FEDERAL SECURITY SERVICES:

CYBER OPERATIONS

DIAGNOSING PRODUCTIVITY AND VULNERABILITY

The nature of today's constantly evolving cyber landscape makes thinking beyond the next technological advancement an imperative. It is no longer enough to simply be familiar with your cyber operations network; you must know every possible interaction of its many interdependent systems and how they affect all aspects of your agency's infrastructure.

It is critical to have a deep understanding of all of the virtual moving parts of your cyber network and how these parts affect the information chain. The way these components determine interactions between people is only part of the scope of understanding. Securicon's knowledge of this bigger picture, and the use of specialized software tools and analysis of data, affords our skilled engineers the ability to diagnose cyber productivity as well as the vulnerability of your data during day-to-day operations.

The importance of providing continuous support in real-time is critical!

Only **one** applicable tool is required for an attacker to be able to connect to a weakness and exploit it.

A network's vulnerability is a combination of 3 factors:

- The discovered susceptibility or flaw
- The potential attacker's access to the flaw
- The attacker's capability to exploit the flaw

The ability to respond in a speed commensurate with the fast-paced operational environment requires careful monitoring and manning of a tactically-planned organizational construct that remains dynamic and fluid in a changing environment.

THOROUGH EVALUATIONS AND CONCLUSIONS

We use proprietary tools and vulnerability scanners to assess the strength of your cyber network, allowing our team to identify possible exposure points and mitigate any damage before it occurs. These vulnerabilities are then manually evaluated and rated according to technical severity. Then, a determination is made as to how they may impact your systems on the network and whether this vulnerability represents an actual exposure that could lead to data loss or theft.

SECURICON
Information Security Solutions

Securicon considers both the technical aspects and mission-critical objectives in our evaluation, and our conclusions and recommendations address both your IT architecture as well as your business functions. This allows for multiple possible solutions to remediate the potential risks discovered, and it enables us to predict the effectiveness of each countermeasure.

Do your cyber operations need strategic guidance?

Learn more about Securicon's expert solutions by giving us a call at 571-253-6565 or email us at sales@securicon.com.