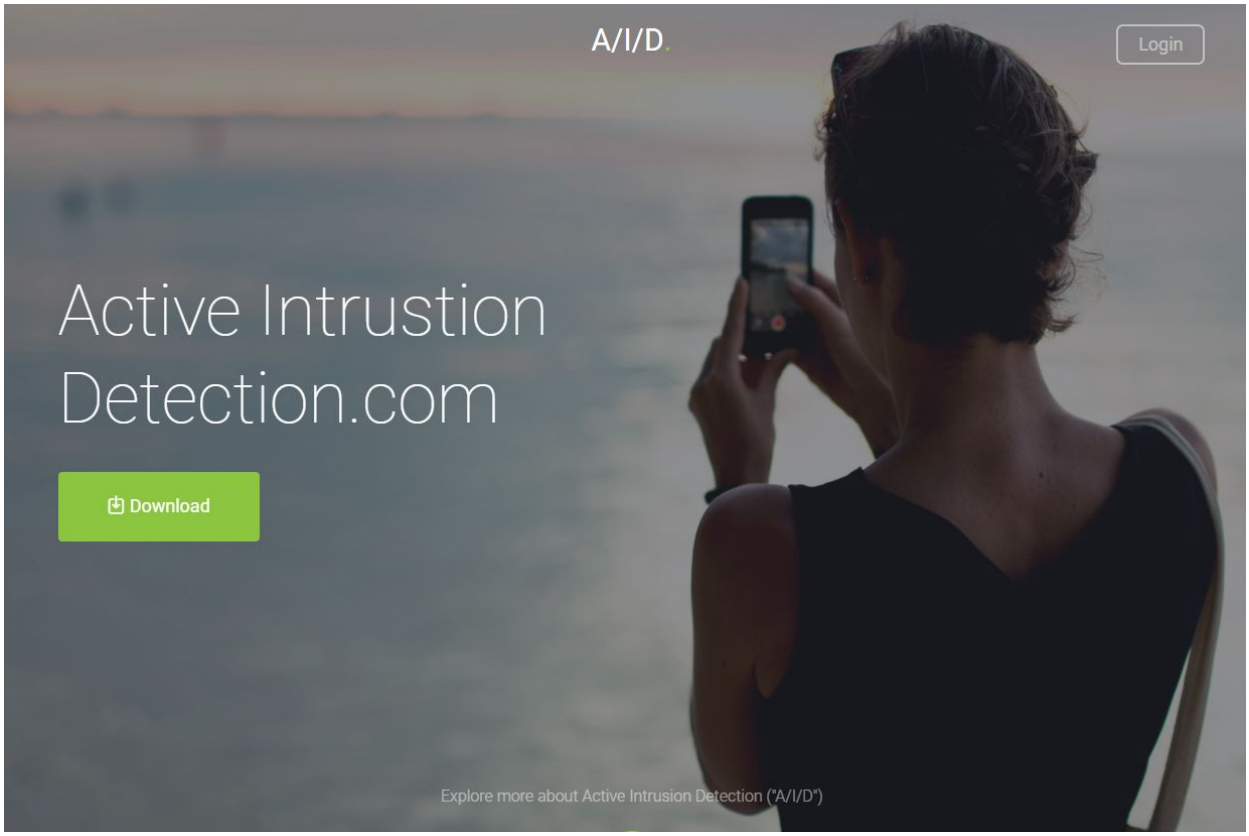

Active Intrusion Detection.com

06.07.2017

Infinite Loop Development Ltd
10 Nualamont Drive
Derry BT48 9PH,
N.Ireland

Overview

The weakest point of security on a network can often be its users. If a disgruntled employee emails your server passwords to a competitor, there is no firewall or antivirus that can detect this.

Systems like Firewalls and Antivirus software stop unauthorised users access your network, but authorised users being either careless or malicious with your sensitive data is not something that would be detected or prevented by standard network security.

What this software does, is allow you define a set of "Red Flags", which can be either password fragments, or other sensitive data, and then it will listen silently to network traffic until such time as the user tries to send this sensitive data insecurely over the network.

If an insecure transmission of sensitive data is detected, then immediately an email is sent to the network administrator, who can take action by resetting the passwords on any compromised systems, and track down the perpetrator of the leak via the user's computer name and IP address.

Although this system does not prevent the transmission of sensitive data over the network, it does detect when such transmission has occurred, and allows prompt action to limit the damage caused by such a leak.

API

1. A REST based JSON API exists at

   https://www.activeintrusiondetection.com/rest.aspx

   This API is designed for configuration purposes.
2. A SOAP based XML API exists at

   https://www.activeintrusiondetection.com/api.asmx

   This API is designed for setup and reporting.

REST API

The rest API has the following endpoints

/users/loginbyip

This returns users registered at the same IP address as called by the API - i.e. local installations.

/users/loginbyid/{userid}

This returns a user as identified by the user GUID

/users/login/{username}/{password}

This returns a user as identified by the user username and password

/users/update/{id}/{email}/{password}/{adaptorId}

This updates the user as specified by its identifier, setting the user's email, password, and selected network adaptor.

/redflag/add/{userid}/{keyword}

This adds a "Red Flag" with the content of {keyword} to the user as specified by its identifier.

/redflag/remove/{redflagid}

This removes "Red Flag" as specified by its identifier.

SOAP API

I. AddAdaptor

Adds a network adaptor to the user as specified by their user id. The endpoint also requires the name of the adaptor, and the local numeric id as enumerated by WinPCap offset by 1.

II. LoginById

This returns the user object as specified by their user id

III. RecordEvent

This records and reports a network data breach. It requires the user as identified by it's ID, The IPv4 addresses for Source and Destination, and the packet data in base64 format.

IV. Register

This creates a new user. It requires the local computer name as an identifier, in the case that there is more than one computer behind the same public IP.