. Rather, all demand-side and usage-side participants are incorporated within a unified analytical framework. Further discussion of this principle can be found in Part IV of the THE COI Model.

The structural complexity of market pathways bears no necessary relation to whether the end user is an enterprise organization or an individual consumer. Large institutions may contract directly with technology vendors, while consumer purchases may also pass through multiple layers of distribution and agency. Such differences are, in essence, alternative manifestations of commercial structure in practice.

03 Notes

1. Premise of the Analysis

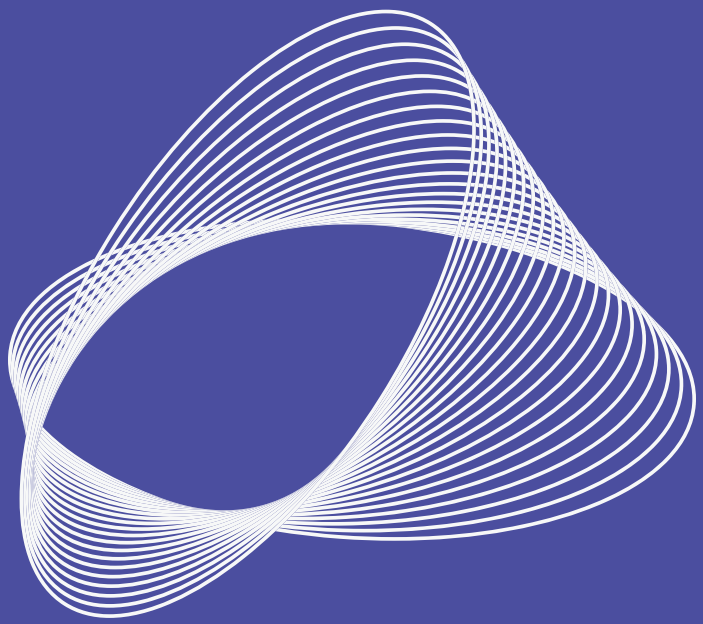
THE COI analytical model is constructed to observe the various roles within the cybersecurity ecosystem and the relationships among them. The model itself is an abstract structure: its function is to reveal relationships, not to render moral judgment.

Yet any analysis must proceed within a concrete setting. Only through the articulation of a scenario can relationships become clear, meaning emerge, and discussion take place.

In examining the roles and relations of the secondary industry, we therefore introduce a default assumption: the discussion concerns the classification of roles within the commercial secondary sector of cybersecurity industry, and the relationships among them.

In fact, upon the same primary foundation—Zero-Day—different forms of secondary industries may arise. One may observe, for example, a black-market cybercrime sector, or a state-oriented cyber capability shaped by political objectives.

When the underlying assumption changes, the roles within it change as well, and so too do their relations to the other dimensions of the model.



ISSN