ISSN: 2473-4901
v8 n5771

Command and Control – Revisiting EATPUT as an IS Model for Understanding SIEM Complexity

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department
St. Vincent College
Latrobe, PA 15650

Abstract

Automation of network security systems has led to ever increasing complexity and opaqueness. Ceding command and control actions to systems that are fully or even partially unknown to administrators can lead to possibly catastrophic results. Theoretical abstract models can aid in gaining visibility and insight into the construction and operations of these systems. This paper will utilize the early command and control information system~~s~~ model EATPUT to allow a better understanding of the stages and operation of a modern Security Incident Event Management (SIEM) system.

Keywords: EATPUT, Information Systems, SIEM, Cybersecurity Models

A full version of the abstract may be found at https://cppj.info