Virtual Outreach Session for DISC 13 challenges (IA) Hosted by iDEX-DIO

Problem statement**: Advanced Autonomous AIDriven Cyber-Security Framework for Isolated LAN Environments.**

Q: **What will be the size of the air gap network**?

A: As per the requirement of the Indian army, the recommendation is about a size of approximately three hundred to four hundred pieces on a network. If the model is successful, then it should meet all the parameters. The model should be a scalable one that can be deployed to Pan India.

The Indian army has its own network. So post-validation of this prototype, this should be capable of the scalability of the model, which should be where thousands of PCs, public, you know, endpoints, and various other network devices are. They can be integrated into the system.

It is exclusively for an isolated air gap network. So the only media through which the subnets are connected is through your physical media, that is, through lights. Okay, so there are, if there are, and in case of a pan-India deployment also, we have our dedicated lines, which are there. So there is no scope of the internet or any kind of Wireless public outside connections for connecting sub-networks. However, if there is a requirement of any data exchange, object two points have to be there, if there are any requirements, so the, you know, as per the global protocols, the use of CDS of the DVDS, which are required to transfer the data from one point to another through the data exchange point, you know, as per protocols and the sanitization issues that are there, that will be there.

Q: **What are the operating systems that the endpoint security models should cover? Like, is there any specific version of Windows, Linux, or something?**

A: The Windows system with the latest version as well as the feasibility of having the Linux at the end point.

Q: **How is the patch management currently done in the air gap network?**

A: There are two issues that you have addressed. Firstly, you know, downloading all the patches and sanitizing it, so definitely the protocol says the use of CDS and sanitization pieces, which will be central. Secondly, the push management system of these operating systems again gives you the flexibility with you. If it can be done securely through a server,

Q: **What are the current practices and what are the current policy or usage restrictions for the removal of storage devices in the gap network?**

A: The use of wireless devices, again, can be restricted, but we are not going to put any kind of limitations if you can propose a much more secure and efficient model by using some wireless device, which you know all parts of the present line communications and the physical device.

Q: **Do you have any form of threat profile data that you've already tried doing, and you do not need to get into if it's confidential, but as a part of modeling, what kind of polymorphic threats or identifiers are there, or any?**

Kinds of signatures associated with them and model any data around the subject?

Any SWOT analysis of existing solutions that would be made available to the developer during the SPOC development? Can we affect network architecture based on the AI requirements?

Any functional requirements or any kind of implementation requirements that we have in order to facilitate the solution?

Does the system have any sort of a priority matrix in terms of an internal assessment of intent?

A: Such data is only from our side because it is easily and readily available commercially; even the analysis of the present adversaries and the targeting profiles and campaigns, what they are, are also in open source. So this is one of our suggested recommendations that if such kind of information and prior knowledge is required initially, yes, definitely it is, but it is very well, it is easily available, so it is back for us like we need to share it if it is required; it can be up, and it can be.

Q: **Do you want to only cover the network-based threats or even host-based and application-based ones?**

go through the problem statement that we have published is, so the requirement is in totality for the network as well as the endpoint, and once we say so the application layer of the endpoint also part of the behaviour analysis and the pattern recognition.

Queries:

output:

Contact of the resource person

Is any pre-qualification needed?

What is the expected duration of the entire competition?