STREAMSCAN BLOCKS EXFILTRATION OF COMPROMISED DATA ON CENGN TESTBED

StreamScan's Compromise Detection System (CDS) is an innovative cybersecurity solution using behaviour analysis to scan networks for malicious data and block the exfiltration of sensitive information. For this project, StreamScan deployed their solution on CENGN's infrastructure to test and validate the functionality of their CDS with pfSense firewalls.

StreamScan is a high-growth Canadian business located in Montreal, Canada on a mission to keep data secure in enterprise networks. The company has developed a Compromise Detection System (CDS) that uses artificial intelligence (AI) and machine learning (ML) to meticulously scan networks and block infected traffic from returning to the source of the malware. StreamScan and their highly educated cybersecurity experts have worked with some of the top universities in Canada to develop their CDS. CENGN's multi-vendor OpenStack infrastructure provided StreamScan the opportunity to test the functionality of their solution in a real-time network environment.

WHY CYBERSECURITY CONTINUES TO EVOLVE?

All organizations, whether small or large, need to keep proprietary and customer information within their own systems. Anti-virus systems may block certain malware, but that's not enough to keep up with the millions of new viruses produced each day. Beyond this, the digitization of our world means more devices are connected to the internet than ever. In fact, by the year 2020 there will be 20 Billion IoT devices connected to the internet. This creates the need for more sophisticated cybersecurity solutions. As opposed to implementing solutions that are a master of one, security systems need to be agile to protect networks against new and less obvious attacks.

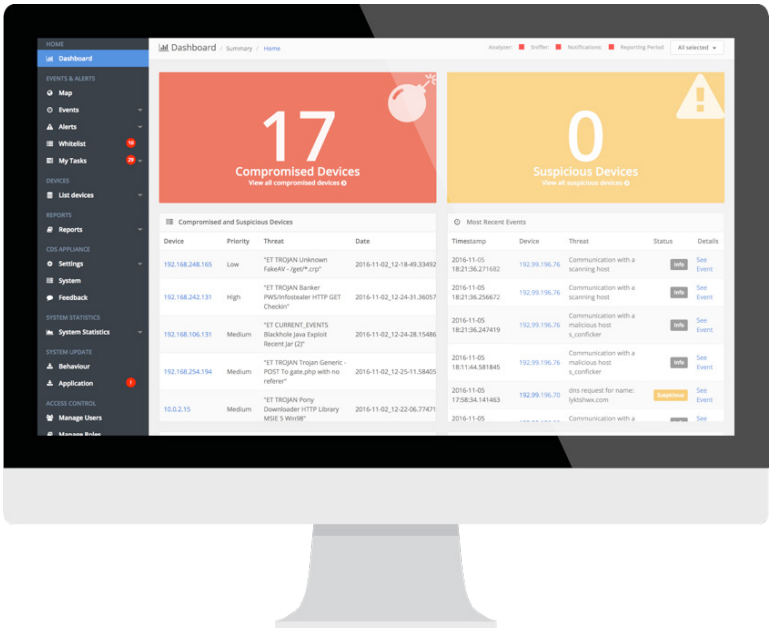

Figure 1. The StreamScan CDS Dashboard

STREAMSCAN'S SOLUTION

StreamScan's Compromise Detection System (CDS) is a leading-edge data breach detection solution that is the result of over five years of intense R&D. The CDS scans the network for unusual traffic and if the network is infiltrated with malicious data the CDS produces an alert and instructs the firewall to cut any communication between the infected device and the source of the malware. After deploying StreamScan's solution on your network, a continuous health and stabilization assessment scans the enterprise network using AI and ML to understand the structure and flow of traffic. Next, the CDS activates its alert and system management service by communicating with the firewall and instructing it to block sensitive information from exiting the network to the source of the malware.
StreamScan's CDS can be deployed as a virtual appliance, physical appliance, or cloud application. Their CDS boasts a 99% threat detection rate, scans enterprise networks 24/7, and is offered in both French and English versions.

CREATING STREAMSCAN'S PROJECT TESTBED

As shown in Figure 2, two Windows Users, a pfSense firewall, and StreamScan's CDS were placed on CENGN's bare metal server to build StreamScan's dedicated project space. The traffic generator produced safe network traffic flowing to Windows Users 1 and 2 and the pfSense firewall. The CDS simultaneously activated a health and stabilization assessment of the network conditions by scanning for irregular patterns. A command and control (C&C) server, running from StreamScan's outside server, then infiltrated the project space network bringing in malware and viruses to infect the Users. The stabilization assessment ran by the CDS sensed the infected traffic travelling through the network setting off alerts. The CDS then instructed the pfSense firewall in the virtual box to block all infected data from exiting the network, effectively disallowing the C&C server to exfiltrate data.

CENGN MEMBERS

Bell · Cisco · EXFO · Huawei · Invest Ottawa | Investir Ottawa · Juniper Networks · Mitel (Powering connections) · Nokia · ribbon · Rogers · Telus · Wind (An Intel Company)

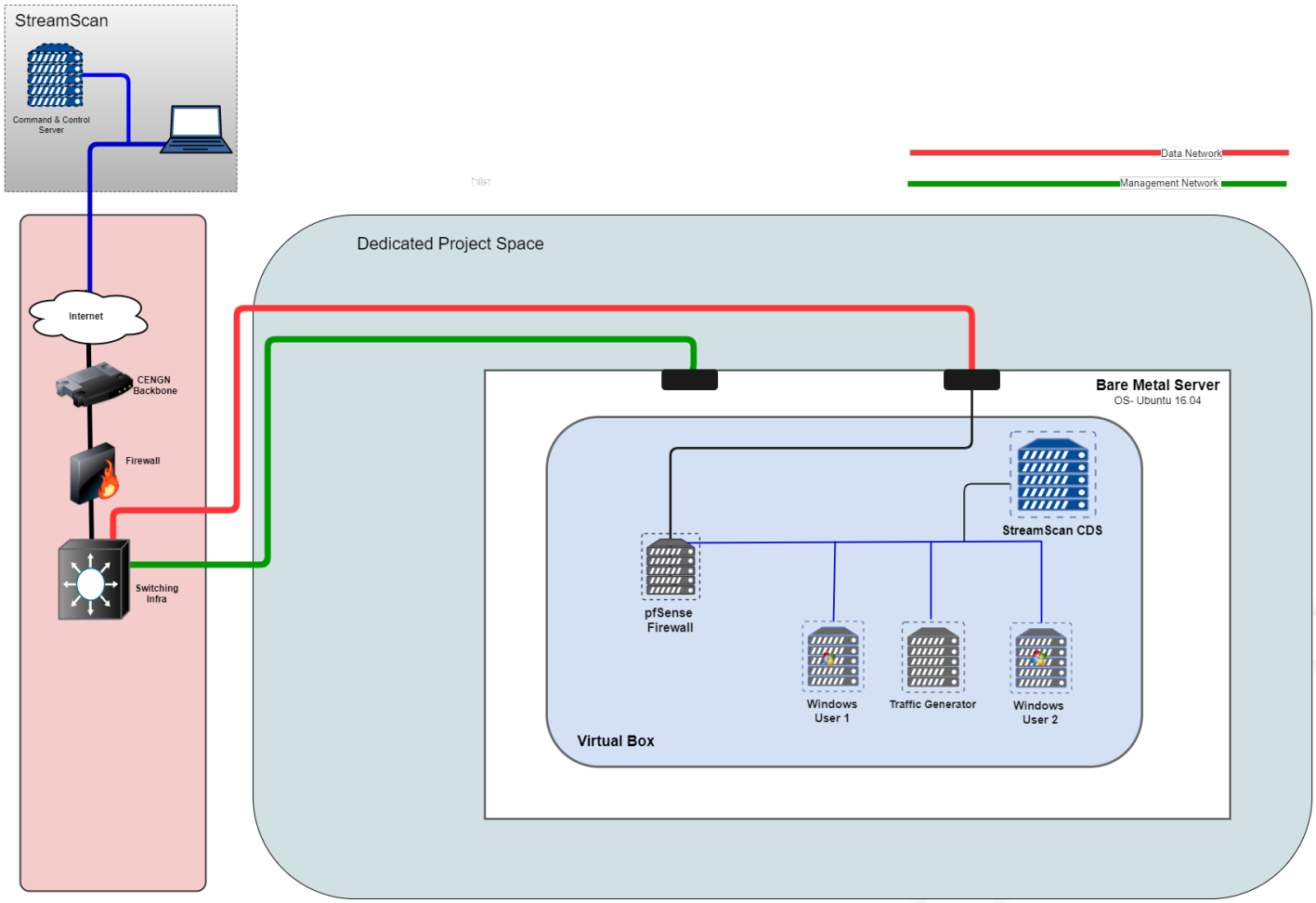

Figure 2. The StreamScan Project Setup

TESTING RESULTS

Step 1: Infect Windows Users with Malware
From a remote C&C server, a Microsoft Word document containing malicious macros was sent to infect Windows User 1 within the project space. When the attachment was opened it asked the User to enable macros to read the document, unleashing the Locky ransomware. Once infected, the Windows User generated an alert on the CDS dashboard showing that the Windows User was communicating with a malicious C&C server.

Step 2: CDS Functionality Test Against Data Exfiltration
StreamScan's CDS continued to scan all network traffic traversing the pfSense. Windows User 2 was then infected with a data exfiltration client using DNS protocol from the outside C&C server. Any file attempted to be downloaded from Windows User 2 by the C&C server was overseen by the CDS. The CDS automatically detected the communication between Windows User 2 and the C&C server and produced an alarm.

Step 3: Successful Integration with pfSense Firewall
The CDS scans the network 24/7 searching for malicious acts, now it was time for the CDS to take action and block data from getting back to the hacker's C&C server. This step of the project validated the integration of the CDS with the pfSense firewall. The infection of Windows Users 1 and 2 alerted the CDS then caused it to instruct the pfSense firewall to block traffic back and forth between the Windows User IPs and the C&C server. The CDS successfully blocked all traffic from the compromised Windows Users to the C&C server, keeping the C&C from exfiltrating any important data from the network.

CONCLUSION

StreamScan is comprised of a team of PhDs and cybersecurity experts with years of experience working with academia and the industry to calibrate their cybersecurity solution. StreamScan came to CENGN because they needed a real-time network to test and validate the functionality of their CDS. StreamScan was provided a bare metal server within a dedicated project space along with project management expertise to test their solution. The result was successful functionality testing of the CDS in an OpenStack environment, proving they have a reliable and adaptable cybersecurity solution.

CENGN
CENTRE OF EXCELLENCE IN NEXT GENERATION NETWORKS

CENGN
Rick Penwarden, Marketing Manager
rick.penwarden@cengn.ca
cengn.ca/projects

Jordan Janisson, COO
jordan.janisson@aerys.in
https://smartshape.io/en/home/

STREAMSCAN