KuppingerCole Report

WHITEPAPER

By Martin Kuppinger

May 31, 2022

Getting Ahead of the Cybercriminals: Understanding the External Threat Landscape

Security leaders face an uphill task as cybercriminals become increasingly creative and armed with an arsenal of seemingly unlimited resources. Rapid digitalization to re-capture post-pandemic growth coupled with an uncertain geopolitical climate requires security leaders to rethink their cybersecurity strategy. Despite the increased in cybersecurity spend, businesses continue to fall prey to cyberattacks. To stay ahead of cybercriminals, “knowing the enemy and knowing yourself” is key to building effective defenses. Organizations must have full visibility to their external threat landscape and be aware of potential attacks targeting them. This predictive capability allows organizations to focus on the biggest risks and avert the most damaging fallout.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

Commissioned by CYFIRMA

1 Introduction / Executive Summary

Cyber risks are on the rise. The number of attacks is growing. Each day, new vulnerabilities are identified. More and more organizations fall victim to cyber-attacks. While cybersecurity has moved into the focus of the board of management, and while cybersecurity spending has been increased, the effectiveness and efficiency of many of the cybersecurity activities must be questioned.

There are three more aspects to consider. Cybersecurity spending will never be able to grow as fast as attacks increase. Just trying to defend is not sufficient – organizations must get ahead of the cybercriminals and move beyond introspective approaches on cybersecurity by understanding the external threat landscape. Finally, the pace of change: Cybersecurity needs to keep up with this pace. Cybersecurity initiatives thus must take a focus beyond the traditional, introspective approach of protection, detection, and response, and become proactive.

This requires a thorough understanding of the attackers, their rationales, their targets, and their methods. To take an analogy: Successful organizations sell strong because they understand their customers. Organizations also will be more successful in cyber defense when they understand their attackers and how they look from a hacker's perspective.

While there always remains the need of knowing the IT assets (including shadow IT) of the organization and the attack surface, but also 3rd party risks along the supply chain, it is equally important to understand which vulnerabilities are currently actively exploited by attackers and which types of organizations, industries, and technology stacks are primarily targeted by attacks. Also, the specific risks for the own organization and brand, by either being a preferred target of certain groups of attackers, or by sensitive information such as code, passwords, or other information sprawling in the dark web, must be considered.

This requires a solution that provides more comprehensive insight into the state of cybersecurity and that correlates information across all these areas, from the insights into the hacker's intent and behavior to the concrete risk exposure of an organization. This is the foundation for targeting cybersecurity initiatives and concentrating on the most critical vulnerabilities at any point in time.

CYFIRMA delivers a Unified External Threat Landscape Management Platform that helps in gathering insights from both the organization and the external world, including proactively and continuously monitoring the dark web, the surface web, and social media platforms, and can correlate all that information, guiding organizations and their cybersecurity teams in taking the right actions and understanding change in the risk exposure or the organization.

2 Key Findings

- With cyber attacks being on the rise and cyber risks for organizations constantly increasing, organizations must review both the effectiveness and efficiency of their cybersecurity spending, as well as their cyber defense capabilities
- Just adding technology is not enough. Organizations must gain a better understanding of their concrete exposure to cyber-attacks, to pick the right tools, but also for retiring legacy cybersecurity tools that don't deliver to the expectations anymore.
- This requires a deeper understanding of the rationales and targets of their attackers. Only when knowing their enemies, organizations will be able to get ahead of the cybercriminals.
- Organizations must understand the currently used attacks and exploited vulnerabilities, the concrete threats against their organizations and industries, and their attack surface, and must map this information to understand where to focus their countermeasures on.
- With constant changes in vulnerabilities, targets, and attack vectors used, organizations must continuously monitor the threat landscape to adapt their measures, beyond just occasional or regular pen testing and red team exercises.
- CYFIRMA provides a comprehensive Unified External Threat Landscape Management Platform that helps organizations in gaining insight into their attacker's intent and activities and focusing on the most critical vulnerabilities in their IT environment.

3 The cyberthreat & cyber-defense landscape: Effectiveness and efficiency in question

While cybersecurity budgets are increasing, the number of attacks also continues to increase, as well as the success of such attacks and the damage caused by these. Increasing just the budget and the number of tools in place is not sufficient. Organizations must step back and analyze the cause of a gap in effectiveness and efficiency of their cybersecurity investments.

Efficiency is about doing the things right. Effectiveness is about doing the right things. For cybersecurity, the obvious question today is whether what is done is efficient and effective. Despite a continuous increase in cybersecurity spendings, the number of cyberattacks as well as the cost of cybercrime increases continuously. According to a recent KuppingerCole Analysts survey, roundabout one third of the organizations increase their 2022 cybersecurity budget by more than 20%, compared to 2021, and other 47% report an increase in the range of 5% to 20%.

Figure 1: Cyberattacks grew massively in 2021, compared to 2020 (Source: CYFIRMA).

This increase in spending is still low when compared to the increase in attacks. With more attacks and new attack vectors, the question is whether the challenge arises from a lack of cybersecurity spending, or from a lack of effectiveness and efficiency. Just spending more money on traditional cybersecurity solutions will not fix the problem. Organizations must step back and think about where to focus their cybersecurity spending on, to successfully counter attacks and getting ahead of their attackers.

Just increasing the cybersecurity spending is not sufficient – the increase in cyberattacks anyway exceeds the increase in what organizations can spend

This is even more essential in an evolving threat landscape. Cybersecurity must evolve when threats evolve. What has been effective and efficient in the past (if that has been the case) might no longer be the right approach for today's threat landscape. Even more important: Organizations must move from a reactive, defensive approach to a proactive model, where they are prepared for the ever-evolving threat landscape. Only then measures can be taken that are effective against the new threats.

The evolution of the threat landscape is manifold. Kinetic cyberattacks that are focused on causing physical damage, e.g., in operational technology; the uptick in state-sponsored attacks triggered by geo-political tensions; the escalation of ransomware menace, powered by a well-working business model; or new technologies such as deepfake for spreading misinformation are symptomatic for this evolution.

In the context of this evolution of threats, the risk landscape of organizations is also changing to the worse. Attackers are after a wide range of data, from financial documentation to product data and blueprints, but also software configurations and employee-related information. Other attacks are just trying to damage systems or trigger a ransom. Critical infrastructures and operational technology (OT) environments, financial systems, supply chains (for disruption), but also SMEs (Small/medium-sized enterprises) are subject to attacks.

Organizations need to better understand which tools they need to counter cyber-attacks, based on the concrete threats to the organization and the IT assets

---

By just adding more or “better” tools, this challenge will not be solved. Unless the right tools are in place to counter what attackers not only are doing today but will do tomorrow, measures are not effective. Efficiency, on the other hand, requires a clear focus on the real risks and tools that help addressing the cybersecurity challenges with reasonable effort, specifically in this age of cybersecurity skills gap.

4 The cause: Not a lack of tools, but their focus

Many organizations immediately start looking at technology when a new cyber threat arises, or when they are hit by an attack. However, tools are just one element of the solution. It is about people, processes, and tools, and about taking a holistic approach. But it also is about better understanding the attackers.

The traditional models for cybersecurity with their cycles starting with identification of risks and preparation for attacks are not wrong. Unfortunately, this assumes that risks are well-understood. This would require understanding both the attack surface and the attacker's intentions. Who could attack you, using which attack vectors to which part of your IT or OT environment? Defining risk only by what is most critical to an organization, or which are the most common or critical attack vectors is not sufficient, because it misses the perspective of the attacker, which affects the probability of an attack and, in case of success, the impact.

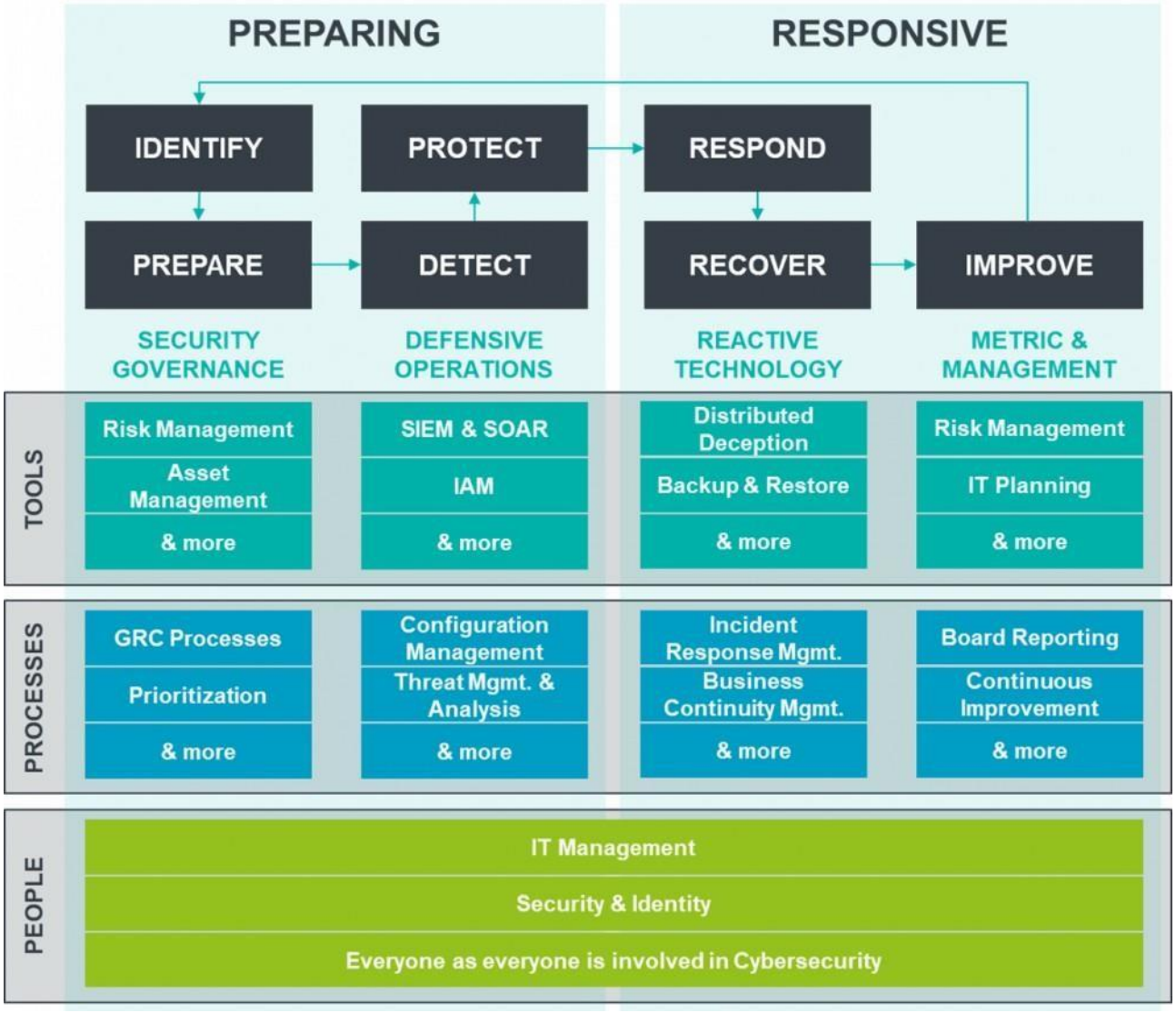

Figure 2: The KuppingerCole model for cyber risk management.

Digging deeper into the field of risk analysis done right, there appear multiple seven major challenges:

- Tools focus: Many cybersecurity teams consist of too few people that must deal with all the technical aspects within cybersecurity. Frequently, there is a lack of time and methodical knowledge for thorough risk analysis. This situation also is depicted by too many false positives, no concise way of prioritizing cybersecurity efforts, and a tendency to focus on low-effort but also low-impact remediations.
- Shadow IT: The known parts of IT are surely more than the tip of the iceberg, but most organizations must deal with a decent amount of shadow IT, which continues to grow in the age of remote work. What isn't known can't be protected.

- Complexity of IT: The complexity of IT environments adds to this. Each system and application can become a target or an entry point for attackers. Protecting complex IT environments requires close collaboration of multiple parties and sophisticated methods and processes.
- Connected 3rd party systems: Additionally, organizations must not only care for their own IT, but also are exposed to risks that come in via connected 3rd party systems. Supply chain risks have arisen as one of the major issues in cybersecurity.
- Growing attack surface: In the digital age and in multi-hybrid, multi-cloud environments, the attack surface is constantly growing by the addition of new cloud services, new digital services, and the agile nature of today's IT.
- Internal perspective: Virtually all approaches for risk management take an internal perspective, focusing on identifying the most critical assets and potential vulnerabilities in their own IT, but don't take the perspective of the attackers.
- Lack of understanding of the attackers: This results in a lack of understanding of what attackers are likely to do, and a lack of context for isolated events that are identified. Without knowing the enemy and continuously analyzing them, beyond occasional pen testing and red team exercises, it is hard to fight the enemy.

Tools alone don't help. They might provide the impression that the required measures have been taken. But the fact that growing investments into cybersecurity don't lead to a decrease in the number of attacks or the cost of cyber incidents shows that it is not just about tools.

The challenges for implementing a strong cybersecurity posture are manifold – main challenges are the insight into the own IT assets and their vulnerability, and understanding the targets of attackers

---

There also isn't a gap in the number of security tools that are in place in most organizations. It is about

- Having the right tools in place
- Not having tools in place that don't add value to other tools

  Using tools efficiently and effectively

  Integrating tools

Selecting the right tools, integrating the tools, and using tools will only work when the risks are understood correctly. This requires taking a different, broader approach on cyber risk management, beyond the internal perspective. Only when the attackers, their techniques, and their agenda are understood, the right actions can be taken.

5 External threat landscape visibility - Predictive Threat Intelligence to get ahead of cybercriminals

No successful business will ignore the customer. Understanding the customer's demand is key to success in sales. The situation for cybersecurity is similar: Without understanding the attackers, organizations will not be able to target their countermeasures. There is a need for predictive threat intelligence that delivers insight into the hacker's intent and actions.

The traditional introspective approach of cybersecurity is no longer enough. There is a need for covering all phases. Cybersecurity has evolved significantly over the past years. It evolved from a mainly protective focus towards a multi-stage approach as depicted in Figure 2. It evolved from a network-centric approach towards a Zero Trust model covering many levels, from identity and endpoints to networks and data. But cybersecurity still didn't manage to get ahead of the cybercriminals but remains reactive.

One, if not the missing element is understanding the enemy:

- What is their target?
- Which types of attacks are currently in use?
- What are they talking about?
- How does this affect your organization?
- What could be used against me?

Cybersecurity must take a different perspective here, like it is common in many other areas of the business. Product management and sales act from the customer perspective. Who is the customer? Who is the buyer's persona at the customer? What do they need? These are basic questions that are always asked in successful organizations.

If you don't know your enemy, you will not be able to successfully protect your organization

---

Successful cybersecurity needs taking a similar approach in understanding the attackers. Who are they? Who is behind them, what is their plan and what are their targets? What do they want to achieve? Who understands the attackers gains a better understanding of the countermeasures that must be implemented?

In cybersecurity, constant change adds to the complexity:

- New vulnerabilities are constantly discovered, as the vast number of patches that are released every month shows
- New attack vectors are constantly developed, sometimes thousands of variants of such vectors
- Attack targets are frequently changing, specifically for state-sponsored attacks
- "Business models" of attackers are frequently changing – once a specific type of attack is successfully blocked, new approaches come "to the market"

This means that analyzing the attacker is not a one-time activity or one that is performed in long intervals, but it needs to become a continuous exercise.

External threat analysis, attack surface management, and vulnerability management require continuous updates – all areas are under constant change

---

The external threat landscape and understanding of the attackers must then be mapped to the state of IT of the own organization. Understanding concrete threats and the existing attack surface help in defining the concrete countermeasures, focusing on protecting the weak spots of the organization's IT against the concrete, current threats.

6 The CYFIRMA Approach for Predictive Threat Intelligence

CYFIRMA has developed a comprehensive platform for Unified External Threat Landscape Management. That platform integrates a range of capabilities, spanning Attack Surface Management, Digital Risk Discovery, and several other areas, and can build the foundation for predictive threat intelligence.

CYFIRMA provides a comprehensive solution for this, their Unified External Threat Landscape Management Platform. This solution covers six areas of capabilities:

- External Attack Surface Discovery: Despite the focus on the attackers, understanding the own attack surface is essential and must not be limited to the known. Shadow IT and 3rd party risks along the supply chain must be equally in scope of this analysis.
- Vulnerability Intelligence: Existing vulnerabilities must be known and understood, regarding their technical severity, but also regarding the current state of exploitation by attackers. This helps in focusing remediation and the high-impact vulnerabilities.
- Brand Intelligence: Brands, products, and services might be a current target for attackers. This is specifically the case for political hacktivism, but not limited to this area.
- Digital Risk Discovery & Protection: Discovering current discussions of hacker groups and analyzing their potential impact on organizations, but also identifying information that is shared on the dark web such as source code, passwords, exploits, etc. helps in understanding the current threat. The dark web capabilities of CYFIRMA count to their differentiators in competition.
- Situational Awareness: The variety of insights from the attack surface and vulnerabilities to concrete threats for an organization must be mapped and results in an assessment of the current cyber risk situation.
- Cyber Intelligence: Based on this, threats and attacks can be better predicted, and better countered. Knowing about who is most likely to attack using which vectors against which vulnerabilities is essential knowledge for improving the cybersecurity posture of organizations.

CYFIRMA has developed a solution that spans all six pillars and provides a platform for unified external threat landscape management. This extends the focus beyond common, internal-only facing solutions such as ASM (Attack Surface Management) and the various protective and responsive tools in cybersecurity.

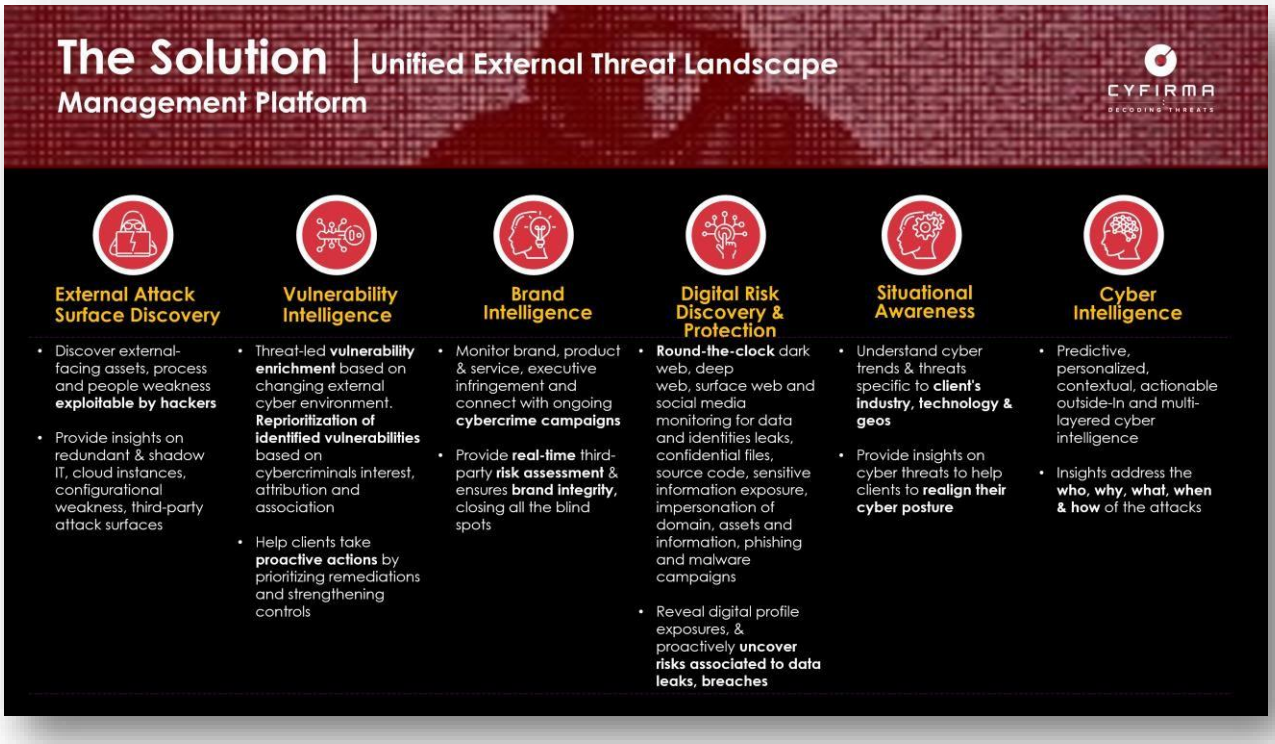

Figure 3: The CYFIRMA model for Unified External Threat Landscape Management (Source: CYFIRMA).

The CYFIRMA solution is based on two core SaaS solutions:

- DeCYFIR: This solution is the platform for External Threat Landscape Management (ETLM) and provides inside into the threats affecting an organization.
- DeTCT: This is the Digital Risk Discovery & Protection (DRDP) platform, delivering further insights into the concrete risks and the digital assets that can be used for attacks against the organization.

DeCYFIR is the main solution. It provides insight into the threats and risks impacting an organization. It discovers and analyzes the current attack surface and delivers real-time insights into weaknesses that could be exploited by attackers. It analyzes brand- and industry-related exposure to cyber-attacks, including the analysis of trends for industries, technology stacks, and geolocation. It provides insight into how hacker motives, campaigns, and methods are related, allowing organizations to understand their exposure, and taking targeted countermeasures.

The information is provided via dashboards, allowing the users to drill-down into details. DeCYFIR provides a strategic, a management, and an operational view. The strategic view focuses on the current risk and the change in risk. The management view provides a guided, systematic approach on addressing the most critical threats. The tactical view provides information for concrete security controls.

DeTCT as the second component of the CYFIRMA SaaS solutions is providing the detailed insights into the outer space, specifically the dark web. DeTCT also provides dashboards, starting with risk and "hackability" scores. It delivers metrics on attack surfaces and the current attack situation across the globe as well as for the geolocation and industry. It also delivers the insight into data that has been leaked and a lot of additional information.

CYFIRMA is unique in its approach to a comprehensive coverage of analyzing and managing the attack surfaces as well as understanding the external threat landscape. Their approach exceeds common ASM approaches by including the external state and gathering a wide range of information that helps in better understanding the current threat to an organization. Based on that, targeted countermeasures can be taken, focusing on the areas that impose the biggest concrete risk to an organization.

7 Recommendations

Improving the cybersecurity posture of organizations is not only a matter of adding tools. It requires the right people and processes, and a thorough understanding of the risk mitigation impact provided by the various tools in focus.

Understanding this impact can't be only based on analyzing the attack surface but requires taking a broader perspective. Whether this is titled "know your enemy", or whether different terminology is used: Getting a unified, comprehensive view on both the external threat landscape and the vulnerability of internal IT is the foundation for targeted countermeasures.

Key elements of such initiative are as follows:

1. Understanding the complete attack surface, including shadow IT. The non-managed part of IT provides the easiest way in for attackers.
2. Understanding the external risk exposure from an organizational perspective: Threats to brand, to the industry, to the geolocation.
3. Understanding the current attacks: Which vulnerabilities are in scope of attackers, which attack vectors are used, what must be in focus of protection?
4. Understanding the concrete exposure of the organization: Which information that can be utilized by attackers is out in the dark web?
5. Mapping: Which concrete threats exist, and which risk arise from the vulnerabilities and the activities of attackers?
6. Mitigation: Taking a continuous approach on identifying and enforcing the right, targeted countermeasures.

It is essential to understand the dynamics of cyber risks and the fact that threats, vulnerabilities, and risks are under constant change. Continuous monitoring and adaptation of countermeasures as well as the ability to react quickly is essential for successfully mitigating cyber risks.

8 Related Research

Leadership Brief: Top Cyber Threats
Advisory Note: Business Continuity in the age of Cyber Attacks
Leadership Brief Cybersecurity Trends & Challenges

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.