History

v1.3.1

- Modified the rule query so that any signatures that have a priority of 99 will not be shown when the "All" priority value is selected on the Rules tab. This allows for developmental rules to be used by snort, and allows analysts to work primarily on alerts generated by known good/production rules.
- Added new NetWitness query format for **Src <- -> Dest (Event Timestamps)**. Thanks CalG

v1.3.0

- Added DNS decoding which displays the DNS questions, Answers, Authoritive Answers and Additional answers. Thanks MattN. This closes github Issue #2
- Prevented the ASCII view from detecting URL's. Thanks JonathanD
- Ensures that the AppData directory exists before attempting to save the application settings. Thanks DanO
- Changed the Filter form to not load a distinct list of priorities from the DB, which greatly improves the form load speed
- Added the priority to the Misc tab on the Event Info control

v1.2.8

- Fixed the exporter on the Rules tab as the query column name had changed
- Added Payload (HEX) to the exporter on the Rules tab. Thanks RussellH

v1.2.7.1

- Fixes to the acknowledgement exporting. Thanks DanO

v1.2.7

- Updated the MySQL .Net provider to v6.8.3.
- Updated NPoco to v2.4.67
- Added/readded Sensor to the the Misc tab on the lower event details tab. Thanks RussellH
- Prevented Acknowledgment.Description being processed by NPoco. Thanks DanO

v1.2.6

- More fixes to acknowledgment queries. Thanks DanO
- Included new acknowledgment classes. Thanks MattN
- Modified the acknowledging to include a "Successful" flag to allow for more granular classification. Thanks MattN

v1.2.5

- Fixed acknowledgment queries. Thanks DanO

v1.2.4

- Fixed SQL queries where a join occurred to the acknowledgement table. Thanks CalG
- Added an auto-refresh to the Events list. To configure set the EventsRefresh attribute in the Settings.xml
- Modified Acknowledgement schema to increase the 'notes' field from VARCHAR 100 to 500
- Updated 'rule_importer.py' so that there is a bulk mode. Thanks AdrianC
- Modified the Events list query as it was limiting the number of results returned due to the LIMIT clause being performed on a sub-query
- Added new Acknowledgement tab which displays the Initials, Timestamp, Classification and Notes for an individual event
- Modified the Search tab to allow LIKE/NOT LIKE wild card searches on the Acknowledgement Notes field

v1.2.3

- Modified the Search tab to allow IP (Source & Destination) range searches e.g. IP > 10.0.0.1 AND IP < 10.0.0.254. Thanks OliverF
- Modified the Search tab to refresh the search results when the "Condition" drop down is change
- Modified the IP address control used on the Filter window so that TAB works within each segment within the IP address
- Modified the "Extract Unique IP" functionality so that the output is in either list or CSV form. This allows for easier queries in other software such as NetWitness where the IP list is expected in CSV form. Thanks ChrisB

v1.2.2

- Add more command replacement strings (Thanks DanO) e.g.

```
#SENSOR_NAME#
#TIMESTAMP#
```

- The commands functionality now URL encodes the data if "http" or "https" is detected
- Corrected a missing colon in the python rule importer script. Thanks DanO

v1.2.1

- Removed erroneous Tools menu entry e.g. import rules. Thanks DanO
- Fixed the extract unique source/destination IP address functionality. Thanks DannyF

v1.2.0

- Added new "rules" table to the barnyard/snort schema which will store the signature/rule information. This removes the import process which occurs on startup and therefore the dependency on SQL CE
- Added new button to Event Info tab that displays the linked rules. This functionality looks at the "flowbit" data for the snort rule
- Updated IP Address control to r57

v1.1.10

- Fixed issue where the rules query errored when a sensor and priority were selected. Thanks CalG
- Modified the highlighted item colour for the Rules drop down list as when viewed under a low colour RDP session it was unreadable e.g. black text on a dark blue background. Thanks MattN

v1.1.9

- Fixed issue where an error occurred when the final rule is acknowledged. Thanks ChrisB

v1.1.8

- Updated the SQL_RULES_EVENTS query and the calling code to include the LIMIT statements as the number of parameters supplied varied depending on whether the "To" timestamp value was required

v1.1.7

- Modified the Acknowledgement export to include the Acknowledgement class (reason)

v1.1.6

- Rewrote most of the queries involved in the loading of rules and events so that it is easier to view events that have already been acknowledged. Thanks DannyF
- Rewrote the rest of the queries to use dynamic WHERE clauses which has reduced the query files from 31 to 17
- Corrected tab order on the Acknowledgement Export window
- Removed selected item check when extracting unique source/destination IP addresses. Thanks ChrisB

v1.1.5

- Added more error checking when performing the acknowledgements
- Added combo box selected index checks when the Rule checks are performed
- General tidy up of some forms so they are consistent
- Updated the list column resizing to reduce redraw messages. Thanks DanO

v1.1.4

- Fixed a bug in the Rules drop down height calculations

v1.1.3

- Added alerting where new events are alerted to the user. The alerts are configurable via the Alerts.xml file (stored in the users local %AppData% for snorbert)

- Added the ability to search on Initials and Acknowledgement Class
- The Rules tab will now only show events that are not acknowledged or have an Acknowledgement of Taken
- Added the ability to Export Acknowledgments to text format as well as TSV
- Sets the Rules dropdown list height to 75% of the main window's height. Thanks DannyF
- Removed the query already running checks in the Querier object
- Added Enter key accept on the Filter window. Thanks DannyF
- Fixed context menu item for Acknowledging. Thanks DannyF
- Added CTRL-ALT-A acknowledging to Search and Events tab. Thanks DannyF
- Updated Search SQL query to include Acknowledgement data. Thanks DannyF
- Fixed the acknowledgement export queries e.g. parameters in wrong order where initials are supplied
- The Acknowledgment Export Window now closes once the export is complete
- Changed the search terms on the Search tab from "Any,All" to "OR,AND"

v1.1.2

- Modified the keyboard shortcuts to:

  CTRL-ALT-A (Show Acknowledgement window)
  CTRL-ALT-S (Show Signature window)

v1.1.1

- Added Signature columns to the Events and Search tab listviews. Thanks JonathanD
- Added filtering and grouping to the Events and Search tab listviews. Thanks JonathanD

v1.1.0

- Fixed issue where the Rules query failed when a particular sensor was chosen and a To date was selected. Thanks DannyF
- Reorganised the code e.g. moved Forms to separate form, same for Controls
- Added ability to include source and destination ports when excluding. Thanks DannyF
- Modified the Exclude window to display the protocol. The protocol is also saved with the Exclude record
- Modified the Commands.xml loading so that it does not error when the file does not exist
- Added extra checks when loading rules e.g. sensor or priority not selected
- Set the Enter key to close/accept the Acknowledgement window. Thanks MattN
- Renamed NetWitness query from “Source->Destination“ to “Src <- -> Dest”. Thanks MattN
- Added “notes” field to acknowledgement table
- Moved all SQL queries to separate files as the current Sql.xml file was getting cumbersome
- Added the ability to categorise from the Search tab. Thanks DannyF
- Added the ability to export all acknowledgements for the selected period and user (initials). (File->Export->Acknowledgements). Leave the Initials textbox blank to get all acknowledgements for the period
- Changed all “Task.Factory.StartNew” code to “new Thread”
- Added a new Misc tab. The new tab shows the sensor name, and the events SID and CID
- Wrapped Acknowledgements with a transaction so the inserts should be quicker
- Modified the Acknowledgements to prevent duplicates. Thanks ChrisB
- Added the Enter key to search when using the Find functionality from the Payload window. Thanks DannyF
- Added keyboard shortcuts to speed up acknowledging. Thanks CalG

  CTRL-ALT-F (False Positive)
  CTRL-ALT-T (Taken)

- Added keyboard shortcuts to speed up analysis

  CTRL-ALT-P (Show payload window)
  CTRL-ALT-A (Show the signature window)

- Added "Web Based Attack" item to the Acknowledgement classes data

v1.0.16

- Modified the acknowledge setting to ensure that no controls are accessed from the background thread

v1.0.15

- Fixed bug on the Search tab where the signature name couldn't be searched. Thanks DannyF

v1.0.14

- Modified the Rules tab context menu to include a Signature option which will display the signature window without having to change the Event Info tab
- Updated the Sensors tab query as barnyard does not update the timestamp of the last event. Thanks DanO
- Fixed issue where the SID's of signatures may be the same. Thanks DanO
- Added the signature GID to the Rule combox. Thanks DanO

v1.0.13

- Modified to allow the filtering of Rules on a per sensor basis
- Modified to allow user configurable commands to be executed via the Rules list context menu. The commands are stored in the Commands.xml file located in the user's application data directory for the application. The command strings will have data substitutions applied using the following mark up so that event data can be passed to the commands:

```
#IP_SRC#
#IP_DST#
#PORT_SRC#
#PORT_DST#
#PROTO#
#SENSOR_ID#
```

- Modified to allow better multi-user collaboration. The user can now right click on an event(s) and use the Acknowledgment context menu item to categorise the event. The user should set event(s) to "Unclassified" when initially looking into an Event, and then assign the actual category once the analysis is complete

- Modified to set use F1 key to set the current set of events to Taken

v1.0.12

- Modified to allow the deletion of multiple excludes in one go. Thanks DannyF
- Modified to allow the export of the current rules on the Rules tab. This is designed to make off line working/note taking easier
- Added two new NetWitness queries e.g. prior traffic to a source host, and prior traffic to a destination host. These queries will locate all traffic to the selected host for a period of two minutes before the event timestamp and one minute after

v1.0.11

- Modified to change mutex permissions

v1.0.10

- Updated NetWitness query. Thank DanO

v1.0.9

- Fixed the search tab so that condition combo box is showing. Thanks DannyF
- Modified the NetWitness query generate to include the NWS prefix for SSL connections

v1.0.8

- Fixed bug in copy functionality
- Modified the NetWitness query generation as the generated query was too complex. Thanks ChrisB
- Added Find window/functionality for use in the Payload window. Thanks ChrisB
- Added the ability to copy the Host column value via the context menu
- Added Enter key event handler to the Rule list which displays the Payload window. Escape now closes the Payload window
- Modified Find window to catch F3 to continue finding text

v1.0.7

- Modified the context menu displayed on the Rule tab so that the menu items are more appropriately enabled/disabled depending on what is selected
- Added new window to display the payload details. Double click the entry to display. Thanks ChrisB

- Added the ability to group the list items. Use the context menu by right clicking on the list header. Thanks MattN
- Enabled the ability to filter the list items. Use the context menu by right clicking on the list header
- Added Host column to list views (Events, Rules, Search) which is parsed from the ASCII payload. Thanks ChrisB
- Recoded all data access to use NPoco rather than Massive
- Removed the preloading of all possible signature names and ID's for the Search facility due to performance issues on slow infrastructure
- Moved the localised rule storage from ESENT to SQL Server CE to permit the opening of multiple instances of the application
- Added Netwitness query string generation. Right click on an event, select Netwitness Query menu item. Thanks MattN

v1.0.6

- Corrected Exclude functionality to reverse byte order of IP addresses. Thanks ChrisB

v1.0.5

- Added the ability to export the current events from the Rules tab to a TSV file. Use the context menu to export
- Added the ability to export all events associated with the current ruleset/time period defined on the Rules tab to a TSV file. Use the context menu to export
- Modified the event loading to recalculate the total records loaded using the number of records loaded
- Reworking of the Hide functionality. It now uses a table within the snort database e.g. "exclude". Thanks MattN
- Added the ability to export all Excludes to TSV for offline analysis
- Added the ability to filter the Rules by Priority. Thanks MattN
- Added alternative row colours. Thanks ChrisB

v1.0.4

- Fixed Rules paging label positioning/anchoring
- Added the ability to extract distinct source/destination IP addresses for a specific rule/date/date range. Access the functionality by using the context menu on an Event. This functionality applies to the Rules tab

v1.0.3

- Updated the rule import to prevent old rules being discarded
- Fixed bug where the Rules drop down list displayed duplicate rules
- Fixed import paths e.g. from application directory to user app data directory
- Added a default MySql connection string example when creating a new connection

v1.0.2

- Modified the Sensor tab to prevent it automatically loading at start up, as some instances may not be accessible. To refresh the Sensor data a new refresh button has been added to the top of the tab
- Removed the Error & Exclamation error handlers within the four main user controls as they were unnecessary

v1.0.1

- Modified the Rules database to store within the users local app data directory. This prevents issues when running with multiple users logged into the same time. Thanks DanO for reporting this on behalf of TomB ;-)
- Modified the Connections config file to store within the users local app data directory
- Modified the Settings config file to store within the users local app data directory
- Modified the HEX view context menu to allow copying of the HEX with and without spaces
- Added the ability to filter out particular events e.g. false positives. The functionality only applies on the Rules list. A false positive entry relates to a particular attribute e.g payload LIKE "test" or Source IP = 192.168.0.100. The false positive data is stored in an XML file under the users local app data directory. Thanks ChrisB

v1.0.0

- Help file added
- Public release

v0.0.3

- Updated the rule import to update existing rules
- Added event handlers for Sensor user control so that messages can be transmitted back to the main UI
- Modified the Event user control to just use next/previous paging as a record count takes too long

- Added the ability to search on Sensor
- Added the ability to search on Protocol (TCP, UDP and ICMP)
- Moved all of the querying to a separate object so that the queries can now be easily run on a background thread
- Increased the granularity of the Page Limits, for very slow connections!
- Moved the “Connections.xml” and “Settings.xml” to a new “Config” folder
- Moved all of the hard coded SQL queries to a new config file (“Sql.xml”). The file resides in the new “Config” folder
- Added TCP flag decoding to the events list. The events is displayed on the Event, Rules and Search tabs

v0.0.2

- Fixed context menu Source Port copy
- Fixed import rules error which resulted in a Disposed object exception
- Added To Date/Time filtering. Thanks TomB
- All controls/lists clear when the Rules combo is refreshed
- Fixed “No Object in Sequence” error when editing an existing connection
- Moved the Connections/Page Limit controls to the toolbar
- Added new Events tab, which displays all events, ordered by event.timestamp, includes paging support
- Rule files are now copied to the Import directory when a manual rule import is performed. This will ensure that the Settings file will contain the file details and reimport will not occur
- Add new Search tab, which allows for user configurable searching on the key fields
- Re-implemented UI code base using User Controls rather than one massive code dump in the main window
- Added custom context menu to the HEX control to allow the copying of the HEX value as well as the ASCII
- Added Sensor tab which displays information relating to the snort sensors

v0.0.1

- Initial release