

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



## True Story 2: How STR-iCT Helped Our Customer Identify a Misconfiguration of Their Firewall

### Our client

Our client is a world-class service group. It manages dozens of IBM i partitions.

### The context

A few minutes after its installation, **STR-iCT** detected attempts to log in with the wrong logins/passwords to NetServer, the Windows file share for the IBM i. Our expert system assessed the risk at very high level, particularly in view of the profiles used for connection attempts and the origin of connections with external IP addresses.

No warning signal was coming up from IBM i. Our client had no way of being informed of these attacks.

**STR-iCT** quickly identified that the firewall that protects the network was misconfigured and was allowing SMB flows to pass through.

### The risk

The risk consisted of:

- Extraction of IFS data shared by NetServer and resale on the dark web or ransom demand in exchange for (potential) return, especially if there is personal data
- Exploiting the extracted data to commit other crimes
- Alteration or loss of IFS data shared by NetServer
- Ransomware encryption and ransom demand
- The ability to bounce back to other systems in the network

Early identification of this attack was fundamental to preserving the security and integrity of the data. Remediation consisting of reviewing the firewall configuration quickly closed the existing gap. No IBM i data leaks were noted.

## REMEMBER

**STR-ICT** is used to identify events during initial attempts to connect to the IBM i. This step is usually the first level of an attack that allows you to take possession of a system before proceeding to exploit this connection to spread across the network.

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](https://i.gayte.it/str-ict)  
[str-ict@gayte.it](mailto: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](https://i.gayte.it/ipp)

