Digital Risk Monitoring

Enterprise Risk Monitoring and Third Party Risk Monitoring

Are you aware of your company's digital footprint and the risks involved? Is your IT dynamic and spread across different locations? And are you aware of weaknesses in your digital infrastructure?

A Chief Information Security Officer (CISO) would like to have a holistic overview of digital risk.

Digital risk can lead to a threat for the entire company. It is therefore controlled centrally, but obtaining a holistic overview is by no means straightforward.

The Service
Digital Risk Monitoring can be defined and expanded on a modular and specific basis. Regardless of the modular approach, each service provides integrated, holistic information.

Modul 1: Enterprise Risk Monitoring
Enterprise Risk Monitoring addresses the digital risks of your own organization or domain. It takes the technological, human and organizational dimensions into account.

Modul 2: Third Party Risk Monitoring
This variant is used to monitor the digital risks of your third parties as vendors or business partners. A holistic approach is applied that incorporates the technological, human and organizational dimensions.

Your Benefits with Digital Risk Monitoring

- You get a picture of your digital tracks (footprint) at all times thanks to 24 x 7 x 365 monitoring by SIX.
- You have access to a dashboard that gives you an overview of risks.
- You obtain a holistic view of your risks: technological, human, organizational.
- You can arrange monitoring of your company (enterprise) or your partners and suppliers (third parties).
- You are not only aware of your risks but also receive a risk assessment in the form of the risk rating and thus learn how to evaluate the threat situation in your IT infrastructure.
- You can compare your digital footprint with other market participants thanks to the risk benchmark.

Both modules, Enterprise Risk Monitoring and Third Party Risk Monitoring, include the following functions:

Application: Get an overview of the webframe utilization of your entire organization.

Automated Scanning: Automated scans can be defined via process scheduler.

Brand Risk: What problems can your customers face when using your domain name? Similar looking domain names can be misused as attack vectors.

Cloud Storage: Identify the storage services used in your company (Amazon, Microsoft, Google, Alibaba, etc.).

Confidential Documents: Search confidential documents which are shared on paste sites for keywords.

Darknet: Get information about trends in the dark net. We can also search the dark net for mentions and alert you if necessary.

Digital Asset: Automatically identify and categorize your digital assets.

DNS: DNS services are often vulnerabilities and DNS security has become a growing problem for many companies. We check your DNS entries frequently.

E-mail: Sender Policy Framework (SPF) is a simple validation system to protect against spoofing. The service checks if the SPF record is set for e-mails.

Encryption: Get an evaluation of the SSL settings of your websites.

Geo Risk: Monitor the geolocation of digital assets.

Hot Threat: Check whether a critical Common Vulnerabilities and Exposures (CVE) for a defined digital asset needs to be patched.

Incident History: Examine past cyber incidents that have happened to your company and have been published.

IoT Devices: Identification of high-risk IoT devices by using the Classless Inter-Domain Routing (CIDR) netmask.

Login Credentials: Identification of the loss of your employees' account information.

Network: Get a report of all open ports and all exposed digital assets on your network

Patching: Get an evaluation and information of vulnerabilities, on known network services, in your network.

Reputation: Every IP address of your organization is scanned in real-time with our Cyber Threat Intelligence (CTI).

Shadow IT: Identify hardware and software that is not operated by your IT department.

Social Media: Detection of fake social media accounts.

Source Code: Source code is one of your company's most important digital assets. Check if confidential information is present in the source code.

SIX – Your Strong Partner from the Financial Industry

Your Benefits

- SIX is the only service provider in Switzerland offering Cyber Threat Intelligence (CTI) that is focused on financial topics.
- SIX develops use cases for the financial sector and updates them on an ongoing basis.
- SIX is itself system-critical, and as an operator of system-critical infrastructures it has an insider's view of relevant, sector-specific threats.

The Following May Also Be of Interest to You:

- SOC as a Service
- Incident Response Support
- Vulnerability Management

SIX Group Services AG
Pfingstweidstrasse 110
P. O. Box
8005 Zurich

T + 41 58 399 3993
cybersecurity@six-group.com
www.six-group.com/cybersecurity

Your Contact
Dieter Bartl
Senior Cyber Security Sales Manager
T +41 58 399 3575
dieter.bartl@six-group.com