Web Analysis - darkSOC®

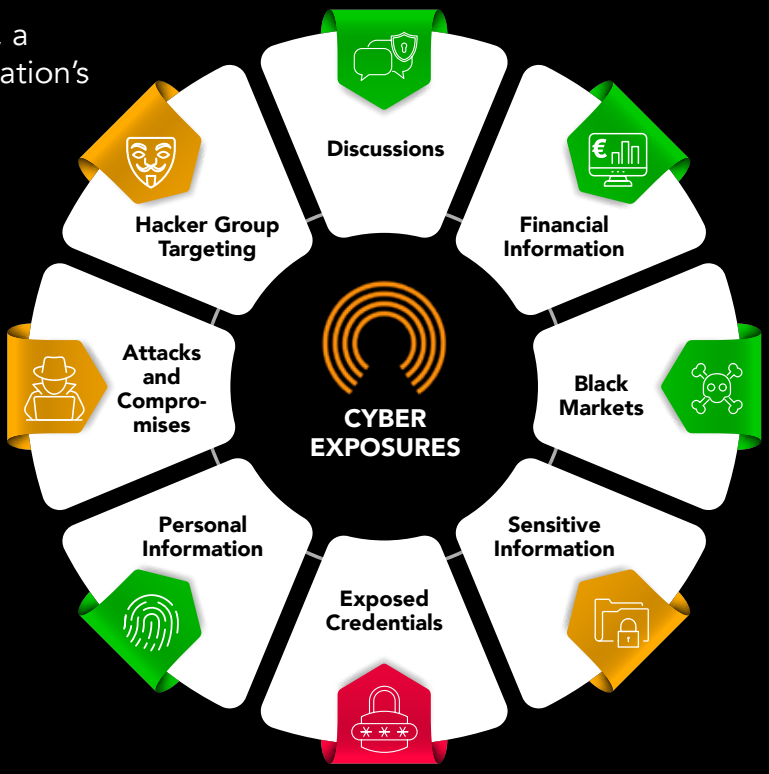
WEB ANALYSIS

DarkSOC® dark and deep web analysis

- DarkSOC® analysis reveals the organisation's profile and level of exposure in the dark and deep web.
- Data is collected on servers located around the world non-stop at 9 Gb per second.
- The analysis can reveal, among other things, shortcomings in the organisation's cybersecurity, leaked information and other potential problems.
- The analysis provides insight into what the organisation looks like through the eyes of cybercriminals and hostile actors.

Attack surface analysis

- In the attack surface analysis, the structure of the organisation's network infrastructure and the state of its cybersecurity are analysed in six different groups of risk factors.
- In terms of the attack surface, a depiction of what the organisation's network looks like in the eyes of an external observer is reported.
- The parts of the network assets related to the organisation, such as servers, open ports, applications and websites are listed.
- The findings are divided into eight categories and three levels based on severity.
- The most important findings are reported in an executive summary report to support decision-making.
- The main report includes a more detailed presentation of the findings, as well as recommendations for corrective actions and strategic-level development targets.



MONITORING

Based on the analysis, monitoring is agreed upon to determine the effectiveness of the measures and to detect new threats. New findings observed during monitoring are examined in relation to previous observations and the reasons why the number of observations has changed are analysed. The results are reported at agreed intervals.

- Regular monitoring: a report delivered at agreed intervals, for example monthly, quarterly, biannually or annually.
- Continuous monitoring: 24/7 monitoring of new findings, and the reporting of information directly to the customer

Security of the Supply Chain

THE NIS2 EU-DIRECTIVE (Network and Information Security Directive 2) COMPLIANCE REQUIRE

Company policies needs to give attention to security around supply chains and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.

The analysis can be done for selected parts of the supply chain organisations (requires an agreement). The findings of the attack surface analysis are introduced to the concerned organisations which are responsible for the implementation of corrective actions and reporting to the customer when the corrective measures have been taken.

An example of service content:

- Preliminary analysis for the supply chain
- Web analysis for the supply chain
- NIS2 implementation training

Auditing the cybersecurity practices of the supply chain increases the customer organisation's cyber maturity and helps the company better meet the minimum requirements of the Cybersecurity Act. It can, for example, enable the customer to determine the cyber maturity of potential partners and to conduct a risk assessment in a corporate acquisition situation.

Cyberwatch Finland

Cyberwatch Oy | +358 40 500 8177
info@cyberwatchfinland.fi