

How STR-iCT helps our customers improve the security of their IBM i and their network



True Story 1: How STR-iCT Enabled Our Client to Identify an Attack Unfolding on Their Network

Our client

Our client is a group of 150,000 people, listed on the stock exchange. It has an AD-centric network and an external SOC to manage its security.

STR-iCT protects a dozen IBM i partitions.

The context of the attack

A few days after its installation, **STR-iCT** detected attempts to log in with the wrong logins/passwords. Our expert system has assessed the risk at a very high level, particularly in view of the profiles used for connection attempts.

STR-iCT identified the position that was at the origin of the access attempts. This position was in the hands of hackers who carried out a discovery of the network quietly, i.e. without being noticed. Moreover, the other Network Security systems had not identified it.

Early identification of this attack was fundamental to preserving the security and integrity of the data. The remediation made it possible to clean up the substation concerned before it committed the irreparable. No IBM i data leaks were noted.

REMEMBER

STR-ICT helps identify events during low-noise network discovery attempts that are difficult to detect. This step is generally the third level of an attack, after the initial access, which consists of taking control of a workstation on the network, and then the installation of the tools necessary for hacking.

Identifying and blocking the attack at this early stage prevents massive data leaks and the infestation of many network devices. The remediation is much simpler and the side effects much less deleterious.



Is a



For more information
i.gayte.it/str-ict
str-ict@gayte.it

You are an IBM partner,
an MSP hosting IBM i
or a SIEM distributor,
We have a partnership contract at
High added value for you :: i.gayte.it/ipp

