SOLUTION SHOWCASE

Accelerate cyber security with a robust automated solution and visibility into your host's execution

Industries

- Finance
- Banking
- Retail
- Telecommunications
- Data centers

Challenges

- Increased volume and sophistication of intelligence data that needs to be processed after an incident
- Lack of reliable information and data acquisition tools

Products Used

- NVIDIA® BlueField® data orocessing unit (DPU)
- Log management solution
- CyVestiGO by Custodio Technologies

Results

- Reliable, automated, and efficient data acquisition
- Automated correlation and pivoting of events of interest from multiple data sources
- Remote administrative functionalities
- Better visualization of investigation findings

CYVESTIGO: ADVANCED MULTI-LAYER CYBERSECURITY INVESTIGATION SOLUTION WITH NVIDIA BLUEFIELD-2 DPU

CyVestiGO is an efficient, out-of-band, and reliable system for the acquisition and analysis of threat intelligence data. CyVestiGO operates in an automated manner to help cybersecurity professionals efficiently handle sophisticated incidents and gain a better view of the root cause and scope of incidents.

Background

When a cyber attack occurs, security analysts often need to race against time to surpass existing defenses, investigating the root cause of the attack, the scope of the incident, and the vulnerabilities exploited by the attackers.

The first stages of the investigation include collecting artifacts from the affected environment, such as operating system logs, application logs, network traffic, file system, and host memory data.

These stages are followed by processing the collected artifacts, which includes zooming into specific logs, following trails of evidence, understanding breach spread, interpreting the reason behind the success of the attack, and discovering the affected systems.

Recently, due to the increased volume and sophistication of cyber attacks, security operations center (SOC) and computer security incident response team (CSIRT) professionals are struggling to process the vast amount of threat intelligence data. They're also inundated with the exponentially increasing number of false positive security event notifications, leading to a waste of time and effort.

Existing Challenges

SOC and CSIRT professionals face a number of key challenges:

- The investigation process is time consuming: In attack analysis, SOC and CSIRT professionals often adopt systematic methodologies such as pivoting (e.g., using the Diamond Model), where they go through iterative rounds of using known indicators to uncover new elements related to the attack from recorded logs. While there are tools to help with correlating common fields across a huge volume of event logs, the repetitive process of pivoting and identifying new elements related to the attack is usually carried out manually, which is a long and tedious task.
- There is a shortage of cybersecurity skills: On the one hand, cyber adversaries constantly improve their attacking techniques and use better tools. On the other hand, the cybersecurity industry is facing a major skills shortage, and there are very few professionals capable of efficiently handling sophisticated cybersecurity incidents.
- There's a lack of reliable information: Nowadays, more adversaries use evasion and anti-analysis techniques to either reduce their attack traces or compromise the integrity and availability of host artifacts. Thus, important artifacts for the investigation go missing or unrecorded.

The Solution

Custodio Technologies developed a solution—CyVestiGO—that provides automated out-of-band memory acquisition from the host's volatile memory and pushes the acquired data into log management systems, which centrally capture logs generated from endpoints or network devices.

The solution automatically correlates and pivots events of interest from multiple data sources and provides a single cohesive picture along with enrichment—tactics, techniques, and procedures (TTP), indicators of compromise (IOC), and risk score—to the investigator. As a result, the root cause and scope of an incident are easily and quickly identified.

Components of the Solution

CyVestiGO is a commercially available investigation platform that provides users with a graphical user interface (GUI), visualization aids, and correlation engines that help SOC and CSIRT professionals carry out their investigation.

CyVestiGO is based on the NVIDIA BlueField data processing unit (DPU), a smart network interface card that introduces a fully isolated environment to support reliable and trusted hardware acquisition of host physical memory through direct memory access (DMA) at a very high rate. Using this functionality, memory is acquired from the host's hypervisor, as well as each individual virtual machine residing on the host hypervisor.

A log management solution collects and consolidates the memory data and logs pushed from the agent running on BlueField.

CyVestiGO supports:

- Graph generation and enrichment of data taken from memory or logs generated by BlueField
- Remote administrative functionalities on all NVIDIA Mellanox® investigation agents

Steps of Operation

1. An agent running on the BlueField DPU uses a software development kit (SDK) to extract memory from the host.
2. The agent pushes the acquired memory and logs to the log management solution.
3. CyVestiGO queries the log management solution for relevant memory data and logs during an investigation.

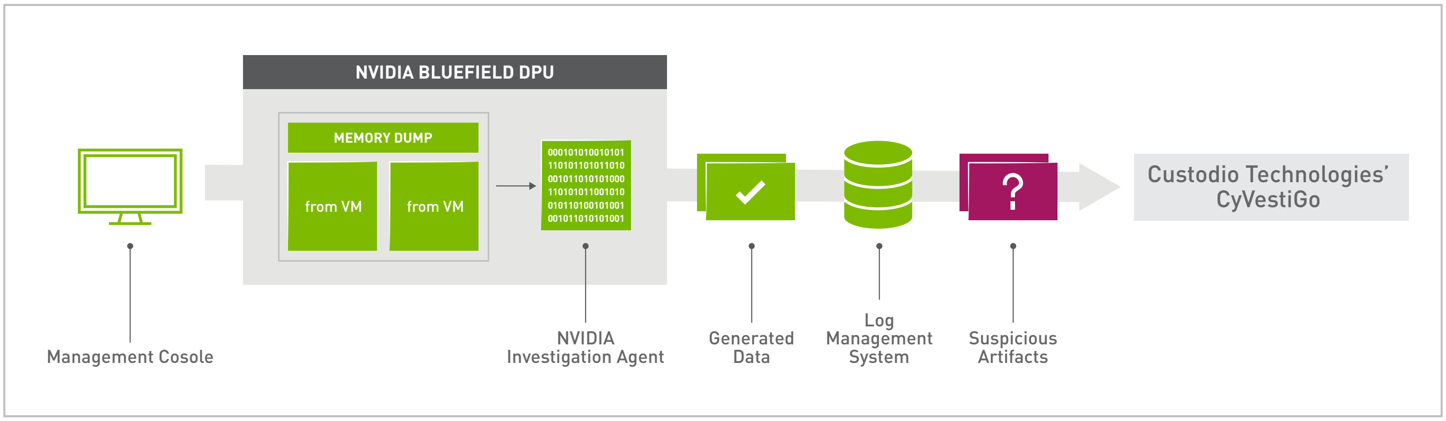

Figure 1: Schematic diagram of the solution

This Solution Compared to the Competition

In today's cyber-threat landscape, it's essential that solutions can get to the root cause of an incident, evaluate its scope, and efficiently collect related evidence.
When evaluating the root cause and full scope of an incident, other systems lack in link analysis and timeline analysis, which form a crucial part of an investigation process. They also need multiple queries to be manually executed in order to pivot from an event of interest. The CyVestiGO solution, on the other side, automatically correlates and pivots events of interest from multiple data sources and provides a single cohesive picture along with enrichment, easing and accelerating the identification of the root cause and scope of an incident.

The solution also demonstrates an advantage when acquiring host physical memory, as it doesn't consume extra computing resources on the host or hypervisor. In fact, one of the novelty features of CyVestiGO is its ability to extract and log relevant information from volatile memory in real time, without depending on the evidence collected from other data sources, which can be tampered with. This makes the product's memory data collection method far more reliable than the conventional method.

The Solution's Unique Benefits

The CyVestiGO solution delivers three benefits that accelerate the crucial response time to cybersecurity incidents.

1. Out-of-band, hardware-based memory acquisition: CyVestiGO runs in a trusted domain that's different and isolated from the host applications, which conserves the computing resources of the host. It doesn't leave a footprint of when and what data was accessed. And it provides the investigator with more reliable data for attack analysis and superior speed when compared with other memory investigation tools.

2. Memory visibility in the post-attack investigation process: Most existing solutions depend on evidence recorded by the operating system, applications, and other software to generate post-attack investigation findings. The CyVestiGO solution automatically records timely information from memory and preserves important context for future investigations.
3. Automated pivoting and correlation: The solution automatically correlates and performs pivoting searches for events of interest across multiple data sources, which helps investigators save the time spent on performing manual pivoting. Investigation findings are presented as a graph to provide a more intuitive visualization aid to the user, highlighting events of interest based on threat intelligence.

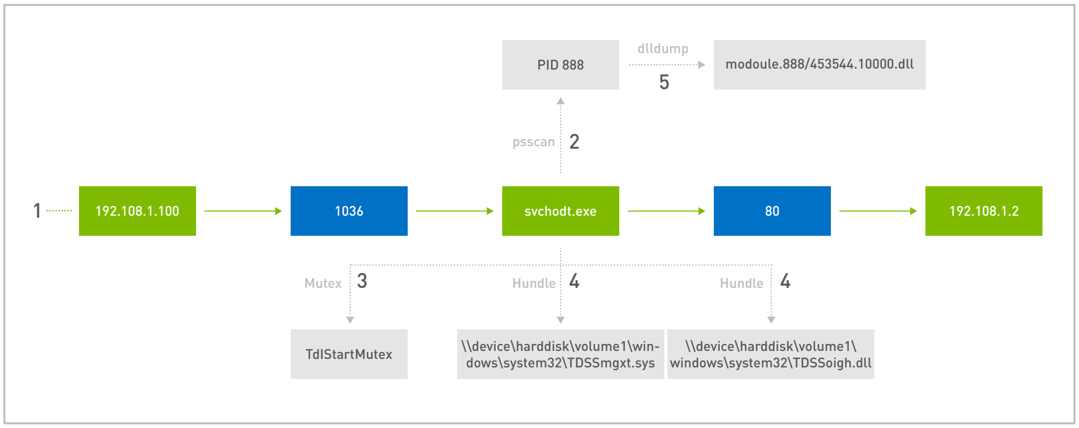
PID 888
dlldump
5
modoule.888/453544.10000.dll
psscan
2
1
192.108.1.100
1036
svchodt.exe
80
192.108.1.2
Mutex
3
Hundle
4
Hundle
4
TdlStartMutex
\\device\harddisk\volume1\windows\system32\TDSSmgxt.sys
\\device\harddisk\volume1\windows\system32\TDSSoigh.dll

Figure 2: Proposed investigation output

CyVestiGO with the NVIDIA BlueField-2 DPU accelerates the response time to cybersecurity incidents and automates the investigation process, giving SOC and CSIRT professionals a critical defense against threats and deeper insights into the sophisticated landscape they work within.

About Custodio Technologies custodio.com.sg/about

Veesion's AI solution is able to detect gestures associated with shoplifting. The software technology uses deep learning algorithms to continuously analyze the content of security cameras, enabling retailers to receive alerts on different devices and optimize their security staff allocation process.

LEARN MORE

Learn more about CyVestiGO: www.custodio.com.sg/cyvestigo
learn more about NVIDIA DPU: www.nvidia.com/en-us/networking/products/data-processing-unit

Contact an Expert:
alvin.cheng@custodiotech.com.sg | AhmadA@nvidia.com