Getting Started

- What is Discovery?
- What is Nimbusec?

What is Discovery?

Nimbusec Discovery's Mission

Nimbusec Discovery aims to identify all websites related to your organization and perform a passive security analysis by simulating *one single website visitor per domain*.

A Nimbusec Discovery report is an objective, external overview of your organization's global web presences with an IT-security focus. Such a report can be used for:

- security incident detection,
- risk evaluation,
- decision basis for subsequent continuous monitoring with Nimbusec Website Security Monitor.
- control for web application life-cycle management and penetration testing strategies.

Contrary to penetration testing tools, *Nimbusec Discovery does not simulate attacks or any kind of brute force scans and does not represent a risk to live web-applications*.

How is it done?

Nimbusec Discovery finds domains based on public WHOIS information and public search engine results. After Discovery *discovered* all domains, a passive security analysis is performed. This analysis includes actual security incidents like *malware distribution, defacements and reputation issues*. However, Nimbusec Discovery also detects preventive risk factors like *outdated and vulnerable applications* and problems with your website *encryption*.

Nimbusec Discovery only focuses on the initial landing page and does not analyze the entire website.

Tech talk.

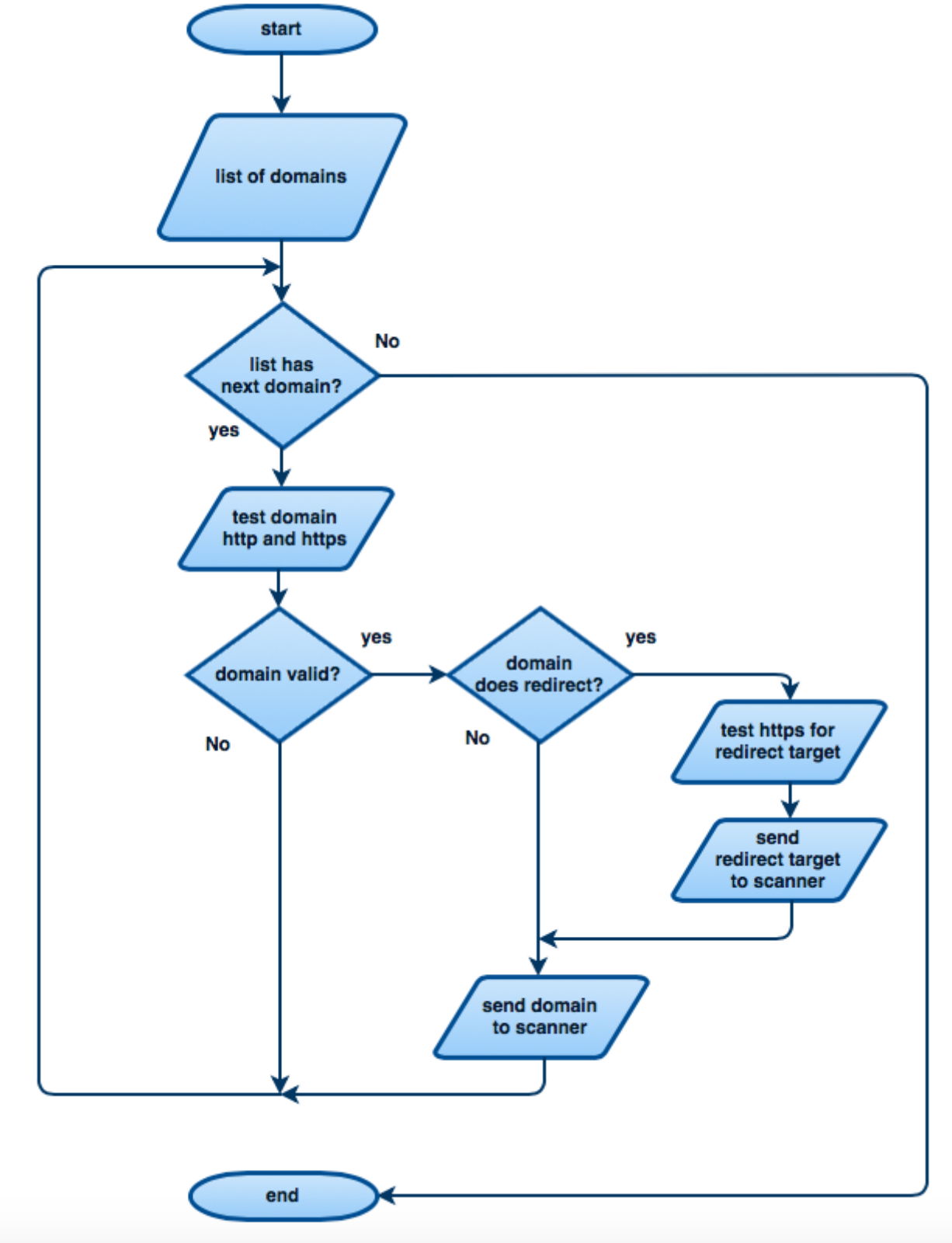
Technical speaking, Nimbusec Discovery transmits **3 HTTP requests** per FQDN (*fully qualified domain name*) to the webserver.

- HTTP request #1: Determine if page is accessible via HTTP.

- HTTP request #2: Determine if page is accessible via HTTPS and check certificate if available.
- HTTP request #3: Simulates one real website visitor that renders the entire website and downloads all linked resources. There are no additional clicks simulated after rendering the initial landing page.

Redirects

Very often an identified domain redirects to another (sub)domain. Nimbusec Discovery follows such redirects and eventually only scans the final redirect-chain target.



Example

http://example.com redirects to https://www.example.com

input is example.com

1. 1st req. --> try https://example.com (connection fail)
2. 2nd req. --> try http://example.com (connection success, status 301 redirect www.example.com)
3. 3rd req. --> try https://www.example.com (connection success, status 200)
4. 4th req. --> scan https://www.example.com (connection success, status 200).

The first 3 requests are comparable to a ping and do not download any additional resources or scripts. They only check whether the request is successful or not.

The 4th request then simulates one real website visitor and performs the analysis.

What is Nimbusec?

Nimbusec is a website security monitoring tool that notifies you, when your website was hacked or is in danger.

It allows you to react before your customers or your reputation are harmed.

- **Safe:** Nimbusec never exposes data of your servers to the cloud, respecting European Data Security Laws
- **Fast:** Depending on your plan you know what happened in minutes

Nimbusec also features:

- Notifications per mail and text messaging
- API for deep integration (SIEM, Ticketing Systems, Automated reactions)
- Plesk Panel Integration: Nimbusec Webhosting Security on Plesk Marketplace