Bio-inspired agile cyber-security assurance framework (BICSAF)

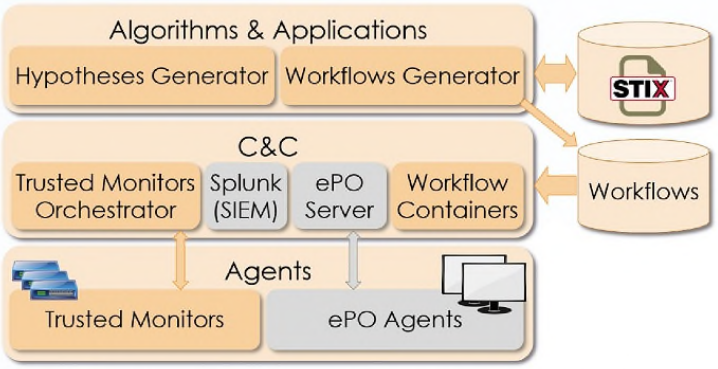
BICSAF – an **autonomous** deep dive for advanced cyber-security forensics

State-of-the-Art

Current Intrusion Detection systems rely on anomaly detection, expert rules and threat signatures to identify cyber-attacks and raise alerts.

Advanced investigations and threat hunting are performed manually by cyber security analysts.

Architecture



The hardware agents perform trusted monitoring to ensure integrity of the data collected by the software agents

Approach

1. Threat intelligence is fed in STIX format to update the BICSAF Attacks Knowledgebase, which organizes the information at multiple levels of abstraction: Indicators of Compromise, tools, malwares and attack patterns.

2. BICSAF introduces two innovative components that increase the level of automation during forensic investigations and aid the security officers during strategic decision making.
   - The **Attack Hypotheses Generator** module predicts the set of tools, malware, and attack patterns used by the attacker during the investigated incident.
   - The **Workflow Generator** module provides the analyst with ready-to-execute distributed threat hunting programs (termed "workflows").

Advantages

Being an agile and adaptive forensic investigation framework, BICSAF automatically hunts down cyber attacks in an organization!

Since BICSAF analyzes current and comprehensive threat intelligence information, it constantly evolves and matures; making itself capable of detecting even the newest cyber-threats that may appear overtime.

Therefore by using BICSAF, one can ensure quality and relevance of forensic investigation results while enhancing and improving the security defense of an organization.

Prof. Yuval Elovici, Dr. Rami Puzis, Dr. Polina Zilberman, Elad Marco, Aviad Elitzur
Cyber@Ben-Gurion University of the Negev, Israel
elovici@bgu.ac.il