Cyber Streaming Effects and Analytic Languages – Cyber SEAL™

Cyber SEAL™ is a suite of tools for real-time attack detection, response, and threat emulation. Originally developed from the ground up at MITRE for tactical environments, this suite of tools has also been successfully applied to enterprise IT networks.

Why Cyber SEAL™?

Near Real-Time & Low SWaP: Tactical environments, including all moving platforms in air, land, sea, or space, must be able to survive cyber attacks during active operations. Cyber attacks can have devastating effects. Defending against them is always challenging, especially in a tactical environment that does not have the computing resources found in larger facilities. Therefore, a cyber defense tool-set is needed. It must operate with low Size, Weight and Power (SWaP) in near real-time and be easily integrated with existing systems, which often generate data in proprietary formats. Cyber SEAL™ uses the same monitoring techniques, whether in a real-time event stream or in logs collected in a file, and produces evidence of the anomaly along with an anomaly alert.

Cyber SEAL allows users to quickly complete analyses of diverse network traffic with a level of fidelity and reliability far greater than what could have been accomplished manually.

MITRE

Cyber Streaming Effects and Analytic Languages – Cyber SEAL™

Cyber Tools for System Operators: Current Cyber defensive tools require cyber skilled operators who are in short supply. Therefore, the Cyber SEAL™ tool-suite is ideal for the non-cyber-savvy.

What is Cyber SEAL™?

Cyber SEAL™ monitors for anomalies in specific events and/or event streams such as system logs, network traffic, and sensor data, encoded in diverse, and sometimes proprietary, formats and protocols. These anomalies can be deviations from a previously generated baseline by Cyber SEAL™, or multi-event state machine based analytics. Cyber SEAL™ supports system security monitoring with a unified and easy-to-use set of Graphical User Interfaces (GUI) for non-cyber-savvy operators. Cyber SEAL™ alerts can also be integrated with commercially available Security Information and Event Management (SIEM) tools.

Cyber SEAL™ can be used to generate attack data sets for complex, multi-stage attacks. This tool-set is supported by graphical programming, libraries, test features, and translators.

Cyber SEAL™ use cases

Baseline configuration analytics: Attackers may attempt to modify system configurations to support hostile activity or data extraction. Cyber SEAL™ learns your system's baseline configuration and continually monitors for deviations from normal behavior.

Periodic bus analytics: Hostile cyber activity may cause missed messages on a periodic bus (e.g., MIL STD 1553, CAN, ARINC 429), or inconsistencies in the interarrival timing of periodic events. Cyber SEAL™ can detect these anomolies and alert users to the risk.

Reduce SIEM data volume: Cyber SEAL™ can reduce the volume of data collected by SIEMs and speed up detection of anomalous behavior by providing alerts of baseline changes.

Post-collection analytics: Cyber SEAL™ can detect anomolies and alert users to a cyber risk from files of logs collected from remote environments such as aircrafts.

Non-cyber-savvy operator response: Cyber SEAL™ provides indication-of-compromise alerts along with simple operator instructions for next steps to resolve the issue.

Attack dataset generation: Cyber SEAL™ can be used to generate attack datasets for simulateously occurring multiple multi-stage attacks.

For more information about licensing Cyber SEAL for commercial use, contact: techtransfer@mitre.org.

Cyber SEAL™ Tools

Happened-Before Language (HBL™)

General-purpose language and detection engine for complex queries and analytics across different communication architectures, protocols, and operating systems.

Effects Language (EL™)

Visual language and orchestration engine that enables emulation of multi-stage attacks and adversary Tactics, Techniques, and Procedures (TTPs).

eLEARN™

General-purpose baseline deviation detection engine that works on system configurations in multiple environments.

EdgeReactor™

Graphical User Interface (GUI) for tactical system operators that provides response options based on detected indicators of compromise.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.