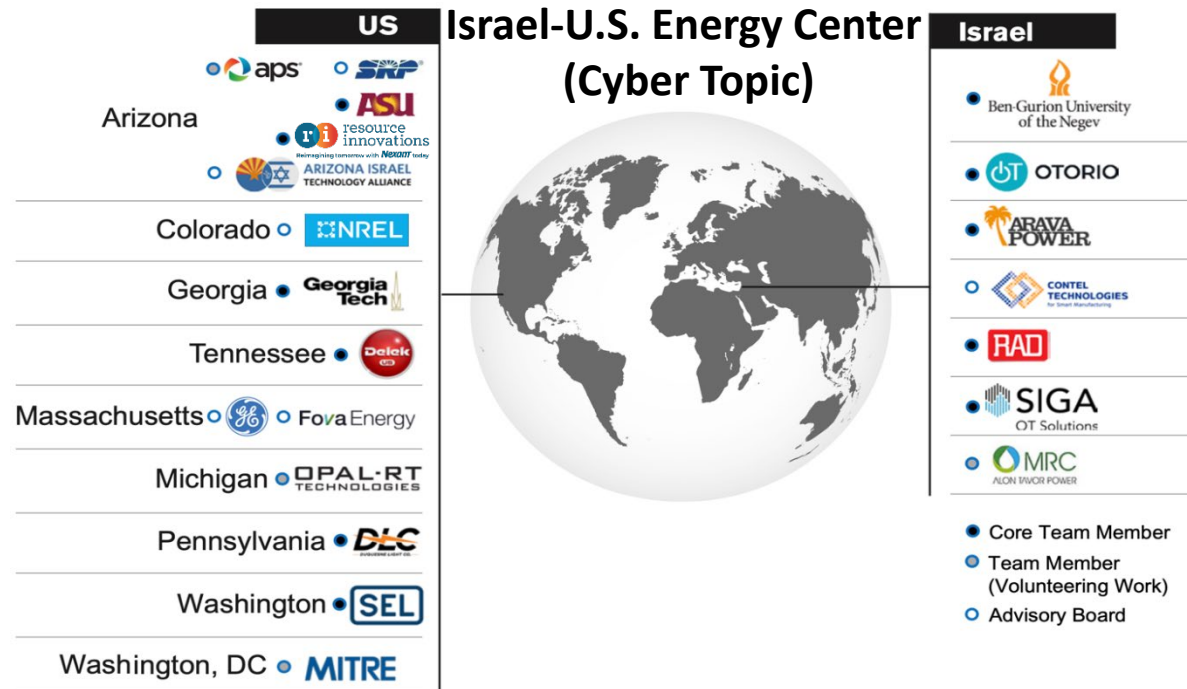


Task 4

Multi-Level Threat Intelligence Knowledge Base



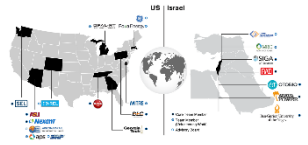
Project Review Workshop

Rami Puzis

BGU

Mar 20, 2023

Cyber threat intelligence (CTI)



- **Structured and actionable** information for identifying adversaries and their motives, goals, capabilities, resources, and tactics
- **Evidence-based knowledge** in the form of measurable events and the context for the events' interpretation.

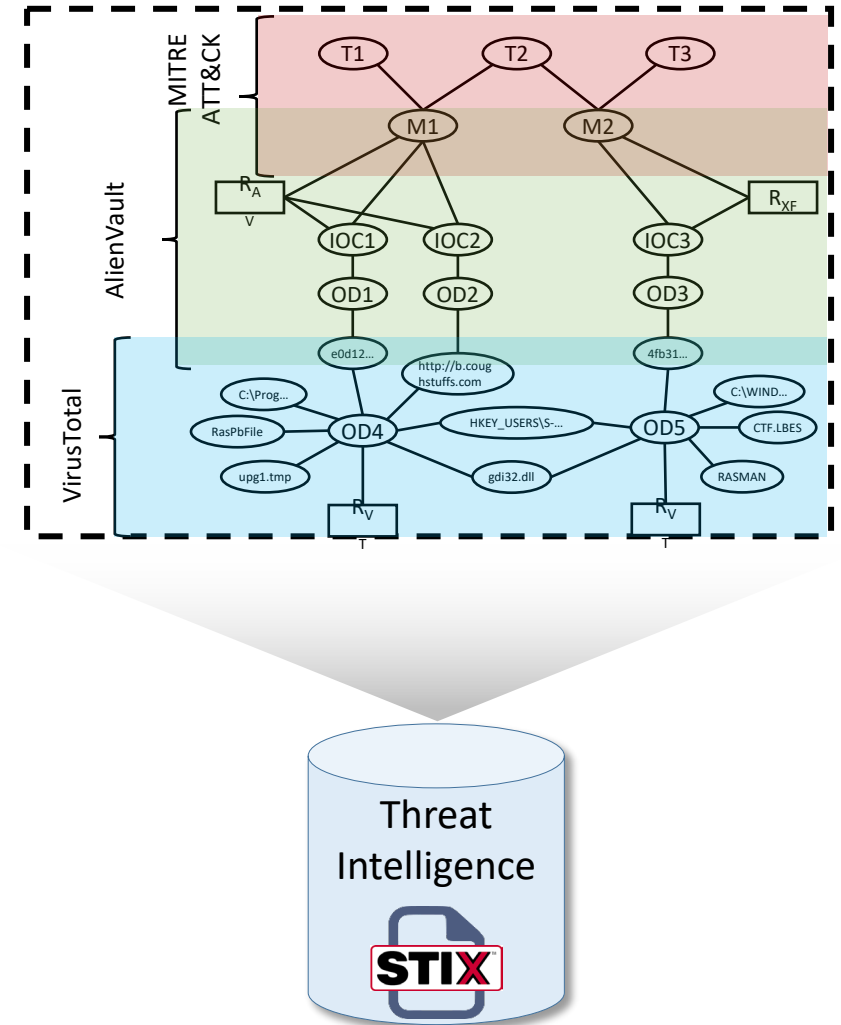
Previous milestones - Multi-Level Threat Intelligence Knowledge Base for Enterprise



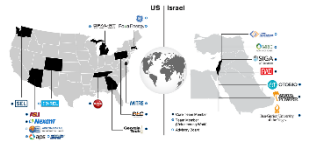
- We populated a graph database for enterprise environments with information from:
 - MITRE ATT&CK
 - AlienVault OTX
 - VirusTotal

Challenges for ICS:

- Few Threat Intelligence sources compared to Enterprise
- Diverse types of observables (vendors/protocols/environments)



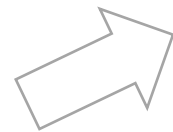
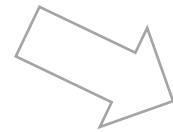
Multi-Level Threat Intelligence Knowledge Base for ICS - approach



- We are currently focusing on constructing an ICS knowledge base from two main sources:
 - SNORT and Suricata firewall rules for ICS
 - ICS Malware reports



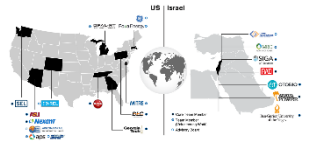
Requirement	Permission	Protocol	Source	Destination	Port
1	ALLOW	IP	ANY	192.168.1.25	80
2	ALLOW	IP	ANY	192.168.1.25	80
2	ALLOW	IP	ANY	192.168.1.25	443
3	ALLOW	UDP	ANY	192.168.1.10	53
4	DENY	TCP	ANY	ANY	53
5	DENY	IP	ANY	ANY	53
6	DENY		ANY	ANY	



ICS Observables Scheme



ICS Base Observable Scheme



Every ICS observable will contain an explanation of the context in which it was observed, the techniques associated to it, and a list of references to sources related to it.

Property	Type	Description
type	String	The type of observable, which should be set to "ics-observable".
context	String	An explanation of the context in which this observable was observed.

Relationship	Description
technique	Relationship to one or more TTP objects representing techniques associated with the observable.
reference	Relationship to one or more reference items associated with the observable. A reference item can be a URL, CVE id, BUGTRAQ id, Nessus id, SID, or any other source of information.

ICS Command Observable Scheme (extends network-traffic and ics-observable)



Property	Type	Description
type	String	The type of observable, which should be set to "ics-command-observable".
command_type	String	The type of command, which can be one of the following values: <ul style="list-style-type: none"> • "execute": Indicates that the command was executed. • "write": Indicates that a value was set by the command. • "read": Indicates that a value was retrieved by the command. • "create": Indicates that a new object was created by the command. • "delete": Indicates that an object was deleted by the command. • "modify": Indicates that an object was modified by the command.
command	String	The name of the command that was executed.
payload	String	The payload contains the command, if any, represented in 'command_format' format.
command_format	String	The format of the command, if any.
command_language	String	The programming language used to write the command, if any.
timestamp	String	The timestamp when the command was executed, in the format YYYY-MM-DDTHH:MM:SSZ.

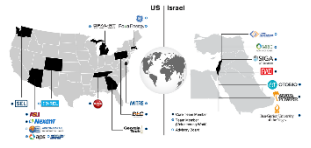
Relationship	Description
command_argument	Relationship to one or more objects representing arguments passed to the command.

ICS Tag Observable Scheme (extends ics-observable)

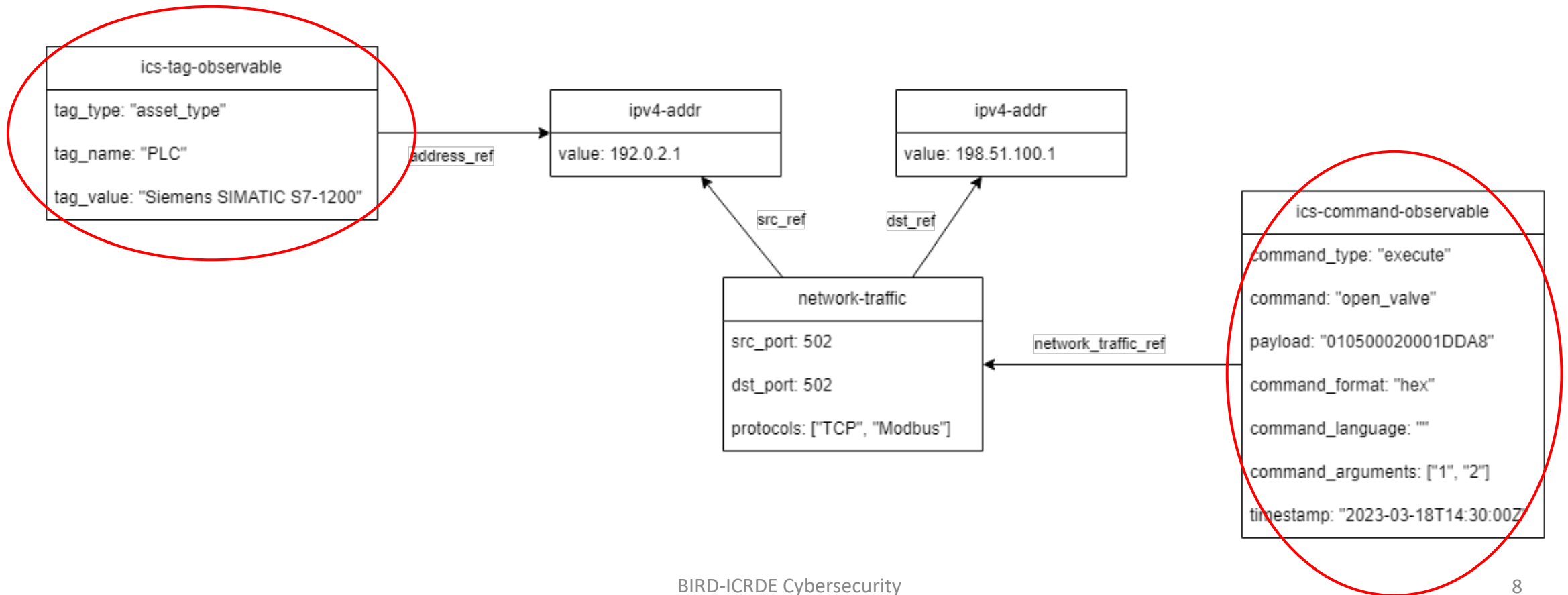


Property	Type	Description
type	String	The type of observable, which should be set to "ics-tag-observable".
tag_type	String	The type of tag. This property is an enumerated list that includes the following types: function, location, criticality, asset_type, manufacturer, model, version, owner, maintenance_status, and access_control.
tag_name	String	The name of the tag.
tag_value	String	The value associated with the tag, if any.
address_ref	String	Reference to an address object (can be an ipv4-addr, ipv6-addr or mac-addr objects) of the device associated with this tag.

Scenario Example



“A Siemens SIMATIC S7-1200 PLC with IPv4 address of 192.0.2.1 sends an open-valve command to a device with IPv4 address 198.51.100.1 via Modbus protocol”



Associating firewall rule to Technique using ChatGPT



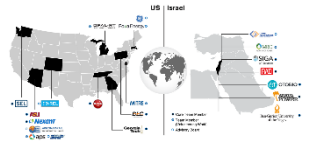
Query:

Search and return a list of as many mitre attack techniques as possible that can be associated to the following rule:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible NOS Microsystems Adobe Reader/Acrobat  
getPlus Get_atlcomHelper ActiveX Control Multiple Stack Overflows Remote Code Execution Attempt"; flow:established,to_client;  
content:"E2883E8F-472F-4fb0-9522-AC9BF37916A7"; nocase; content:"offer-"; nocase;  
pcre:"/<OBJECT\s+[^>]classid\s=\s*[\x22\x27]?[s]*clsid\s*\x3a\s*\x7B?[s]*E2883E8F-472F-4fb0-9522-AC9BF37916A7.+offer-  
(ineligible|preinstalled|declined|accepted)/si"; reference:url,www.securityfocus.com/bid/37759;  
reference:url,www.kb.cert.org/vuls/id/773545; reference:url,www.adobe.com/support/security/bulletins/apsb10-02.html;  
reference:url,www.exploit-db.com/exploits/11172/; reference:cve,2009-3958; reference:url,doc.emergingthreats.net/2010665;  
classtype:attempted-user; sid:2010665; rev:7; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,  
attack_target Client_Endpoint, deployment Perimeter, tag ActiveX, signature_severity Major, created_at 2010_07_30, updated_at  
2016_07_01;).
```

For each technique you found, write: "Technique ID - Technique name - Explanation why this technique is associated with the rule and how you understood that". after you found all the techniques try to find more techniques using what you have learned from found techniques.

Associating Observable to Technique using ChatGPT



Output:

Based on the given rule, the following MITRE ATT&CK techniques can be associated:

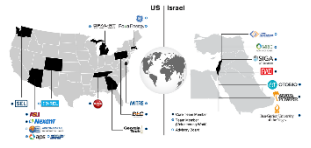
T1204 - User Execution - This technique involves an attacker tricking a user into running a malicious script or code. In the given rule, the attacker is attempting to exploit vulnerabilities in the Adobe Reader/Acrobat getPlus Get_atlcomHelper ActiveX Control to execute remote code on the victim's machine. The user must click on the link or visit a website that contains the malicious ActiveX control.

T1214 - Credentials in Files - This technique involves an attacker searching for and stealing credentials stored in files on the victim's machine. If the attacker successfully exploits the vulnerability in the ActiveX control, they may be able to gain access to sensitive information, including login credentials, stored in files on the victim's machine.

T1059 - Command and Scripting Interpreter - This technique involves an attacker executing commands or scripts on the victim's machine to achieve their objectives. In the given rule, the attacker is attempting to execute remote code on the victim's machine by exploiting vulnerabilities in the ActiveX control.

(And more)

Next Steps



- Define more ICS related extensions
- Associate the extracted observables to MITRE ATT&CK's techniques – using ChatGPT
- Explore the ability of ChatGPT for extracting observables from ICS Malware reports
- Test the accuracy of ChatGPT using expert study