Gazprom Neft

System for detecting external channels of communication with the Internet

Background / Problem statement:

For many large, geographically distributed companies concerned about their information security, detecting and neutralizing unauthorized Internet communication channels is a challenge. It's no secret that 80% of attacks occur from within a company, and one of the main things for a threat actor is the availability of uncontrolled channels of communication with the Internet.

These uncontrolled Internet communication channels can be organized via third-party (non-corporate) Internet access gateways (such as modems, smartphones, etc.).

The task in this case is to find unauthorized Internet communication channels that insiders have arranged via third-party (non-corporate) Internet access gateways (such as modems, smartphones etc.).

Task:

Develop an algorithm (flowchart), software module and the architecture for an information system (hereinafter referred to as 'the System') capable of searching for unauthorized Internet communication channels on corporate hosts connected to a corporate data network.

The following points should be taken into consideration:

- Internet access for corporate hosts is arranged via corporate proxy servers;
- Routing and network address translation (NAT) between the Internet and the internal ('insider') IP address within the corporate network is disabled;
- It's necessary to provide the ability to download information about hosts and accounts from the Active Directory for further analysis;
- A mechanism should be provided so the developed software module can be delivered to and periodically launched on hosts;
- The module in question must search for the maximum possible number of unauthorized proxies being used, including those specified in browser extensions, and other unauthorized communication channels;
- Functionality needs to be developed that will analyze the obtained results;
- Measures need to be implemented to protect the information communicated by the module in question and to protect the System;
- The System will be used by information security department officers.

Solution requirements:

The following must be provided for evaluation:

1. Algorithm (flowchart) showing the operation of a software module that will detect unauthorized Internet communication channels.
2. System architecture that will ensure the functioning of the software module.
3. Software module that searches for unauthorized Internet communication channels on corporate hosts connected to a corporate data network.

Technical requirements for the solution:

System architecture must be provided in the form of:

- A structured diagram showing all the servers, APMs and network equipment required for the System to operate. The diagram should also show the corporate infrastructure elements with which the System communicates (e.g. database management system servers, Active Directory servers, active networking equipment, APM, etc.).
- Text describing the System's information flows.

The software module must provide the host name, its IP address and network interface, timestamp and account that has an unauthorized channel with the Internet.

Evaluation criteria:

- Criterion: Quality of development of algorithm (flowchart) of the software module's operation
  Evaluation: maximum 5 - minimum 1.
- Criterion: Completeness of system architecture scheme
  Evaluation: maximum 5 - minimum 1.
- Criterion: Text description of the System's information flows
  Evaluation: maximum 5 - minimum 1.
- Criterion: Delivery of a debugged and operating software module
  Evaluation: maximum 5 - minimum 1.

Five extra points may be awarded for creative, distinctive and/or novel technical solutions.