SEENGN.

INTERSET PROVES OPERATIONAL EFFICIENCY OF SECURITY ANALYTICS ENGINE

Interset is a cybersecurity company that detects threats on client networks with an Al-powered security analytics engine. For the company's second CENGN project, interset deployed an enhanced version of its product on the CENGN infrastructure to validate that the resource utilization of the solution has improved significantly since the first project that was completed early this year.

Interset allows organizations to cut through the vast volumes of security data to automatically surface events related to data theft, fraud, and insider threats on a network. At the core of Interset's value is their principled math approach to cybersecurity and a security analytics engine that guards against unknown and emerging threats. The Canadian company is trusted by organizations across the globe that operate in industries such as banking, telecommunications, utility and energy, critical infrastructure, high-tech manufacturing, and more. Interset is an In-Q-Tel backed company, whose scalable architecture and machine learning algorithms help detect insider threats.

INCREASING NETWORK TRAFFIC LEADS TO STRAIN ON SECURITY MEASURES

With today's network traffic levels, advanced cybersecurity solutions are needed to process hundreds of thousands of events per second. The increase in the volume of information makes it difficult for security software to identify whether there are hidden threats that require attention. For organizations to stay secure, they require a security software solution that is scalable to the number of events occurring on their network and algorithms that focus on scarce resources.

SECURITY ANALYTICS ENGINE

Interset's highly extensible security analytics engine has a growing library of hundreds of algorithms and analytics programs designed to detect even the newest and unforeseen security threats. It prioritizes security threats in a multidimensional manner, taking into account users, files, and devices to rank threats, which provides security teams with a reliable list of threat leads to investigate so they're not chasing deadends. In addition, the machine learning features of the solution makes the platform smarter as data is analyzed over time.

PROJECT GOALS

In February 2018, Interset completed their first CENGN project to determine the resource requirements of its solution, with a focus on its endpoint sensor data processing throughput. Interset's sensors monitor endpoint activity such as data exfiltration, network activity, and asset access. The data gathered by each of the sensors is authenticated by the Endpoint Server and then passed to the analytics engine in real time or when connected.





Based on the results of the first CENGN project, Interset made a number of fundamental optimizations to its endpoint server. The purpose of this second project was to compare the performance of the enhanced endpoint server with the results of the first project. This controlled environment allowed Interset to quantify the performance improvements and identify whether there were any further optimizations that could be made before rolling out to market.

THE RESULTS

Interset was provided three bare-metal servers and a cloud tenancy in their dedicated project slice to carry out their project on the CENGN Testbed. On each bare-metal server was an Interset endpoint server, which would analyze network data. Traffic was generated to the endpoint servers from the cloud tenancy, and metrics were recorded on the CPU, RAM, network, and disk space utilization on the bare metal servers.

From project 1 to project 2 there were significant improvements found in Interset's solution. The results were as follows:

- Events processed per second increased 450%
- CPU usage decreased by 76.1%
- Memory usage decreased by 90%

THE CENGN ADVANTAGE

Interset is a great example of how Canadian businesses can utilize the CENGN Testbed to cost-effectively improve the operational performance of their solutions. Beyond saving on infrastructure services, using CENGN's pre-configured environment freed up the Interset engineering team from the setup and maintenance aspects of beginning a project. This permitted them to focus on their product development, successfully validating a significant decrease in resource utilization for their clients. By proving the new version of the solution heavily reduces the hardware requirements for client deployments, Interset can now confidently provide current and new clients with an upgraded product that has improved performance at drastically lower operational costs and keeps their organization secure.



Rick Penwarden, Marketing Manager rick.penwarden@cengn.ca cengn.ca/projects Steve McDougall, Director of Development smcdougall@interset.com https://interset.com/

