DREAMLAB TECHNOLOGIES

Supply Chain Security

WHY SUPPLY CHAIN SECURITY MATTERS

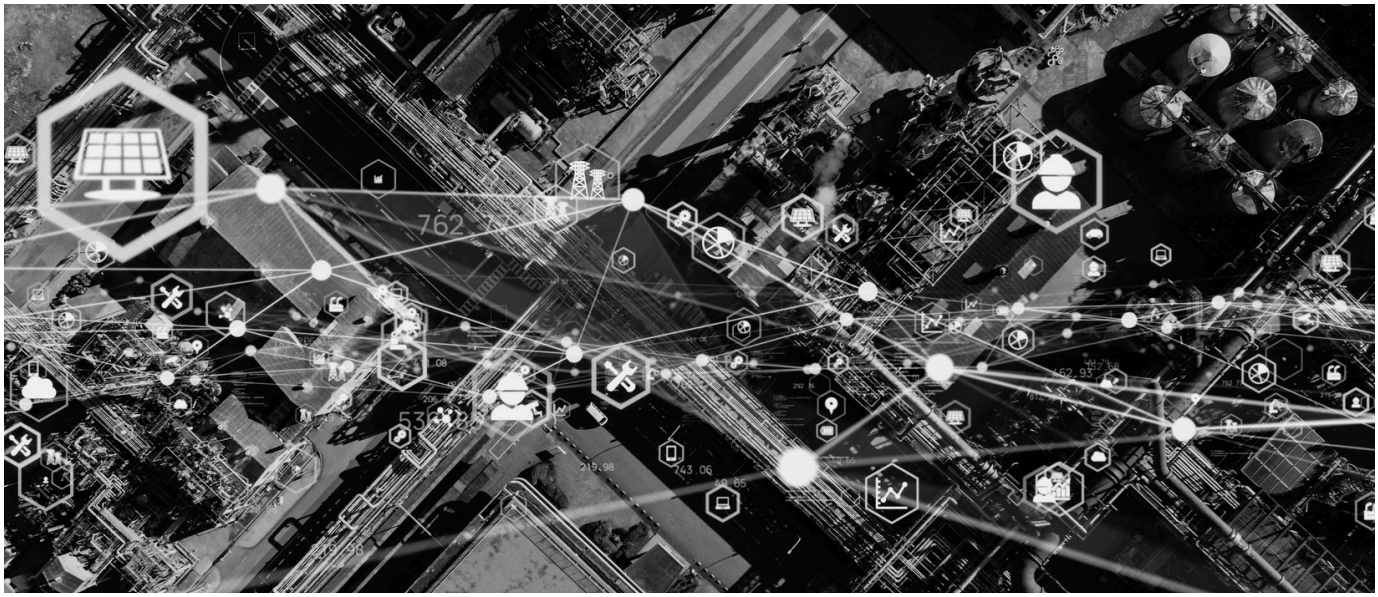
CYOBS
SEE THE CYBER

IF YOU CAN'T SEE IT, YOU CAN'T MANAGE IT.

STEP OUT OF THE DARK.

CyObs is a high-precision cyber radar system that offers a complete view of your country's cyberspace, combining threat detection, risk management and insights needed to eliminate threats and reduce your attack surface.

The Challenge



Increased Complexity of Supply Chains

Today's business ecosystems are becoming increasingly complex, interconnected, and global in nature. Both public entities and private organizations are facing growing dependencies on a diverse array of stakeholders to deliver their products and services. These stakeholders can take various forms, such as suppliers, manufacturers, producers, wholesalers, retailers, logistics providers, and technology providers.

A Chain is only as Strong as its Weakest Link

Beyond an organization's direct control, its supply chain poses complex challenges from a cybersecurity risk perspective. Many cybersecurity analyst reports have highlighted the increasing complexity of supply chains as a contributing factor.

As ecosystems grow and become more distributed, it becomes increasingly challenging for companies to effectively control and secure their supply chain. The more stakeholders involved, the more dependencies exist, which multiplies the complexity and expands the attack surface, ultimately increasing vulnerability.

Increase in Supply Chain Cyberattacks

This dynamic is confirmed by the dramatic rise in targeted cyberattacks on value chains in recent years (Robinson & Editor's Desk , 2023), where threat actors target high-impact product suppliers or service providers. “Software supply chain attacks are not an esoteric or isolated tactic, [...] they are popular, impactful, and have been used to great effect by state actors.” (Loomis, Scott, Lee, & Herr, 2020).

Global examples of supply chain attacks, such as the Solarwinds incident (Oladimeji & Kerner, 2024), have demonstrated the devastating consequences of such breaches . Even local examples in Switzerland, like the Xplain cyber attack (Inside IT, 2023), have shown the significant impact that the compromise of a key service provider can have on other organizations with heightened security requirements, such as government, defense, and law enforcement entities.

According to Gartner (2024), by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a threefold increase from 2021. The impact of these supply chain attacks is much greater than direct cyberattacks, as all customers of the compromised product or service provider are potentially affected.

Why Should Organisations and Businesses Care?

Multiplied Effect of Supply Chain Attacks

Organizations should care deeply about the growing threat of software supply chain attacks. These types of attacks exploit vulnerabilities in the third-party software, components, or services that organizations rely on, significantly expanding the potential attack surface beyond what the organization can directly control. This creates a complex challenge, as the interconnected nature of modern business ecosystems means that a successful supply chain attack can have widespread, rippling impacts, affecting not just the targeted organization, but all the customers and users of the compromised software or service (SANS, 2021; Wysopal , 2024).

Detecting and attributing responsibility for supply chain attacks can also be exceptionally difficult, as the malicious code or activity may be expertly hidden within legitimate software updates or service integrations. This makes it tedious for organizations to identify the source of the attack and hold the responsible parties accountable.

Consequences beyond Operational Disruption

The consequences of falling victim to a software supply chain attack can be severe. Organizations can suffer significant reputational damage, as they may be perceived as unable to protect their own systems and data, as well as that of their customers and partners. There are also regulatory and compliance implications, as many industries have standards that require robust supply chain security measures. Failure to address these risks can lead to costly fines and penalties.

Beyond the reputational and regulatory impacts, supply chain disruptions caused by a successful attack can also have severe business continuity and financial implications. Operational downtime, lost productivity, and the costs associated with incident response, remediation, and potential litigation can all take a substantial toll.

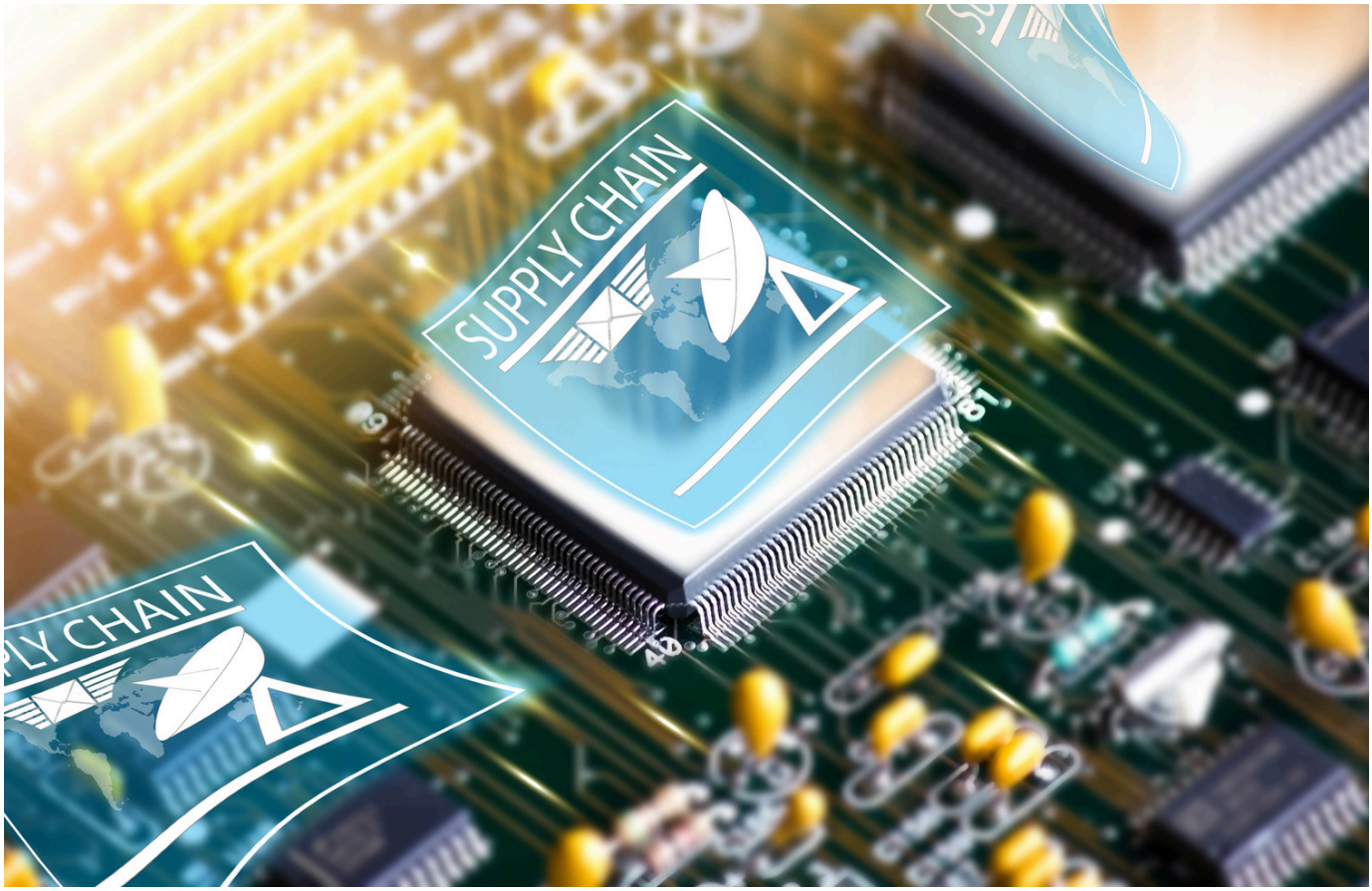
European Cyber Resilience Act puts Pressure on Companies

Additionally, the impending enforcement of The European Cyber Resilience Act (2022) in Europe should have a significant positive impact on organizations operating in the region. Approved by the EU Parliament in March 2024, this new regulation goes beyond simply ensuring that products with digital elements placed on the EU market have fewer vulnerabilities. It takes a comprehensive approach, addressing the entire product life cycle, from the planning and design stages through development, production, delivery, and ongoing maintenance.

The Cyber Resilience Act places a strong emphasis on the accountability of manufacturers, who will be required to remain responsible for the cybersecurity of their products throughout the entire life cycle.

This includes providing security updates to users and mandating that manufacturers notify ENISA (the EU Agency for Cybersecurity) and the relevant CERT teams within 24 hours of an actively exploited vulnerability or security incident.

Failure to comply with the Cyber Resilience Act can result in substantial penalties, with fines of up to 5 million Euros or 2.5% of a company's global turnover. This heightened regulatory pressure further reinforces the need for organizations to prioritize proactive measures to secure their software supply chains.
Lastly, (business) consumers and users must also play a role by monitoring for emerging vulnerabilities and applying patches in a timely manner to maintain the overall security of the products they use.



DREAMLAB TECHNOLOGIES

Holistic Approach to Address Supply Chain Cyber Risks

What Can Organizations Do?

To effectively combat the growing threat of software supply chain attacks, organizations must take a holistic approach that encompasses the key elements of governance, identification, protection, detection, response, and recovery:

1

Governance

Organizations should establish clear policies and procedures for supply chain risk management, with executive-level oversight and accountability. Integrating supply chain security into the overall cybersecurity strategy and risk management framework is crucial.

2

Identification

Organizations must maintain a comprehensive inventory of all suppliers, understand the services or products they provide, and assess the data and IT assets they have access to. Regular risk assessments are essential for identifying vulnerabilities and dependencies within the supply chain.

3

Protection

Implementing minimum security requirements for suppliers through contractual clauses, providing clear communication about security expectations, and ensuring compliance are key protection measures. This helps mitigate risks and strengthen the overall security of the supply chain.

4

Detection

The deployment of specialized tools, such as a Cyber Radar, is a critical component. These solutions enable organizations to continuously measure and monitor the attack surface of their supply chain, identify potential vulnerabilities, and receive timely alerts on emerging threats.

5

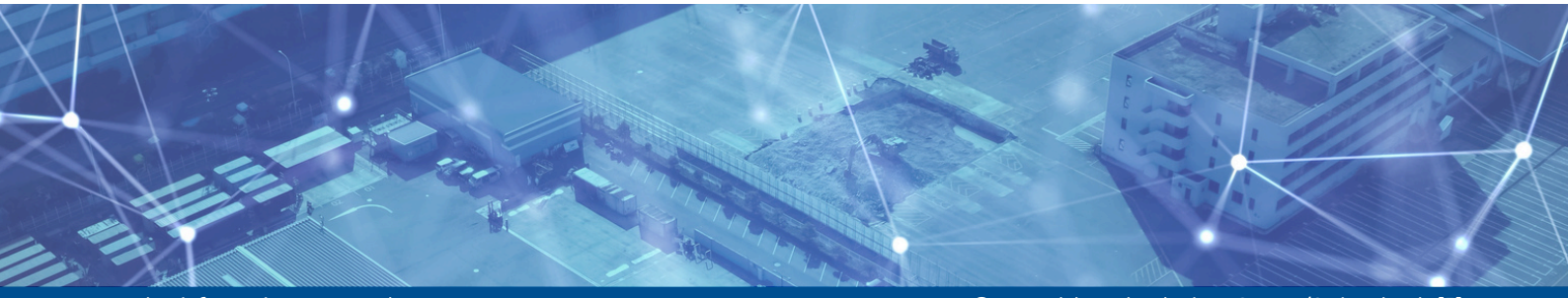
Response

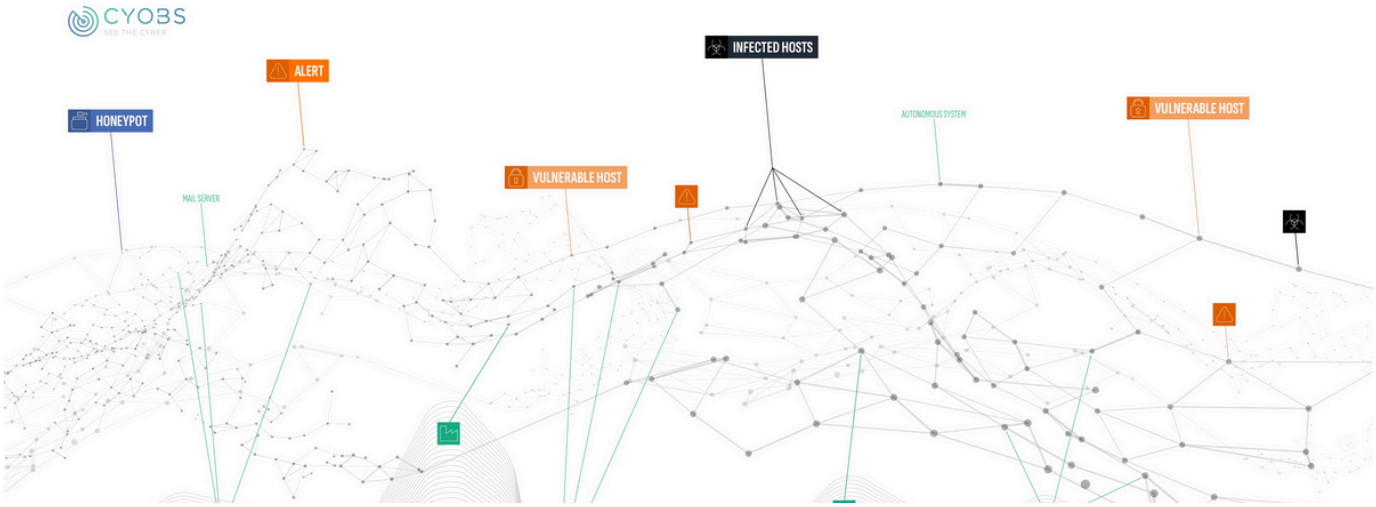
The ability to respond effectively to supply chain-related incidents is paramount. Organizations should develop and regularly test incident response playbooks specifically designed to address such disruptions, ensuring clear communication and coordination with suppliers and other stakeholders.

6

Recovery

Finally, robust recovery strategies, including backup and restoration procedures, are essential to facilitate the swift recovery of systems and data affected by a supply chain attack. Collaboration with suppliers and industry partners to share information and lessons learned further enhances the overall resilience of the supply chain ecosystem.





How Can a Cyber Radar Help?

The most important element of having a Cyber Radar solution like **CyObs** is the ability to continuously monitor the attack surface and emerging vulnerabilities within the supply chain. By providing real-time visibility and alerting mechanisms, CyObs enables organizations to act swiftly to identify and resolve issues before they can be exploited by threat actors. This proactive approach is crucial in mitigating the risks posed by software supply chain attacks and safeguarding the organization's critical assets and operations.

Mastering Supply Chain Security with CYOBS

Mastering supply chain security requires a holistic approach. Proactive inventorization of assets, supply chain risk management, and proactive supply chain monitoring as a whole contribute to reduce supply chain cyber risks.

A cyber radar such as CyObs can uncover previously unrecognized potential vulnerabilities, exposed services and infrastructure dependencies.

Similar to a police patrol that regularly drives through the neighborhood to check that everything is in order, CyObs can proactively alert companies and cantonal administrations about security risks and thus help to eliminate them and avoid exposure and compromize.

Here is how CyObs can help to reduce supply chain risks:

Make Attack Surface Visible

CyObs supports you in identifying and visualizing vulnerabilities in the external attack surface so that existing security gaps can be closed before they can be exploited by criminals and cause damage.

Uncover Dependencies

Recognize dependencies in the supply chain such as shared infrastructure and cluster risks.

Proactive Risk Identification

Identify risks in your own infrastructure and in the supply chain at an early stage, minimize the attack surface and thus strengthen resilience.

Predictive Security Management

CyObs uses proactive monitoring and warning functions to identify potential vulnerabilities before they can cause damage.

A CyObs Case Study

A Swiss governmental entity engaged in Supply Chain Risk Monitoring by measuring the external attack surface of selected participating companies and suppliers in order to evaluate the participants in the form of a security rating.

The main goal was to identify and minimize risks in the organisation's own infrastructure and in the supply chain at an early stage, thereby strengthening resilience. The main challenge has been the onboarding of all participating companies.

Here is how CyObs helped to reach the main goal:

Quantify the risk using KPIs: a security risk metric helps to assess the risk of particular entities in your supply chain.

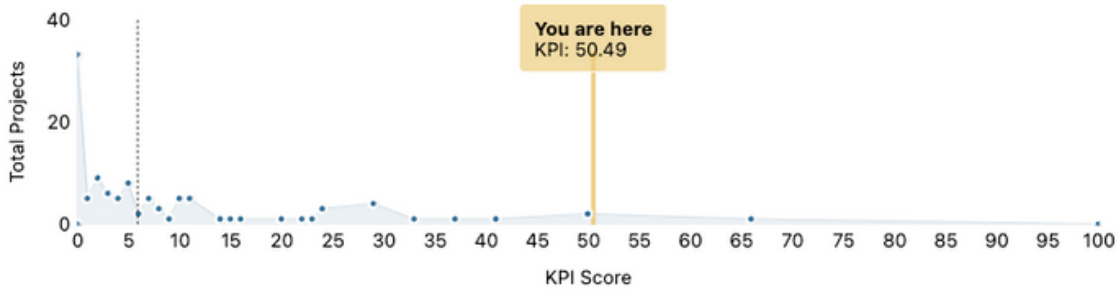


Figure 1. Risk KPI & Trends

Visualize Dependencies: dependencies on infrastructure level have been revealed such as entities using the same IT infrastructure providers down to IP (host) level.

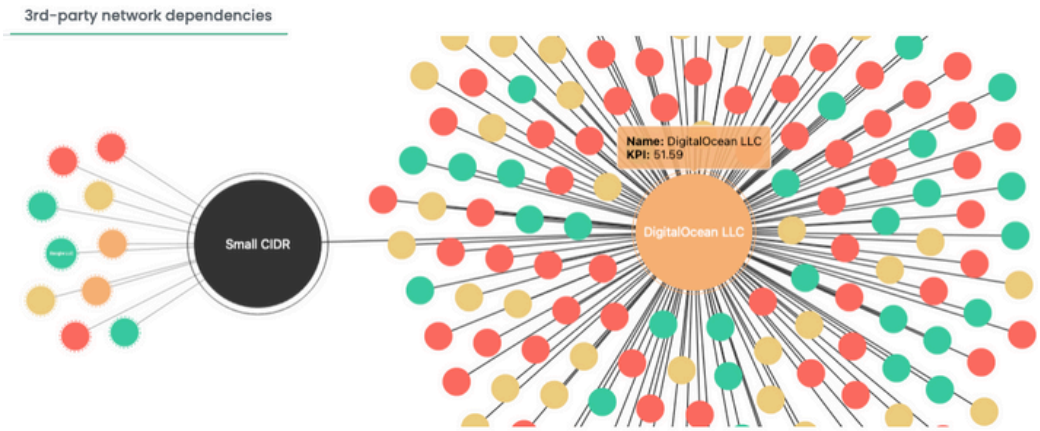


Figure 2. Massive dependencies on large infrastructures are made visible.

Identification of potentially vulnerable assets and exposures provides the visibility on where a compromize is more likely to occur.

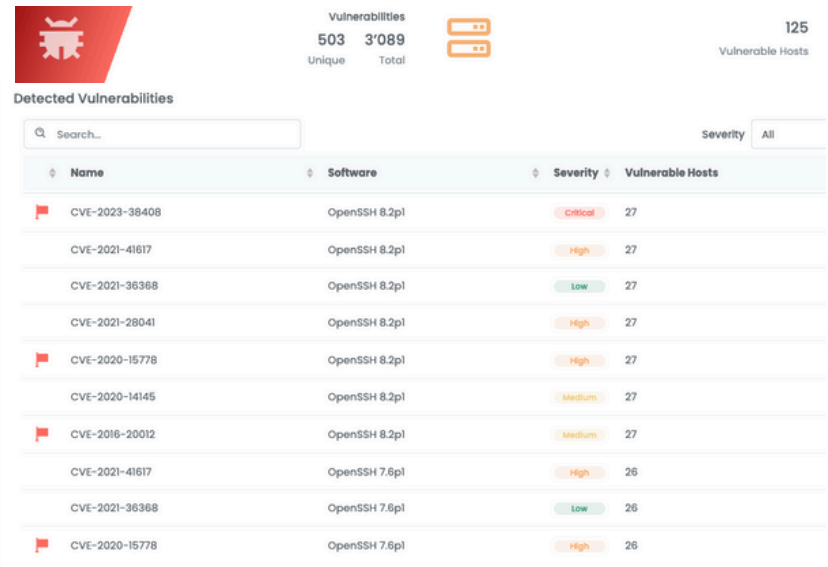


Figure 3. Detected vulnerabilities highlight areas at higher risk of breach.

Early warning system: Using alerting features the customer has been equipped with an early warning system to identify potential risks in its own and its supplier's infrastructure.

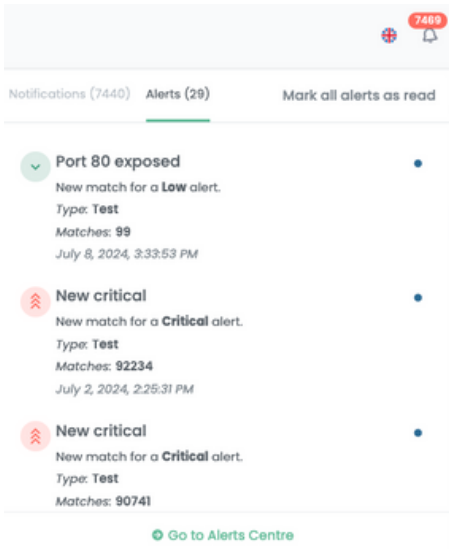


Figure 4. Early warning system identifies potential infrastructure risks.

The employed CyObs verification and monitoring process is depicted below.

Figure 5. CyObs Verification and Monitoring Process

Act now: Know and Secure Your Supply Chain.

Act now. Create transparency. Secure your supply chain.

The value chain is part of your attack surface. Create transparency and examine not only your own IT infrastructure, but also that of your suppliers.
With the help of KPIs, you can create transparency and increase your ability to act.
Recognize dependencies: reveal shared infrastructures, identify exposures, and manage resulting risks.

- **Transparency:** Make your attack surface visible, reduce exposures and attack points, increase your resilience.
- **Swissness:** CyObs is developed by Dreamlab Switzerland.
- **Security:** CyObs is hosted in Switzerland, your data is hosted in Switzerland and secured according to modern standards.

See **CyObs** in Action - ask for a demo: **https://cyobs.com/**

References

Gartner. (2024). Retrieved 2024, July from Cybersecurity Trends: Optimize for Resilience and Performance: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

Inside IT. (2023, July 3). Retrieved July, 2024 from Xplain-Hack: Daten aus Darkweb verschwunden und wieder aufgetaucht: https://www.inside-it.ch/xplain-hack-daten-aus-darkweb-verschwunden-und-wieder-aufgetaucht-20230703

Loomis, W., Scott, S., Lee, J., & Herr, T. (2020, July 26). Atlantic Council. Retrieved July, 2024 from Breaking trust: Shades of crisis across an insecure software supply chain: https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/

Oladimeji, S., & Kerner, S. M. (2024, July 30). TechTarget. Retrieved July, 2024 from SolarWinds hack explained: Everything you need to know: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Robinson, P., & Editor's Desk . (2023, August 27). CyberSecurity Magazine. Retrieved July, 2024 from Why are supply chain attacks increasing?: https://cybersecurity-magazine.com/why-are-supply-chain-attacks-increasing/

SANS. (2021). Retrieved July, 2024 from What You Dont Know About Vendor Risk Management & Data Privacy Could Cost you Millions in Fines - SANS @Mic: https://www.sans.org/webcasts/dont-about-vendor-risk-management-data-privacy-cost-millions-fines-atmic-118710/

The European Cyber Resilience Act (CRA). (2024). Retrieved July, 2024 from The European Cyber Resilience Act (CRA): https://www.european-cyber-resilience-act.com/

Wysopal , C. (2024, February 6). Forbes. Retrieved July, 2024 from Rising Threat: Understanding Software Supply Chain Cyberattacks And Protecting Against Them: https://www.forbes.com/sites/forbestechcouncil/2024/02/06/rising-threat-understanding-software-supply-chain-cyberattacks-and-protecting-against-them/

About CyObs

CyObs is an instrument for monitoring cyberspace. It builds on the four pillars measurement, analysis, visualisation and monitoring, providing the first comprehensive coverage of cyberspace. CyObs was developed as part of public-private partnership research project of Dreamlab Technologues AG with support from Swiss Confederation, with the aim of quantifying Swiss cyberspace. From this emerged a first generation of the product in collaboration with universities of applied sciences, used mainly for research purposes. At the same time, CyObs matured in the lab to become a fully functional management information instrument.

Further information: https://cyobs.com/

Contact us today to see how our team of knowledgeable experts is ready to help you strengthen your security posture.

CYOBS
SEE THE CYBER

info@cyobs.com

Powered by

DREAMLAB
TECHNOLOGIES

Monbijoustrasse 36
CH-3011 Bern
Tel: +41 31 398 6666
Fax: +41 31 398 6669
contact@dreamlab.net