Exploit, Malware and Vulnerability (EMV) Scoring Application

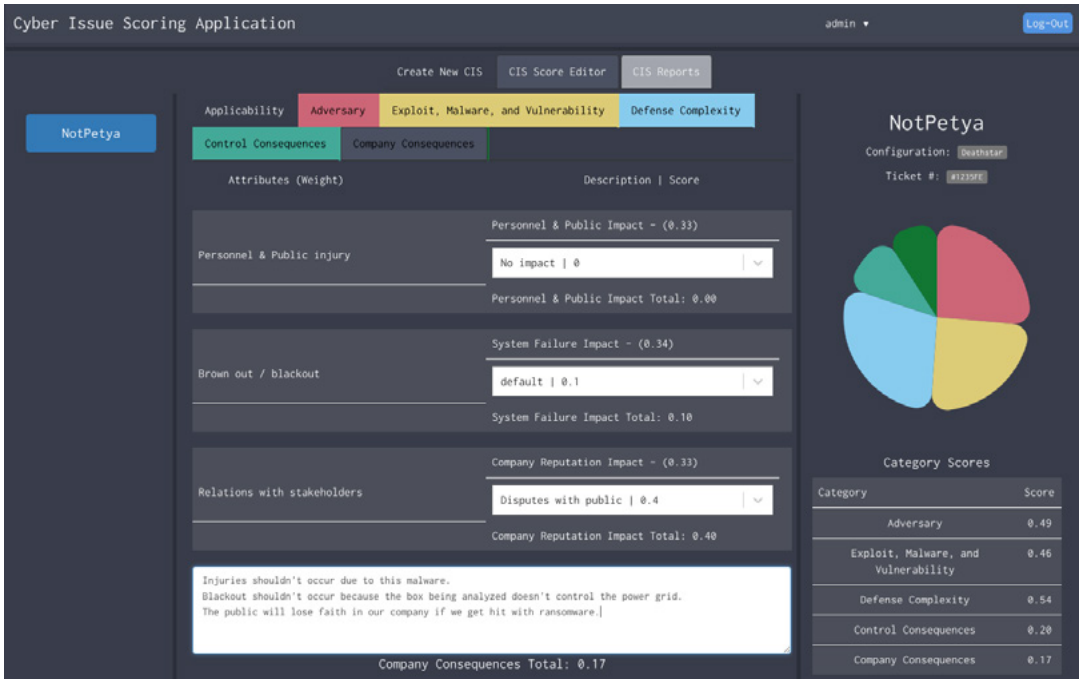
EMV provides a novel process to score cyber issues against various hardware configurations and compare that score against other scored issues for prioritization and trending over time.

There are a large number of potential exploits, malware and vulnerabilities (EMV) that can be used to attack control systems on critical infrastructure. There are simply too many cyber issues evolving over time for limited cyber resources to manage.

Cyber security professionals are flooded with urgent cyber issues that need to be addressed. The translation of information technology to operational technology cyber issues is more complex due to varying applicability, defense capabilities and consequences.

EMV scoring allows for prioritization based on a score derived from 6 characteristics: applicability, adversary, exploit malware and vulnerabilities, defense complexity, control consequence and company consequence. The scores and weights associated with the attributes of each characteristic are variable and can be fine-tuned by the user. An added benefit of this EMV scoring process is the identification of potential threat object characteristics that can then be used for indicators and courses-of-action.

EMV was developed by INL as part of the larger California Energy Systems for the 21st Century (CES-21) Program, with further development championed by Southern California Edison (SCE). EMV leverages previous frameworks: Attack Technology Analysis and Characterization (ATAC) and Response Analysis and Characterization Tool (ReACT) developed under DOE-OE-CEDS.



Dynamic data driven cyber issue scoring with references as EMV evolves over time

Idaho National Laboratory

For more information

Robert M. Caliva
Program Manager
208-526-8238

Zachary M. Priest
Infrastructure Security Software Developer
208-526-1111

Rita Foster
Infrastructure Strategist & Technical Lead
208-526-3179

www.inl.gov

github.com/idaholab/emv

A U.S. Department of Energy National Laboratory

EMV Scoring for Prioritization

Applicability is not a simple binary answer. As experience through years of analyzing malware demonstrates, a simple change to that malware will change the applicability of the malware's impact to a system.

Adversary defines a way to score both the motivation and capability of the attacker.

Exploit, Malware and Vulnerabilities are integrated together in malware to create functional software for the adversary. Enabling the ability to score these areas for urgency, maturity/ sophistication and functional impact is important to focus limited cyber resources.

Defense Complexity is focused on how difficult it is to detect, defend, and remedy an EMV.

Control Consequences is focused on the large scale impacts of an EMV to the command and control functions and the implications for equipment function.

Company Consequences are focused on the large scale impacts of an EMV to the community in which the system operates. Traditional risk managers understand the personnel safety and public impacts as well as the impact to a company's reputation.

This application allows users to interface with another INL product Structured Threat Intelligence Graph (STIG) by exporting partially created Structured Threat Information eXpression (STIX) 2.0 objects that can undergo further enrichment.

Side by side comparisons of current scored cyber issues

The EMV application provides a framework in which to score Exploits, Malware and Vulnerabilities against known configurations of equipment. The variable scoring schema allows users to tune the application into what works best for their systems and equipment. The prioritization process allows users to efficiently utilize limited cyber security resources.