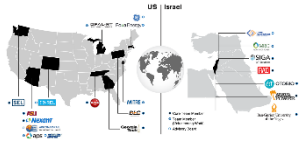
Task 3

Data Collection and Aggregation

Task status

8/24/2022

The Task Overview - Recap

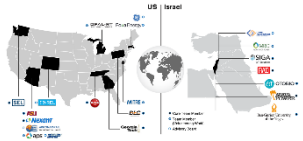


- Task Leader - ASU
- Participants - ASU, BGU, OTORIO, DK Innovation, DLC, Nexant, Delek, Arava
- Task Goal - Provide **reliable & comprehensive IT/OT datasets** that will include Cyber attacks simulated in various of ways and logged 360°
- Task objectives - Lab environments operations, Advisory emulation + Datasets generation

How -

- Setting up multiple lab environments
- Setting up multiple sensors to monitor the network from different aspects
- Setting up RAM² as central logging system + build necessary plugins
- Execute live attack scenarios

What’s been Done - This Q

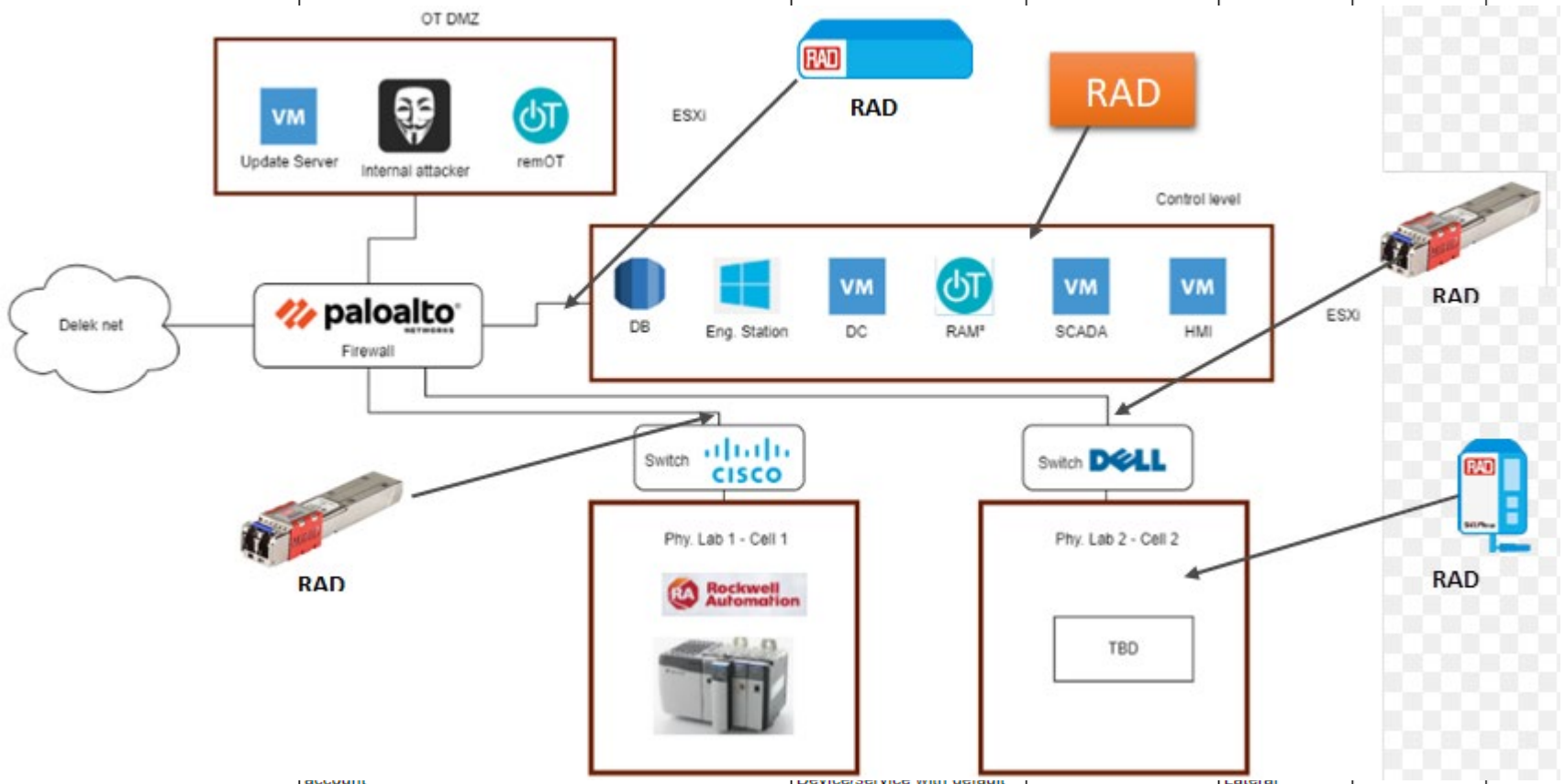


- ✓ Attack scenarios for Delek US - final drafts
  - Synced with Task 2 and Task 4 (Also MITRE)
- ✓ Started implementation of missing abilities in Caldera (implant)
- ✓ RAD incorporation in the lab
- ✓ Meptagon
  - Physical visit + kickoff workshop with BGU Done
  - Next steps and small modifications in order to make it full IT/OT lab - in progress
    - Small hardware modifications and additions
    - Attacks implementation
  - Received project file of S7-1200 + Cimplicity SCADA file

Some pictures from our visit in Meptagon’s lab

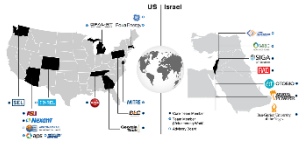
Abilities from the Delek Scenarios (draft)

	A	B	C	D	E	F	G	H	
1	**Use case**	**Ability name**	**Description**	**Options**	**Requirements**	**Effort / Threat level**	**TTP type**	**TTP**	**T**
2	Trisis - 1	Watering hole (OT site)	A user is downloading a sandcat agent from an OT site	* Easy - agent is "as is" in the website, * Medium - improvement - implanted inside another 'legit exe' ~~* Possible - exploitation of browser?~~	Site needs to be opened in the Firewall		initial Access	T0817	D
3	Trisis - 1	Phishing mail	A user is installing a sandcat agent from malicious macro in doc file	* Easy - Macro Office Document * Possible - Office CVE	Possible - SMTP server, improvement - better email provider for the attacker...		initial Access	T0865	S
4	Trisis - 1	Supply Chain Compromise	A user is installing a sandcat agent embedded in python/apt package	* Easy - implant agent installtion in python package * Hard - infect apt package			initial Access	T0862	S S T
5	Trisis - 1	Agent Persistence	Set Pers						
6	Trisis - 2	Persistence on a remote machine - Create a new Windows admin user	Creates prompt.						
7	Trisis - 2	OT persistence	Set pers downgra						
8	Trisis - 2	Privilege Escalation	Escaleti perform						
9	Trisis - 2	Evasion Technique	Evasion						
10	Trisis - 2	Network Discovery	locating their tar						
11	Trisis - 2	Search for OT files / stations	Search extensic						
12	Trisis - 2	Lateral movement	Moving through the environment	account using remote services like RDP	Device/service with default creds		Lateral movement		
				* Easy - direct access to OT / valid account to FW / Brute					



https://docs.google.com/spreadsheets/d/1tBUWPJoWcc1vuGh3ZGjWhb4Ia-1f3e0HxqOUBlvWRoY/edit#gid=1880750238

Plans for the next Q



- ✓ Delek lab completion
  - Hardware configuration, lab setup (Users, HMIs, PLCs…)
  - Process engineering + simulation (Meptagon)
- ✓ Execution of attacks & data collection -
  - **Delek US - basic**
  - **Meptagon - Full**
- ✓ Complete set of abilities (without process manipulation)
- ✓ Grid lab next steps
- ✓ Possible additional labs (DLC, Arava…)