Election Operations Assessment Summary

Election Assistance Commission

Scope of the Project

Phase 1 - completed

- Develop generic voting system models

Phase 2 - currently under review

- Analyze models to identify threats
- Use results of analysis to develop a threat assessment tool
- Tool will assist EAC and NIST in evaluating benefits and costs of proposed security requirements for VVSG 2.0

Seven types of attacks (threats) identified

- Attack voting equipment
- Perform insider attack
- Subvert voting process
- Experience technical failure
- Commit errors in operations
- Attack audit
- Disrupt operations

Voting Technologies Assessed

Generic Technology Types

- Direct Recording Electronic (DRE)
- Precinct Count Optical Scan (PCOS)
- Central Count Optical Scan (CCOS)
- Vote by Mail (VBM)
- Vote by Phone (VBP)
- Internet Voting (IV)
- Hand Counted Paper Ballots (HCPB)

Explanation of Terms

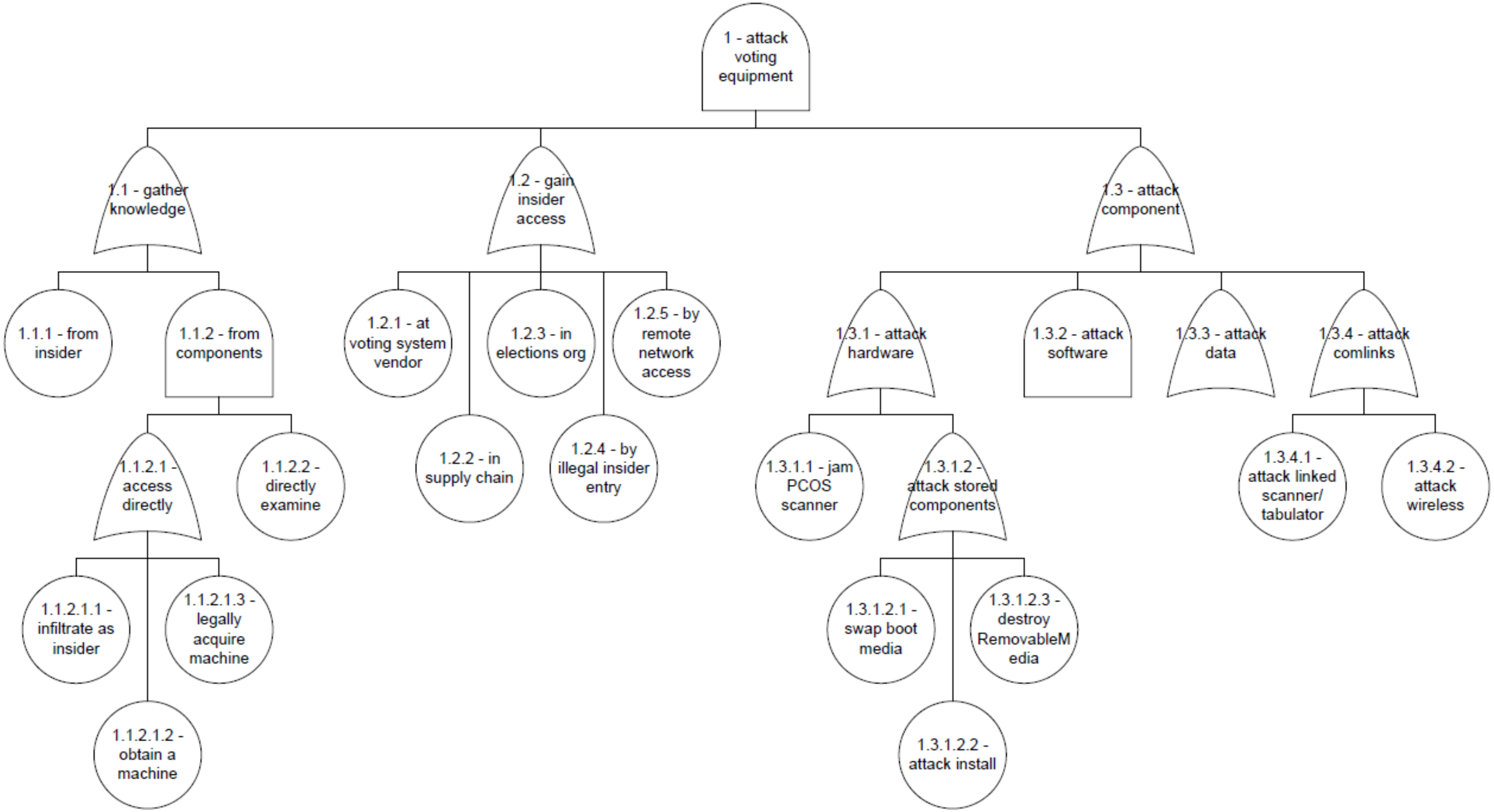
- A threat tree is a method to outline each type of attack (i.e., threat) and the steps required to exploit a potential system vulnerability
- A threat matrix documents additional information to more fully describe the nature of a threat action, its implications, and possible controls to prevent or mitigate its impact

Describing Threats

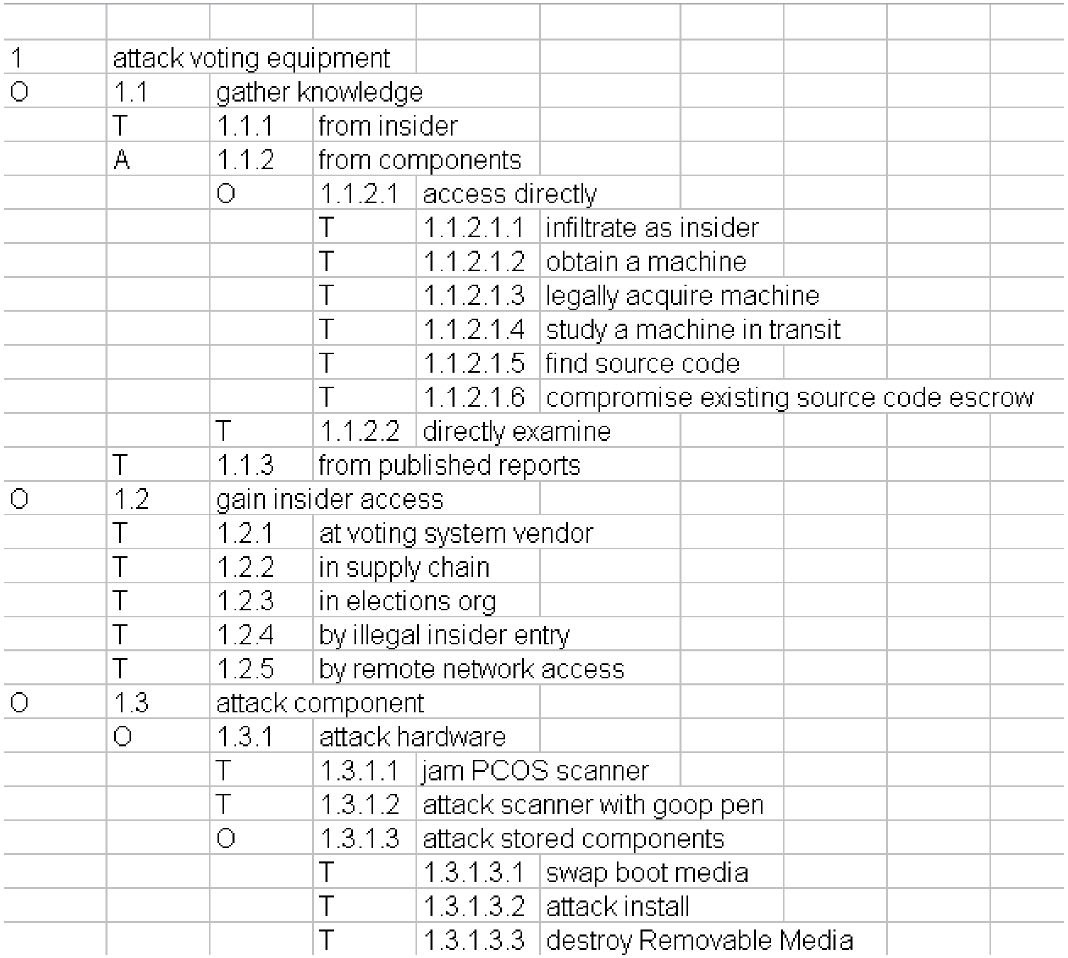
Technology threat information is described in three ways:

- A graphical threat tree
- A tabular threat tree
- A threat matrix

Graphical Threat Tree for Precinct Count Optical Scan (PCOS)

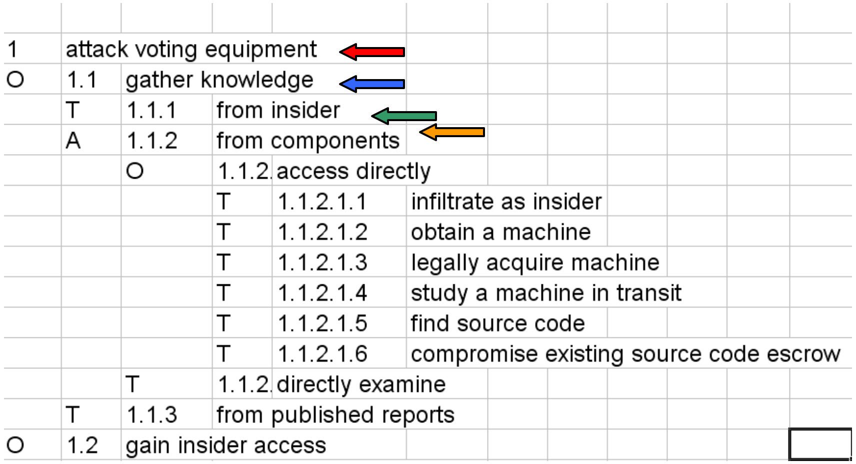

1 - attack voting equipment
1.1 - gather knowledge
1.2 - gain insider access
1.3 - attack component
1.1.1 - from insider
1.1.2 - from components
1.1.2.1 - access directly
1.1.2.2 - directly examine
1.1.2.1.1 - infiltrate as insider
1.1.2.1.3 - legally acquire machine
1.1.2.1.2 - obtain a machine
1.2.1 - at voting system vendor
1.2.3 - in elections org
1.2.5 - by remote network access
1.2.2 - in supply chain
1.2.4 - by illegal insider entry
1.3.1 - attack hardware
1.3.2 - attack software
1.3.3 - attack data
1.3.4 - attack comlinks
1.3.1.1 - jam PCOS scanner
1.3.1.2 - attack stored components
1.3.1.2.1 - swap boot media
1.3.1.2.3 - destroy RemovableMedia
1.3.1.2.2 - attack install
1.3.4.1 - attack linked scanner/ tabulator
1.3.4.2 - attack wireless

Tabular Threat Tree for Precinct Count Optical Scan (PCOS)

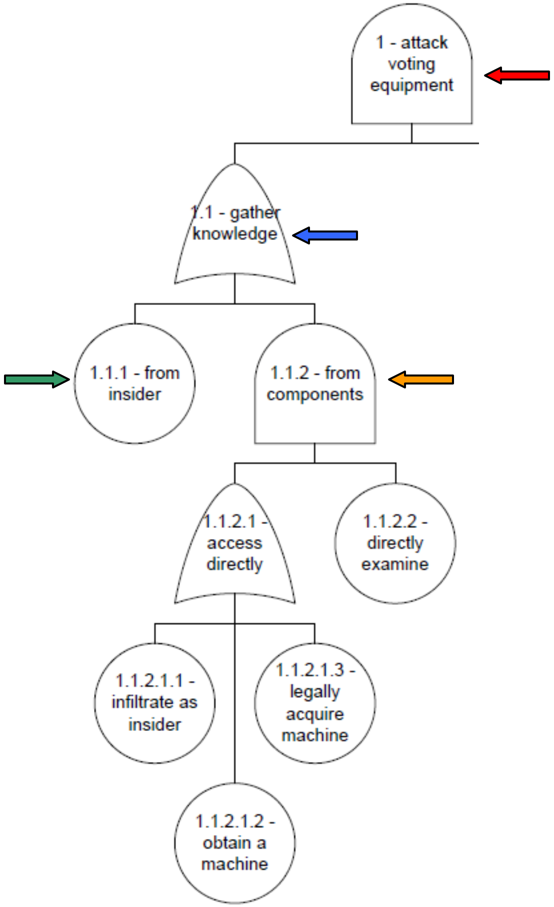


1	attack voting equipment				
O	1.1	gather knowledge			
	T	1.1.1	from insider		
	A	1.1.2	from components		
		O	1.1.2.1	access directly	
			T	1.1.2.1.1	infiltrate as insider
			T	1.1.2.1.2	obtain a machine
			T	1.1.2.1.3	legally acquire machine
			T	1.1.2.1.4	study a machine in transit
			T	1.1.2.1.5	find source code
			T	1.1.2.1.6	compromise existing source code escrow
		T	1.1.2.2	directly examine	
	T	1.1.3	from published reports		
O	1.2	gain insider access			
	T	1.2.1	at voting system vendor		
	T	1.2.2	in supply chain		
	T	1.2.3	in elections org		
	T	1.2.4	by illegal insider entry		
	T	1.2.5	by remote network access		
O	1.3	attack component			
	O	1.3.1	attack hardware		
		T	1.3.1.1	jam PCOS scanner	
		T	1.3.1.2	attack scanner with goop pen	
		O	1.3.1.3	attack stored components	
			T	1.3.1.3.1	swap boot media
			T	1.3.1.3.2	attack install
			T	1.3.1.3.3	destroy Removable Media

Comparison of Tabular and Graphical Trees



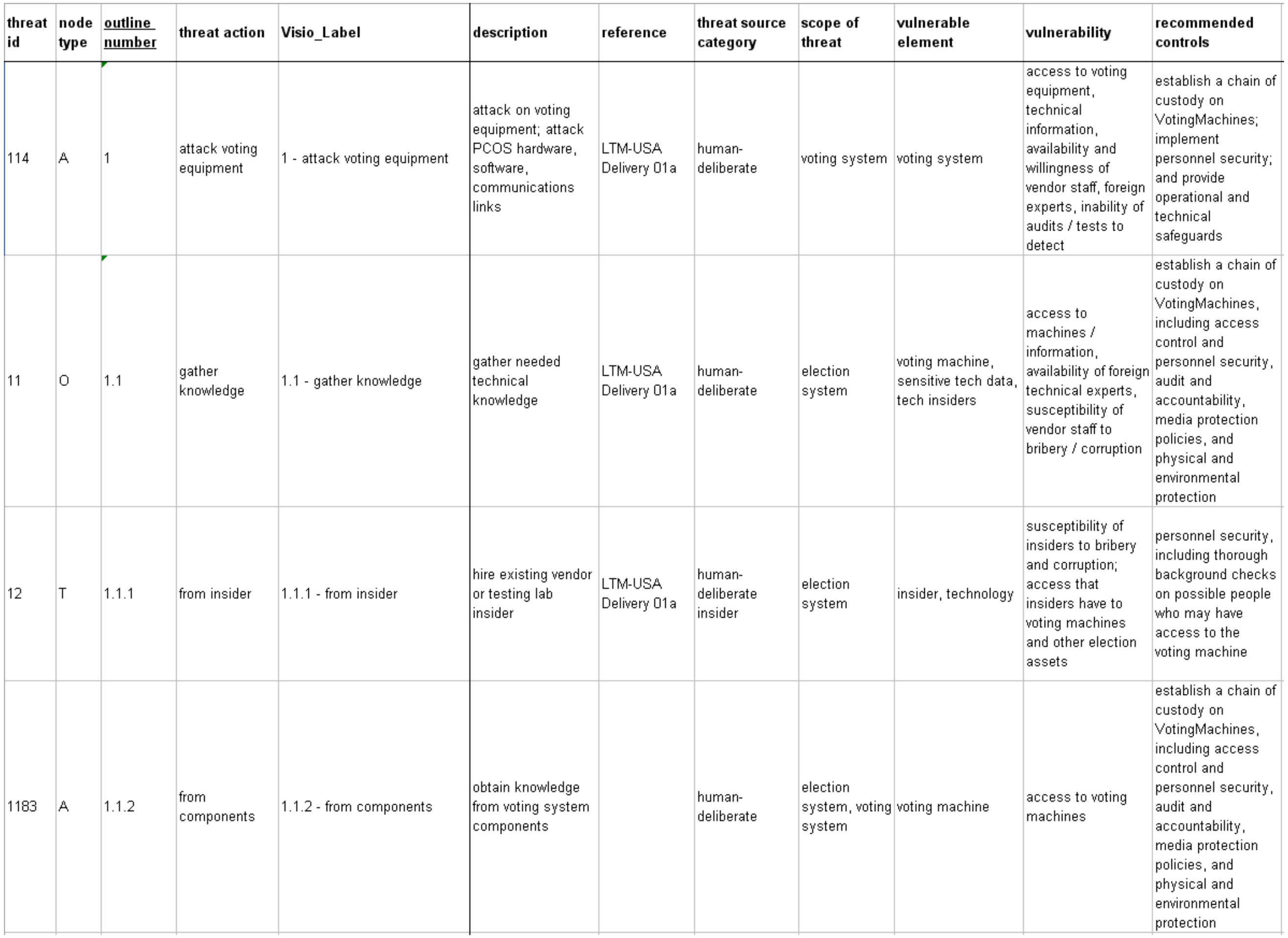
1	attack voting equipment				
O	1.1	gather knowledge			
	T	1.1.1	from insider		
	A	1.1.2	from components		
		O	1.1.2.	access directly	
			T	1.1.2.1.1	infiltrate as insider
			T	1.1.2.1.2	obtain a machine
			T	1.1.2.1.3	legally acquire machine
			T	1.1.2.1.4	study a machine in transit
			T	1.1.2.1.5	find source code
			T	1.1.2.1.6	compromise existing source code escrow
		T	1.1.2.	directly examine	
	T	1.1.3	from published reports		
O	1.2	gain insider access			


1 - attack voting equipment
1.1 - gather knowledge
1.1.1 - from insider
1.1.2 - from components
1.1.2.1 - access directly
1.1.2.2 - directly examine
1.1.2.1.1 - infiltrate as insider
1.1.2.1.3 - legally acquire machine
1.1.2.1.2 - obtain a machine

Comparison of Tabular and Graphical Trees

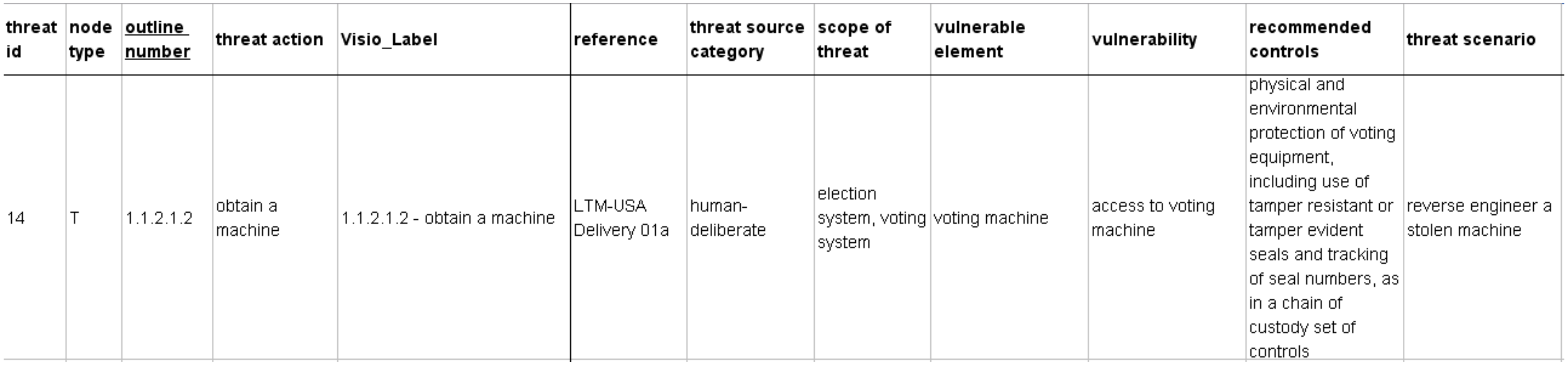
- Both trees display the same information
- To illustrate, the colored arrows point to the corresponding information in each tree
- By representing trees in both tabular and graphical formats, we accommodate both textual and visual information processing styles

Example of PCOS Threat Matrix



threat id	node type	outline number	threat action	Visio_Label	description	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls
114	A	1	attack voting equipment	1 - attack voting equipment	attack on voting equipment; attack PCOS hardware, software, communications links	LTM-USA Delivery 01a	human-deliberate	voting system	voting system	access to voting equipment, technical information, availability and willingness of vendor staff, foreign experts, inability of audits / tests to detect	establish a chain of custody on VotingMachines; implement personnel security; and provide operational and technical safeguards
11	O	1.1	gather knowledge	1.1 - gather knowledge	gather needed technical knowledge	LTM-USA Delivery 01a	human-deliberate	election system	voting machine, sensitive tech data, tech insiders	access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection
12	T	1.1.1	from insider	1.1.1 - from insider	hire existing vendor or testing lab insider	LTM-USA Delivery 01a	human-deliberate insider	election system	insider, technology	susceptibility of insiders to bribery and corruption; access that insiders have to voting machines and other election assets	personnel security, including thorough background checks on possible people who may have access to the voting machine
1183	A	1.1.2	from components	1.1.2 - from components	obtain knowledge from voting system components		human-deliberate	election system, voting system	voting machine	access to voting machines	establish a chain of custody on VotingMachines, including access control and personnel security, audit and accountability, media protection policies, and physical and environmental protection

PCOS Threat Matrix Detail



threat id	node type	outline number	threat action	Visio_Label	reference	threat source category	scope of threat	vulnerable element	vulnerability	recommended controls	threat scenario
14	T	1.1.2.1.2	obtain a machine	1.1.2.1.2 - obtain a machine	LTM-USA Delivery 01a	human-deliberate	election system, voting system	voting machine	access to voting machine	physical and environmental protection of voting equipment, including use of tamper resistant or tamper evident seals and tracking of seal numbers, as in a chain of custody set of controls	reverse engineer a stolen machine

- This matrix detail illustrates the same PCOS Attack Voting Equipment example shown in the threat trees. The entries in the matrix describe the characteristics of each threat action identified in the threat trees.

Threat Instance Risk Analyzer (TIRA) Tool

TIRA is an automated tool that allows the user to quantify his/her professional intuition/judgment about the likelihood of a given threat happening and its potential impact on election operations. The analyst can rerun the analysis multiple times using different assumptions to see how much the result changes.

How to Use TIRA

- Analyst creates a scenario by selecting threat instances from the trees
- Analyst uses TIRA worksheets to record scenario and assumptions
- Analyst assigns values for parameters of motivation, complexity, and impact
- Analyst runs TIRA simulation
- Result is a rank ordering of threats

Benefits of TIRA

- Organizes and structures thinking about risks
- Enables ‘apples to apples’ comparisons of different analysts assessments
- Allows analysis of hundreds of scenario variations in short period of time
- Permits analyst to make changes to threat matrices to create additional scenarios

Suggestions for Reviewing Threat Trees

- Begin with a technology you are familiar with.
- Compare what you know with what you see.
- Identify any missing threat actions or other elements.
- Remember that TIRA uses these trees as inputs for creating scenarios. If something is missing from a tree it can’t be considered in the TIRA analysis.

Review Questions for Threat Matrices

- Do you understand the terms used in the column headings?
- Are there other threat actions you would add?
- Are there other mitigations / controls you would add?
- Would you change any entries in the cells of the matrix?

If your review time is limited, feedback on the overall matrix structure is more important than comments on the individual cells.

Thank you for your time