HNG: Attack Surface Explorer Features List

Contents

[Visual Studio Integration 2](#_Toc198527393)

[Toolbar 2](#_Toc198527394)

[Menu Item 2](#_Toc198527395)

[Task List Integration 2](#_Toc198527396)

[TFS Work Items Integration 2](#_Toc198527397)

[Properties Pane Integration 3](#_Toc198527398)

[ASE Project Types 3](#_Toc198527399)

[ASE File Types 3](#_Toc198527400)

[Solution Explorer Integration 3](#_Toc198527401)

[Test Integration 3](#_Toc198527402)

[Testpoints Pane 3](#_Toc198527403)

[Resource Popup View 3](#_Toc198527404)

[Warning Pane Integration 4](#_Toc198527405)

[ASE Project Elements 4](#_Toc198527406)

[Attack Profile 4](#_Toc198527407)

[o Attack Tree View 4](#_Toc198527408)

[o Attack Map View 4](#_Toc198527409)

[o Dashboard 5](#_Toc198527410)

[Snapshots 5](#_Toc198527411)

[Reports 5](#_Toc198527412)

[Product Assessment Checklist 5](#_Toc198527413)

[Discovery & Testing 6](#_Toc198527414)

[Launch and Discovery 6](#_Toc198527415)

[Resources which contribute to Attack Surface 6](#_Toc198527416)

[Set Resource damage and exploitability magnitude 6](#_Toc198527417)

[Tests for each Resource Type 6](#_Toc198527418)

[Testpoint management 6](#_Toc198527419)

[Application crash dump 6](#_Toc198527420)

[Guidance 7](#_Toc198527421)

[Attack Surface Library 7](#_Toc198527422)

[TeamMentor Integration 7](#_Toc198527423)

[Licensing and Product Support 7](#_Toc198527424)

[Product Keys and Licensing Enforcement 7](#_Toc198527425)

[Update delivery 7](#_Toc198527426)

[Report a bug 7](#_Toc198527427)

[Customer support options 7](#_Toc198527428)

# Visual Studio Integration

### Toolbar

* Provides useful shortcuts
* Displays most commonly used items by default
* Customizable
* *Has pretty icons*
* *Matches look and feel of Visual Studio*

### Menu Item

* Provides links to major ASE features
* Provides link to BBS and Customer Support site
* Provides link to Help documentation
* Provides link to Purchase Site
* Feature links are disabled when out of context
* *Matches layout, look and feel of Visual Studio*

### Task List Integration

* ASE Tasks have own Category
* Tasks can be related to resources or other ASE artifacts
* Easy to list all Tasks related to resources or other ASE artifacts

### TFS Work Items Integration

* Reliable detection of TFS
* Work Items can be related to resources or other ASE artifacts
* Easy to list all Work Items related to resources or other ASE artifacts

### Properties Pane Integration

* Display useful information about ASE artifacts
* All configurable properties of ASE artifacts should be editable
* Uses Expand\Collapse to keep pane tidy
* ASE artifacts must be consistent in property naming and order

### ASE Project Types

* Project Types should cover most common type of applications
  + Desktop, Server, Middleware, Database etc.
* Application Questionnaire Wizard collects information about Test Application
  + Title of Test Application
  + VS Project Name \ Path to Test Application \ Service Name \ Process Name (attach on run) \ Unspecified (prompt for PID on run)
  + Deployment options: Intranet \ Internet \ Standalone – No Network \ IPSEC
  + Privilege Level Requirements

### ASE File Types

* VS New Item Dialog should list all ASE File Types: Attack Profile, Snapshot, Report and Checklist

### Solution Explorer Integration

* Project Settings should be viewable and editable
* Be able to launch Test Application from Attack Profile Node
* Allows more than one ASE Project per VS Solution

### Test Integration

* Common ASE Tests are available as Templates in the New Test dialog
* Test Results are shown in VS Test Results pane
* Allows creation of VS Tasks and TFS Work Items from VS Test Results pane

### Testpoints Pane

* Has similar look and feel to Breakpoints pane
* Allows disabling\enabling\creating\deleting Tests
* Visual property and\or column value of Testpoint is changed every time Test is executed
* Allows creation of VS Tasks and TFS Work Items from pane
* Allows information to be copied to clipboard

### Resource Popup View

* Provides information on selected resource or resource type from Tree or Map view
* Information should contain Available and Active Tests \ Test Results \ Attack Surface Library and TM content \ Resource Notes
* Allows setting tests for resource
* Allows writing notes for resource
* UI should make it clear to the user that information displayed is for resource selected in Tree\Diagram or Dashboard
* Cannot be hidden
* Allows information to be copied to clipboard

### Warning Pane Integration

* Contains warnings about failed Attack Surface Library checks
* Gets populated during discovery
* Allows direct creation of TFS workitem

# ASE Project Elements

### Attack Profile

* Considers only those resources which contribute to the attack surface
* Does not display or save information on resources accessed indirectly by OS
* Has the following views:

### Attack Tree View

* + - This view will have several columns with the following UI elements in them:
      * Tree View, Icon + Text, Icon + Text, Icon + Text
    - Displays resources in a well categorized manner as grouped by:
      * Channels, Methods and Data Items
      * Detailed Resource Types (Files, Registry Keys, Pipes etc.)
      * Alphabetically?
      * Ascending and Descending wrt user defined level of threat?
    - Filters can be used to hide information
    - Pre-set filters are provided to hide: Ignored items, Specific types of resources
    - Tree should allow fast searching
    - Search criteria can be saved as Filter
    - When filter is applied, enough visual feedback needs to be provided to signify that a filter is currently active
    - Resource nodes icons clearly signify the assigned threat level
    - Selecting a node should bring up the *Resource Popup View*
    - Allows tree items to be copied to clipboard
      * If one item is selected; copy node name and associated information from property page
      * If multiple items are selected; copy node names and maintain indenting

### Attack Map View

* + - Displays componentized view of Test Application using a diagram
    - Should have Filter and search options comparable to Attack Surface Tree
    - Resources objects should visually signify the assigned threat level
    - Clicking a resource object should bring up the *Resource Popup View*
    - Provides option to take save diagram as image file (jpeg, png) and\or copy to clipboard

### Product Assessment Checklist

* + - Provides a useful way of keeping track of security mitigations and other checks
    - The key questions asked shall be those described in the section named “Security Risk Assessment” and include appropriate items from the Setup, Attack Surface, Mobile-Code, Security Feature—Related, and General question list.
    - Should display related Attack Surface Library and TeamMentor content to help user understand checklist requirements
    - Allow users to add\edit questions and answers
    - Context menu allows for Email and\or Attachment as TFS Work Item
    - Show allow import\export from disk location
    - One ASE Project can have only one checklist.
    - Importing from disk location overwrites project Checklist
    - User should be notified of overwrite before importing

### Snapshots

* + - Saves all information available in a Attack Profile
    - Allows snapshot to be marked as read-only or locked
    - Allows comparison between snapshots
    - Allows export\import of snapshots
    - Allows Report creation
    - Allows users to write notes (such as milestone information or whatever)

### Dashboard

* Provides a comparative view of two or more Attack Surfaces
* Provides a temporal view of the Attack Surfaces
* Multiple Dashboards can be added to an ASE Project
* Dashboards can be moved across ASE Projects
* Dashboards can be exported\imported to\from disk

### Reports

### Live Reports

* + Provides a live summary view of the state of the Test Application

### Static Reports

* + Supports multiple views
  + Supports popular formats: HTML, XML, DOC, PDF
  + Can be generated from Live Reports, Snapshots, Attack Profile and Dashboard.
  + Context menu allows for Email and\or Attachment as TFS Work Item

# Discovery & Testing

### Launch and Discovery

* Discovery supports Test Application launch via VS (Project Name)
* Discovery supports Test Application launch via Attack Profile (**Launch**: Project Name \ Application Path \ Service Name. **Attach To**: PID \ Process Name \ Service Name)
* Discovery supports Test Application launch manually (**Attach to**: PID \ Process Name \ Service Name)
* Discovery can be paused\resumed

### Resources which contribute to Attack Surface

* Uses **entry-point\exit-point** and **damage potential-effort ratio** methodologies to list and prioritize resources
* Resources not accessed directly by the Test Application should not be displayed (Ex. by the OS)

### Set Resource damage and exploitability magnitude

* Resources can be assigned a Damage magnitude (Critical, Dangerous, Neutral, Not Dangerous, Inert)
* Resources can be assigned an Exploitability Magnitude (Given, Very Likely, Somewhat Likely, Not Likely, Very Unlikely)
* Resource Icons and other visual cues should instantly tell user about security magnitude of resource

### Tests for each Resource Type

* Relevant Tests should be available for each resource type
* Tests should include:
  + Fuzzing (from Holodeck 2.8)
  + Blocking
  + Permission Tweaking (in API call parameters)

### Testpoint management

* Testpoints pane should have look and feel of Breakpoints pane
* Displays all tests created by User
* Tests can be disabled and\or deleted

### Application crash dump

* If Test Application crashes a mini-dump should be packaged along with other information
* Mini-dump package can be exported to disk location
* Mini-dump package can be emailed
* Mini-dump package can be attached to a TFS Work Item
* If Visual Studio Debugger is present, User should be provided with the option to debug the crash right away

### ASE SDK

* Provides calls to start, pause, resume, stop discovery for a given Test Application
* Allows saving discovery information to a new or existing Attack Profile
* Allows creating Snapshots from an Attack Profile
* Allows creating Static Reports from an Attack Profile
* Allows creating Static Reports from Snapshots
* Provides calls to push a Snapshot or Attack Profile to a new or existing Dashboard

# Guidance

### Attack Surface Library

* Provides helpful guidance on known vulnerabilities or threats in the *Resource Popup View*
* Resources which match database artifacts with high confidence should be automatically marked as dangerous
* Looks for things that static analysis tools can’t do:
  + Look for things that run as admin, not following the principle least privilege.
  + Look for ways to grab programmatic CAS commands
* Library Checks are stored as Individual XMLs

### TeamMentor Integration

* Provides helpful guidance to related items in the Product Assessment Checklist
* TeamMentor pages should load inside VS IDE
* Should require subscription to TeamMentor for displaying full content; otherwise only trial summaries of topics are visible
* TM items reference related Attack Surface Library checks in their XML.

# Licensing and Product Support

### Product Keys and Licensing Enforcement

* Keys should bind to a specific machine using CPU serial# / MAC Address or a similar common attribute.
* Keys should be version aware
* Product should be disabled at the end of the trial –period
* Should be easy to purchase and register the product
* Registered product can be unregistered if the user desires OR un-installation of product should remove stored licensing information

### Update delivery

* User should be able to check for product updates
  + ASE Updates web page should load inside VS IDE

### Report a bug

* Bug reporting web page should open inside VS IDE
* ASE should automatically fill in web-fields that tell us about the user environment
  + Get user consent before automatically filling

### Customer support options

* Bulletin Board link should open page inside VS IDE
* Should allow email to customer support
* Should provide phone number for customer support