

CLAIMS:

1. A cyber threat intelligence identification, integration and analysis system comprising:
 - a) an intelligent selector that receives two parent forms, wherein the parent forms represent abstract constructs of data, and merges the two parent forms into a hybrid form;
 - b) a mode module that defines the type of an algorithm in which the system is being used, wherein the intelligent selector decides parts to merge based on the type of the algorithm;
 - c) a static criteria module that receives input of customization data for how forms should be mergedwherein the intelligent selector comprises a raw comparison module that performs raw comparison on the two parent forms based on the customization data provided by the static criteria module, wherein the raw comparison module outputs regarding changes and non-changes, wherein the intelligent selector ranks importance of the changes based on the customization data, wherein the changes and the non-changes are merged into a hybrid form based on the customization data of the static criteria and the type of the algorithm of the mode.
2. The system of claim 1, wherein the customization data comprises ranking prioritizations, desired ratios of data, and data to direct merging which is dependent on the type of algorithm defined by the mode module.
3. The system of any of previous claims, wherein the merging comprises adjusting ratio distribution of data, importance of data, and relationship between data, wherein a ratio mode, a priority mode, and a style mode are preset in the system.
4. The system of claim 3, wherein in the ratio mode, the amount of overlapping information is filtered through according to the ratio set by the Static Criteria, wherein if the ratio is set to large then a large amount of form data that has remained consistent will be merged into the hybrid form, wherein if the ratio is set to small then most of hybrid form will be constructed has a very different from its past iterations.
5. The system of claim 3, wherein in the priority mode, when both data sets compete to define a feature at the same place in the form, a prioritization process occurs to choose

which features are made prominent and which are overlapped and hidden, wherein when only one trait can occupy in the hybrid form, a prioritization process occurs.

6. The system of claim 3, in the style mode, the manner in which overlapping points are merged, wherein the Static Criteria and mode direct this module to prefer a certain merge over another.

7. The system of any of previous claims, wherein a trait makeup and indexed security Points of Interest (POI) are provided to query security events with their responses, wherein the POI's are stored in a security POI pool, and POI's are bridged with the trait index, wherein when a personality trait regarding a security issue is queried, relevant POI's are looked up in the POI pool and the relevant Event and Response storage are retrieved and returned, wherein in a POI interface module, personal traits are associated with POI's.

8. The system of any of previous claims, further comprising a response parser, which comprises:

- a) a cross reference module, in which that data describing a security event and a response to the security event are received; the security behavior module provides known POI, and input for a personality trait tagged to a security event is received;
 - b) a trait tagging module that associates the security response with personal trait based on prescription of the personal trait and pattern correlation from past security behavior; and
 - c) a trait interaction module that receives a trait makeup from the trait tagging module, and assesses its internal compatibility;
- wherein the security event, response, trait are stored in the security behavior cloud.

9. The system of any of previous claims, wherein a security ruleset is tested with an artificial exploit, wherein after an exploit is performed, result feedback module provides the result if the exploit worked and if it should be incorporated into the Exploit DB, wherein an information release module provides details to a creativity module for how the next exploit should look like, wherein information is merged between the information release module and the Exploit DB, wherein the exploit is performed as a batch in which all the evolutionary pathways get tested in parallel and simultaneously with the same exploit, wherein the creativity module produces a hybrid exploit that uses the strengths of prior exploits and avoids known weaknesses in exploits based on result by the information release module

wherein an oversight management module monitors developments in an exploit storage and usage, wherein exploits are produced/modified/removed by external inputs, wherein the exploits are stored along with known behavioral history that describes how the exploits performed in the past within certain conditions and exploit importance.

10. The system of any of previous claims, further comprising a monitoring/interaction system, in which a creativity module produces the next generation for a pathway, wherein two input forms are compiled security behavior from a security behavior cloud, and variables from a security review module, wherein the resultant hybrid form is pushed to an iteration processor, wherein the iteration processor processes the hybrid form pushed from the creativity module, and assembles a new generation, and loads the new generation into the relevant evolutionary pathway, wherein the security review module receives report variables from the evolutionary pathway, and evaluates its security performance against the Artificial Security Threat (AST) system, outputs report for further review, and sends the report to the creativity module to iterate the next generation, wherein the security behavior cloud supplies relevant events and responses to the security review module, wherein the criteria is determined via a trait index query, wherein if a good performance evaluation is received, the security review module attempts to find a better exploit to break the exploit in the security behavior cloud, wherein the trait makeups are provided to the security behavior cloud and the security behavior cloud provides the trait makeups to the creativity module to guide how the generational ruleset should be composed, wherein an automated growth guidance system intervenes between external control and the monitoring and interaction system, wherein a module type discerns what the desired module behavior is, and wherein forced feedback is a response by a module informing about its current condition every time it is given new instructions, wherein high level master variables are externally input to the static criteria, wherein the creativity module discerns a new desired result after being given the previous desired result and the actual result, wherein the actual result that comprises status and state of the controlled module is stored in a module tracking DB, wherein the module tracking DB is populated by the module and the creativity module, wherein the module tracking DB provides an input form to the creativity module which reflects the internally chosen growth pattern for the controlled module, wherein the creativity module pushes the new controls for the module to the module tracker and the module itself, wherein the modules are controlled in parallel, except that the module tracking operates in a single instance and is partitioned to deal with multiple modules

simultaneously, wherein the feedback from the controlled module, which comprises information derived from actual module history, is stored in a realistic DB, wherein a theory DB contains theoretical controls for the module, which are provided by the creativity module, wherein if a control performs as expected then the same growth pattern is kept, and if a control performs odd, then alternate growth pattern is adopted.

11. The system of any of previous claims, further comprising a malware predictive tracking algorithm, in which an existing malware is iterated to consider theoretical variances in makeup, wherein as the theoretical time progresses, the malware evolves interacting with a creativity module, wherein CATEGORY A represents confirmed malware threats with proven history of recognition and removal, CATEGORY B represents malware that the system knows exists but is unable to recognize nor remove with absolute confidence and CATEGORY C represents malware that is completely unknown to the system in every way possible, wherein the process starts from category A, wherein known malware is pushed to the creativity module to produce a hybrid form which includes potential variations that represent currently unknown malware, wherein then based on category B, a theoretical process represents the best estimate of what an unknown threat is like, wherein a process based on category C represents the actual threat that the system is unaware of and trying to predict, wherein a pattern is produced to represent the transition of a known and confirmed iteration, wherein the transition pattern is used to predict a currently unknown threat.

12. The system of any of previous claims, further comprising a critical infrastructure protection & retribution through cloud & tiered information security (CIPR/CTIS) that comprises trusted platform security information synchronization service, wherein information flows between multiple security algorithms within a managed network & security services provider (MNSP), wherein all enterprise traffic within an enterprise intranet, extranet and internet are relayed to the MNSP cloud via VPN for realtime and retrospective security analysis, wherein in the retrospective security analysis, events and their security responses and traits are stored and indexed for future queries, conspiracy detection provides a routine background check for multiple security events and attempts to determine patterns and correlations, parallel evolutionary pathways are matured and selected, iterative generations adapt to the same AST batch, and the pathway with the best personality traits ends up resisting the security threats the most, wherein in the realtime

security analysis, syntax module provides a framework for reading & writing computer code, purpose module uses syntax module to derive a purpose from code, & outputs such a purpose in its own complex purpose format, the enterprise network and database is cloned in a virtual environment, and sensitive data is replaced with mock data, signal mimicry provides a form of retribution used when the analytical conclusion of virtual obfuscation has been reached, wherein it checks that all the internal functions of a foreign code make sense, uses the syntax and purpose modules to reduce foreign code to a complex purpose format, detects code covertly embedded in data & transmission packets, wherein a mapped hierarchy of need & purpose is referenced to decide if foreign code fits in the overall objective of the system.

13. The system of any of previous claims, further comprising a logically inferred zero-database a-priori realtime defense (LIZARD), in which every digital transfer within the enterprise system is relayed through an instance of LIZARD, wherein all outgoing/incoming information from outside the enterprise system are channeled via the LIZARD VPN and LIZARD cloud, wherein an iteration module (IM) uses a static core (SC) to syntactically modify a code base of dynamic shell (DS), wherein the modified version is stress tested in parallel with multiple and varying security scenarios by an artificial security threat (AST), wherein if LIZARD performs a low confidence decision, it relays relevant data to AST to improve future iterations of LIZARD, wherein AST creates a virtual testing environment with simulated security threats to enable the iteration process, wherein the static core of LIZARD derives logically necessary functions from initially simpler functions, converts arbitrary generic code which is understood directly by syntax module, and reduces code logic to simpler forms to produce a map of interconnected functions, wherein iteration expansion adds detail and complexity to evolve a simple goal into a complex purpose by referring to purpose associations, wherein a virtual obfuscation module confuses & restricts code by gradually & partially submerging them into a virtualized fake environment, wherein malware hypothetically bypasses an enterprise security system, LIZARD has a low confidence assessment of the intent/purpose of the incoming block of code, the questionable code is covertly allocated to an environment in which half of the data is intelligently mixed with mock data, a real data synchronizer intelligently selects data to be given to mixed environments & in what priority, and a mock data generator uses the real data synchronizer as a template for creating counterfeit & useless data.

14. The system of any of previous claims, further comprising a clandestine machine intelligence & retribution through covert operations in cyberspace module, in which a sleeper double agent silently captures a copy of a sensitive file and the captured file is pushed outside of an enterprise network to a rogue destination server, wherein standard logs are generated which are delivered for real-time and long-term analysis, wherein real-time analysis performs a near instant recognition of the malicious activity to stop it before execution, and the long-term analysis recognizes the malicious behavior after more time to analyze.

15. The system of any of previous claims, further comprising a critical thinking, memory and perception algorithm that produces an emulation of the observer, and tests/compares all potential points of perception with such variations of observer emulations, wherein priority of perceptions chosen are selected according to weight in descending order, wherein a policy dictates the manner of selecting a cut off, wherein perceptions and relevant weight are stored with comparable variable format (CVF) as their index, wherein CVF derived from data enhanced logs is used as criteria in a database lookup of a perception storage, wherein a metric processing module reverse engineers the variables from selected pattern matching algorithm (SPMA) security response, wherein a part of the security response and its corresponding system metadata are used to replicate the original perception of the security response, wherein debugging and algorithm trace are separated into distinct categories using traditional syntax based information categorization, wherein the categories are used to organize and produce distinct security response with a correlation to security risks and subjects.