H-CYBER RISK

(SUPPLY CHAIN AND THIRD-PARTY RISK ASSESSMENT SERVICE)

CYBER EFFECT - LEVEL 3 - PRODUCTIVE

SERVICE DESCRIPTION

The CIS Components, Supply Chain Trustworthy Analysis and Third-Party Risk Service, provides assessment to CIS components and their trustworthiness as well as analysis of vendor risk. This service provides analysis and evaluation on the reliability of CIS components and the trust that can be placed upon them. Coordination in Security Risk Assessment of Customer Working Groups supports, leads, or coordinates Security Risk Assessment Working Groups for Customer programmes or projects.

VALUE PROPOSITION

Support to Customer Cyber Security - Sustainment. CIS Components and Supply Chain Trustworthiness analysis enables the deployment and operation of CIS infrastructure with an understood level of trust. This allows the appropriate management of risk to the confidentiality, integrity and availability of communications and information. Coordination in Security Risk Assessment Customer Working Groups leverages specialist knowledge of cyber risk to enable Customer risk assessment.

In this service a package of Pentest can be included provided that the customer has the right to audit clauses in their contracts. The Pentest will be aimed to the selected Vendors.

The Team will engage the Vendors that require improvements in their Cybersecurity Posture, by promoting an improvement roadmap to test the awareness and reaction capability of the internal teams towards Security events.

As an added flavor to this service, Cybersecurity Awareness Programs can be included aiming the most critical vendors to assure that People in their end will be conscious of the importance of conducting good behaviors.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER RISK

(SUPPLY CHAIN AND THIRD-PARTY RISK ASSESSMENT SERVICE)

CYBER EFFECT - LEVEL 3 - PRODUCTIVE

SERVICE FEATURES

CIS Component Cyber Security: Analyse and evaluate the extent to which one can rely on a CIS component, be it hardware, software, or both, to function as intended. The assessment can be made through either a set of assurance techniques or less rigorous means.

Supply Chain Cyber Security: Plan for, collect information about, assess, and handle the level of trust that can be placed in the components of a CIS based on the supply of sub-components, manufacturing, and logistics.

Coordination in Security Risk Assessment Working Groups: Support, lead, or coordinate Security Risk Assessment Working Groups for Customer programes or projects. This includes lead or coordinating the meetings and ex-committee work, providing advice regarding security risk assessment and risk management process, and support conducting SRA by Hardsecure. This service entails the review and approval (in coordination with Customer Security Audit Authorities) of the specification of risk assessment/management tools used for Customer CIS (e.g. Customer profile for EAR/PILAR), the development and maintenance of generic security risk assessment for Customer CIS scenarios.

Security Test and Verification (ST&V): Pre-Production Security Testing and Consultancy services conducted in support of Change Management and accreditation processes, for projects includes documentation review, vulnerability assessment and penetration testing.

Third-party Risk Assessment support the analysis of vendor risk posed by an organization's third-party relationships along the entire supply chain, including vendors, service providers, and suppliers. Risks to be considered include security risk, business continuity risk, privacy risk, and reputational risk.

ADDED VALUE OF OUR SERVICE

» We do Automated Third-Party Security Risk Assessments. This is necessary for organizations to conduct a comprehensive security evaluation of new vendors, and grant security of all supply chain of services & solutions.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER RISK

(SUPPLY CHAIN AND THIRD-PARTY RISK ASSESSMENT SERVICE)

CYBER EFFECT - LEVEL 3 - PRODUCTIVE

» Our third-party assessment team with an OT/ICS background can connect manufacturer products and solutions with industry best-practices and methodologies that meet customer requirements. It fills in the OT knowledge gaps that customer IT team may lack. For example, assessors with OT backgrounds can provide insight on which control hardware customer system uses that meet ISA Secure program (based upon the IAC security life-cycle as defined in ISA/IEC 62443). This is especially critical if customer control system uses hardware and software from many different manufacturers.

» Our Third-Party assessment team, who do not represent any hardware or software manufactures, take an unbiased approach to your system. While internal teams may have critical knowledge of customer control system and may have even designed it, Hardsecure third-party assessors can see the high-level view of customer control system as well as the minute parts of it. We will see gaps in a system that internal teams can miss.

SERVICE QUOTE REQUEST

For further information, please contact us using one of the following means:

"Hardsecure – Supply Chain and Third-party Risk Assessment Service" form (available on the service page on the website)

Contact Hardsecure Account Management:
(+351) 218 278 126 (PT)
(+44) 204 538 6686 (UK)
(+1) 202 2318 9859 (USA)
geral@hardsecure.com

Website:
https://en.hardsecure.com (**"Request Proposal"** form).