Tuitio™

Comparison of Tuitio™ with Machine Learning AV

June 2018

Tuitio™ by **Bravatek Solutions, Inc.**

Key Points (Know the Differences…)

- Machine Learning (ML) has only Marginally Improved Detection over Traditional Signatures
  - Tuitio BLOCKS the same Attacks plus all that ML Misses
- ML Fails to Detect Zero-Day Attacks because they are Different from Past ones
  - Tuitio Blocks Zero-day and altered Known Attacks
- ML Detection Degrades with Time and when Offline; it also Fails to Learn
  - Tuitio Protection Never Degrades because it Never needs Signatures of any kind
- Adversaries are using ML to find "ML Blind Spots" to elude Detection
  - Tuitio has No "ML Blind Spots" to elude
- The Same Obfuscation & Evasion Tactics that have fooled AV, do so for ML. Plus, there are newer tactics specifically made to fool ML
  - Obfuscation & Evasion Tactics are Irrelevant to Tuitio; it Blocks what they try to do, regardless of how they disguise themselves
- ML AV Fails to Detect Non-Malware (e.g., PowerShell, macros, etc.) and In-Memory (e.g., code injection, RAM scrappers, etc.) Attacks, which often begin via Weaponized Documents
  - Tuitio Blocks these Attacks, yet Allows Safe Use of the Legitimate Endpoint Utilities Adversaries try to use Against the Enterprise
- False Positives and False Negatives from ML AV are a terrible Burden to IT/Sec-Ops, and they Disrupt End-users
  - Tuitio produces No False Positives or False Negatives
- ML Requires Constant Tuning and Re-tuning by Specialists
  - Tuitio is so Simple that Windows Administrators can Manage it
- Unpatched Endpoint Applications further Degrade ML AV Effectiveness
  - Tuitio Prevents Endpoint Compromises Regardless of whether Applications are Patched or Not
- Ineffective Endpoint Protection by ML AV Drives up Cyber Costs Downstream: SIEM, Threat Hunting, Incident Response, Forensics, User Entity Behavior Analytics, etc.
  - Tuitio Slashes all Downstream Costs by Preventing Compromises at the Endpoint very Effectively