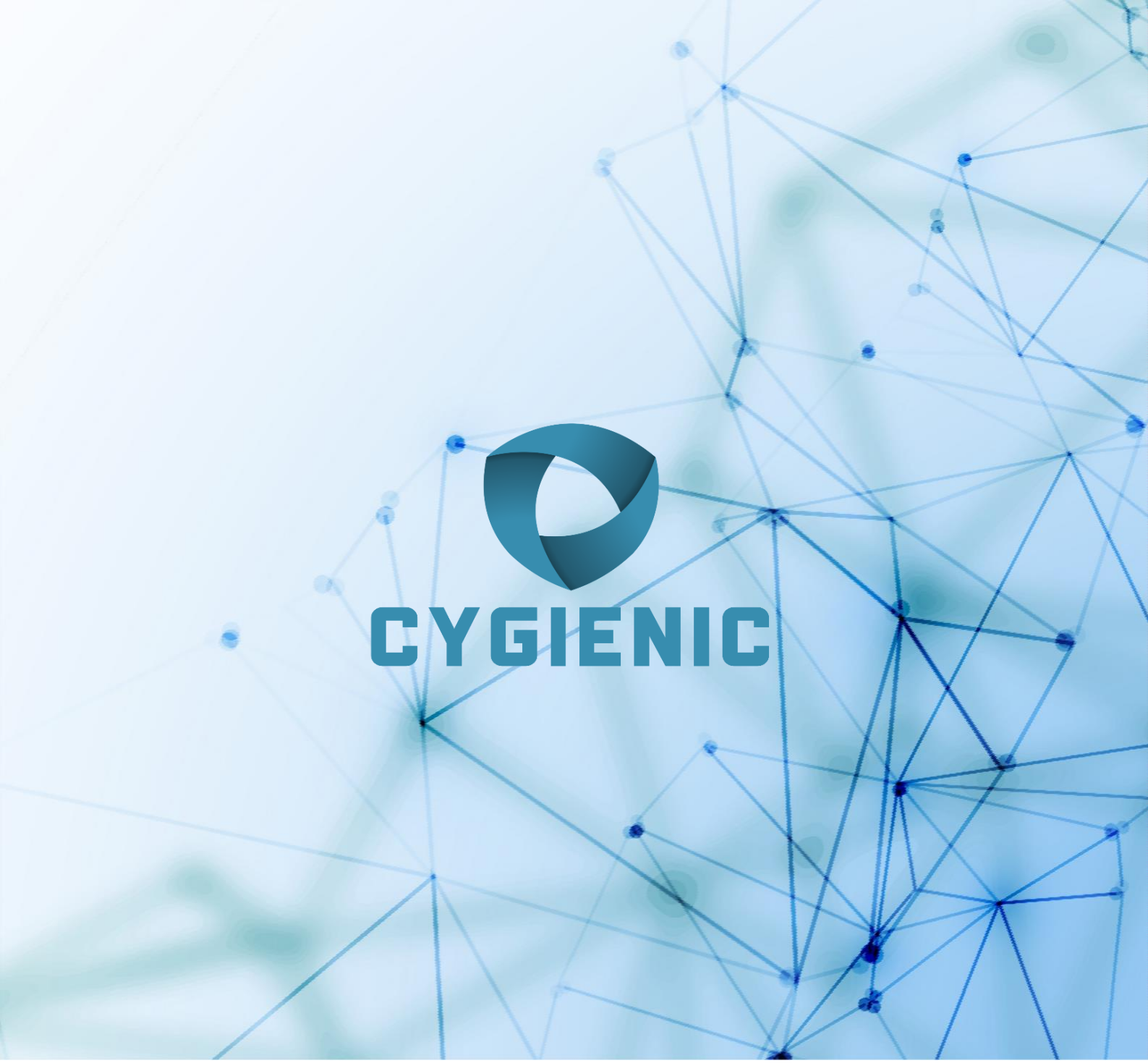


3rd Party Compliance Management

Managed Service

Powered by
Cygienic.com

Managed Services
Overview

Cygienic's managed services offer a comprehensive suite of solutions to fortify your organization's cybersecurity posture. With a focus on Attack Surface Management, we meticulously monitor your digital landscape, identifying and mitigating potential vulnerabilities before they can be exploited.

Cygienic also provides an Email Credentials & Data Leak discovery service to help identify your sensitive information.

Our Vulnerability Assessment service further enhances your security by proactively identifying and addressing weaknesses in your systems.

Lastly, our 3rd Party Compliance Risk Assessment Management services helps you to identify cyber risks and regulatory compliance gaps across your supply chain.

Uncover hidden threats and protect your company with Cygienic's managed service

3rd Party Compliance Mgmt.
Managed Service Overview

Cygienic's 3rd Party Risk and Compliance Managed Service is a comprehensive solution designed to help organizations navigate the complexities of third-party relationships while ensuring regulatory compliance and robust security.

In the first phase, our service conducts an industry standard questionnaire assessment of third-party vendors, examining their security practices, data handling procedures, and compliance with industry regulations. Through thorough due diligence, we identify potential risks and vulnerabilities associated with these partnerships.

The second phase involves continuous monitoring of third-party vendors cyber rating and attack surface. Cygienic employs cutting-edge technology to keep a close eye on these entities, regularly assessing their security and compliance performance. Any deviations from established standards are quickly detected, and organizations are promptly alerted, allowing for timely remediation actions.

By proactively managing third-party risks and ensuring ongoing compliance, Cygienic's service empowers organizations to maintain the integrity of their operations and protect sensitive data from potential breaches or regulatory penalties.

"Cygienic's 3rd Party Risk and Compliance Managed Service fortified our supply chain by delivering real-time insights, proactive risk mitigation, and streamlined compliance management."

-Singapore Manufacturer

"Cygienic's 3rd Party Managed Service helped us identify poor partner security where we were dependable on sharing our data – this has now been remediated."

-Singapore Hospice

3rd Party Compliance Management
Scope of Work

Completing a 3rd party compliance assessment, which includes attack surface scans of 3rd party external web-facing servers and industry standard compliance questionnaires, involves several critical stages:

1. **Identification and Onboarding:** Begin by identifying the 3rd party vendors or partners that require compliance assessments. Establish communication and onboarding procedures to ensure they understand the assessment process and requirements.

2. **Scoping:** Define the scope of the assessment, specifying the servers, systems, and services that will be evaluated. Ensure a clear understanding of the attack surface that needs to be scanned.

3. **Attack Surface Scans:** Utilize specialized tools and methods to conduct thorough attack surface scans on the 3rd party's external web-facing servers. This step involves identifying vulnerabilities, misconfigurations, and potential entry points for attackers.

4. **Compliance Questionnaires:** Administer industry standard compliance questionnaires to the 3rd party, which assess their adherence to relevant regulatory standards and best practices. This may involve questions related to data security, privacy, access controls, and more.

5. **Data Collection and Validation:** Collect and verify the responses to compliance questionnaires provided by the 3rd party – in Cygienic Cloud.

6. **Reporting:** Prepare comprehensive reports that consolidate the results of the attack surface scans, vulnerability assessments, and compliance questionnaires. Clearly presenting vulnerabilities and compliance gaps, along with recommended remediation actions.

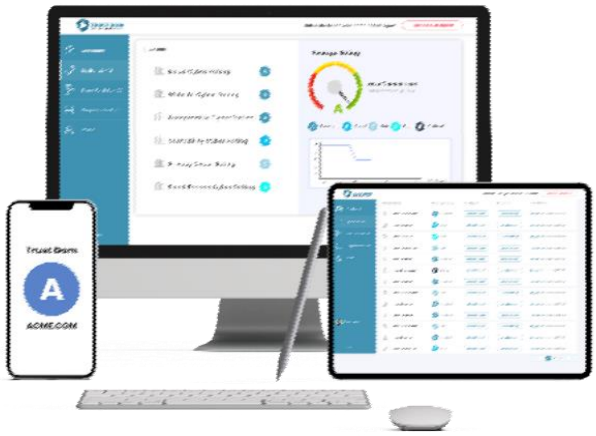
7. **Review and Validation:** Collaborate with the 3rd party to review the assessment results and remediation plan. Validate that the proposed fixes adequately address the identified vulnerabilities and compliance issues.

8. **Remediation Verification:** After the 3rd party has implemented the remediation plan, conduct follow-up assessments to verify that vulnerabilities have been addressed and compliance requirements met.

9. **Documentation:** Maintain detailed documentation of the entire compliance assessment process, including scan results, reports, remediation plans, and validation records.

10. **Ongoing Monitoring:** Implement continuous monitoring processes to ensure the 3rd party maintains compliance and security standards over time.

By following these stages, organizations can effectively assess and ensure compliance with industry standards for their 3rd party vendors and mitigate potential security risks associated with external web-facing server



Contact sales@cygienic.com
To discuss our managed services.