Cat Scan II Big Dog

By Evelyn Wolfe

This document is created with the intention that I am on the team of Cat Security Solutions, providing our expert advice to our client “Big Dog.” This is why I used “We, Our” instead of “I.”

Table of Contents

Overview of Big Dog

Executive Summary

After being assigned to the client Big Dog, the following has been identified; on October 28th 2024, Big Dog faced an Indicator of Compromise (IoC.) This breach impacted the windows systems within the company. The breach was indicated as CVE-2024-0126 and CVE-2024-0117. This breach was due to the results of improper updates on one of the devices that had an NVIDIA Graphics Card. The threat actor was able to use a method of pinging the Host IP addresses within the company. Once a target was discovered, they were able to trace the details in a similar method to NMAP. In this case, they were able to identify several machines on the local host, and further investigate what each machine was the target for the initial attack.

If PRTG was in operation at this time, the communication from an outside source would have been flagged and alerts would have been triggered. Unfortunately this was not the case, and this is where Cat's Security Solution began our investigation and remedies of the problem with solutions to prevent this from happening in the future. After the isolated hit from the vulnerability to Big Dog company on the Windows workstations with this type of graphics card was installed, the company was fortunate that the Linux based server and workstations did not contain the opening for the threat actors.

After the repairs and recovery, our team was then tasked with providing a recommendation of network monitoring with sensors. This documentation is an overview of the tasks the team was assigned to and how this was executed to provide the best solution to Big Dog.

The following review of Big Dog's organization is as follows: we found that there are currently thirty-five active users within the company, with thirty-six active workstations. These workstations comprise of a series of Laptops and Desktops under the Windows Operating System, as well as one user in the IT Department using Kali Linux on a desktop. Further findings found that there is one laptop with Kali Linux running on this, and this laptop was flagged as a test system for the Development Team.

The infrastructure that Big Dog company runs on is Windows Server and Linux Server. The Windows Server currently houses SQL Database, IIS Web Server, and PRTG Monitoring. The Ubuntu - Linux server, and was flagged as confidential, and contains the Intelligible Property or IP.

During the security breach, the agents that conducted the IoC did not compromise the Linux environments, however the 5 out of the 36 windows workstations were compromised. Further reviewed on the Windows Server would have been an issue if it was not for the current measures in place around that system.

Sensors

Sensor	Description	System	IOC Associated	Rationale	Priority	Thresholds / Assumptions
Packet Sniffer	Monitors the headers of data packets	NetworkHost / Probe Device	DoS/DDOS, Network Scanning, Malware, Port Scans, and IP Scans	IP Traffic - Abnormal or Unusual Traffic Volume - Spikes or abnormal trends	High Priority - “5 Stars”	Setting Threshold around 150%, when abnormal traffic spikes over 150%, this would trigger review. Assuming that network traffic wont have abnormal spikes in the normal
SNMP Traffic	Monitor Traffic Both (In and Out)	All	DDOS, Network Scanning, Malware, Port Scans, and IP Scans	Network Traffic for abnormal or suspicious traffic in both directions	High “5 Stars”	Assuming that regular traffic will not exceed the setted threshold to 90%.
IPFIX (Internet Protocol Flow Information Export)	Monitors Received Packets on UDP Ports. Sender and Receiver Packet on IP Addresses	Windows	Network Scanning, Phishy Attacks for websites and email traffic, password attacks	Monitoring for abnormalities with packet transfers	Medium - High “4 Stars”	Setting the flow counts for packets at Maximum 7000 purely based on the packet traffic with in the network More customization with this that can expand into IP Monitoring for new or untrusted IPs
MySQL_V2	Monitors for performance and execution on Queries	Windows Server	SQL Injection Attacks, Credential related attacks	Monitoring abnormal, anomalies related to extended query times, or unexpected outages with SQL Database.	Medium - High “4 Stars”	Multiple options for settings, Execution Time max of 5 seconds. Assumption that the latency is not impacting the query time. Downtime set with assumption there is no network outages
SNMP - Linux Physical Disk Sensor	Monitor Utilization of Hardware, this will determine usage irregular	Linux - Server	Spikes with the performance of the machine, Disk Errors	Monitoring the disk for hardware anomalies	Medium “3 Stars”	Setting disk usage threshold downtimes at 1 minute, with the assumption no power

	spikes			(Spikes)		outages. Disk Usage at 80% with the assumption that it should remain below 80%
SNMP - Linux Meminfo Sensor	Memory Monitoring	Linux - Server	High or Unusual Memory Usage, Dos/DDOS	Over Usage of Memory, abnormal memory spikes	Medium “3 Stars”	Free Memory and Free memory % set to 10% error limit, with a warning set to 20% Assumption is Linux has 10-20% memory free. Free Swap Space and Free Swap % set to 10% error limit, with a warning set to 20% Assumption is Linux has 10-20% memory free.
WMI Security Center Sensor	Windows Security Center and Action Monitors Firewall, antivirus, malware for example	Windows	Antivirus, Malware, network scanning	Maintaining the Antivirus that is deployed, assist with overall security on windows	Medium -High “4 Stars”	Setting running to maintain the inactivity as a flag, assuming the WMI security Center would not be disabled or turned off.
WMI Event Log Sensor	Monitors logs that have been specified, creates alerts for security incidents, or system errors, or other related items	Windows	Brute Force, Malware, DDoS/Dos Changes/Tampering	Monitoring the event IDs for changes, errors. Specific targets	High “5 Stars”	Event Type - Monitoring Event ID for privilege changes Setting the threshold for no more than 5 with in a 5 minute window. Assumption that the new users setup are not administrators.
HTTP	Monitors the IIS Web Server and the time to take to load the page.	Both	DDoS/Dos, Malware	Maintaining the Web Server that is hosted on the IIS Web Server.	Medium - High “4 Stars:	Setting up the following Thresholds: Timeout in Secs, Max set can be up to 15 minutes or 900 secs, Assumption is that the time frame would not impact a power outage or down for maintenance.

About the Sensors

Packet Sniffer
This sensor is great for monitoring the header of packets when they are being transferred around the network. This is a top level monitoring, which means that this is at the root of the network, and monitors network coming and going out.
IoC Impact Monitors: Denial of Service(DoS) or Distributed Denial of Service(DDOS,) Network Scanning, Malware, Port Scans, and IP Scans
Threshold: Setting Threshold around 150%, when abnormal traffic spikes over 150%, this would trigger review.

SNMP Traffic
This is a top level monitoring, which means that this is at the root of the network, and monitors network coming and going out. Can be placed on a device or on the network.
IoC Impact Monitors: Dos/DDOS, Network Scanning, Malware, Port Scans, and IP Scans
Threshold: Set a threshold of 90%, assuming that the regular traffic levels will generally remain below limit.

IPFIX (Internet Protocol Flow Information Export)
This Sensor monitors the received packets on User Data Protocol (UDP) Ports, monitors the sender and receivers packet based on IP Addresses, overall a great sensor for packet monitoring on Windows.
Recommended UDP Port to monitor is as follows.
Port 2055 - For Netflow with Cisco
Port 4793 - Standard port for IPFIX
Additionals can be added, 9995-9999. Please be advised each individual port will need individual IPFIX Sensor setup.
IoC Impact Monitors: Network Scanning, Phishy Attacks for websites and email traffic, password attacks, and port scanning
Threshold: Starting threshold recommendations are set to Minimum 50, Maximum 7000.

MySQL_v2 Sensor
This sensor is meant to monitor the SQL database, watching for abnormalities within the queries that are being made to the database.
IoC Impact Monitors: SQL Injection Attacks, Credential related attacks
Threshold: Multiple options for settings, Execution Time max of 5 seconds.
Assumption that the latency is not impacting the query time. Downtime set with assumption there is no network outages

SNMP - Linux Physical Disk Sensor
With the Linux Server having a confidential IP stored here, the utilization of the disk drives may be of importance in monitoring.
IoC Impact Monitors: Spikes with the performance of the machine, Disk Errors.
Threshold: Setting disk usage threshold downtimes at 1 minute, with the assumption no power outages.Disk Usage at 80% with the assumption that it should remain below 80%.

SNMP - Linux Meminfo Sensor
This sensor is a great monitor for the Linux Server having a confidential Intellectual prosperity, this would be great for monitoring and verifying that the RAM/Memory does not appear to be out of normal.
IoC Impact Monitors: High or Unusual Memory Usage, Dos/DDOS
Threshold: There are multiple configurations that would apply to SNMP - Linux Meminfo Sensor, these are our recommendations for starters.
Free Memory and Free memory % set to 10% error limit, with a warning set to 20%
Assumption is Linux has 10-20% memory free.
Free Swap Space and Free Swap % set to 10% error limit, with a warning set to 20%
Assumption is Linux has 10-20% memory free.

WMI Security Center Sensor
In addition to a security monitoring system and antivirus, this is a great way to monitor those solutions to verify that the AV is not disabled or inactive.
IoC Impact Monitors: Antivirus, Malware, network scanning
Threshold: Setting running to maintain the inactivity as a flag, assuming the WMI security Center would not be disabled or turned off.

Windows Event Viewer Sensor
This monitor is a great option to keep track of Event Viewer Logs that may go missing. This can be configured to monitor security incidents, system errors, and other flagged items or warnings.
IoC Impact Monitors: Brute Force,
Malware, DDoS/Dos
Changes/Tampering
Threshold: Event Type - Monitoring Event ID for privilege changes, setting the threshold for no more than 5 within a 5 minute window. Assumption that the new users setup are not administrators.

HTTP Sensor
Monitors the IIS Web Server and tracks the time it takes to load the web page(s) hosted on it, helps to identify performance issues or delays in the server response.
IoC Impact Monitors: DDoS/Dos, Malware
Threshold: Timeout in Secs, Max set can be up to 15 minutes or 900 secs, Assumption is that the time frame would not impact a power outage or down for maintenance.

Cat’s Team Recommendation

Here at Cat’s Security Solution, our recommendations regarding the Windows Server is to split this server into two server as soon as possible, keeping the SQL Database and PRTG Monitoring tool on the original device, and migrating the IIS Web Server on a segregated network, with its own firewall. We also recommend segregating the network with a separate firewall for the Linux Server for further protection of Big Dog’s IP.

With the sensors in play, monitoring for Indicators of Attack before the turn into Indicators of Compromise will be more mainstream now. As always, verifying that updates are done in a timely manner, and following the best practices with the monthly patches is key.

Citations/References

PRTG Manual: Available Sensor Types. (n.d.) Paessler The Monitoring Experts
Retrieved November 3, 2024,
From https://www.paessler.com/manuals/prtg/list_of_available_sensor_types

R. Grimmick(2023, June 23) *Network Flow Monitoring Explained: NetFlow vs sFlow vs IPFIX*
Varonix. https://www.varonis.com/blog/flow-monitoring

Vulnerabilities Citation:

NVD - CVE-2024-0126 (2024, October 26) NIST
https://nvd.nist.gov/vuln/detail/CVE-2024-0126

NVD - CVE-2024-0117 (2024, October 26) NIST
https://nvd.nist.gov/vuln/detail/CVE-2024-0117

Security Bulletin: Nvidia GPU Display Driver - October 2024 (2024, October 22) NVIDIA
https://nvidia.custhelp.com/app/answers/detail/a_id/5586

CVE-2024-0126 (2024, October 26) CVE
https://www.cve.org/CVERecord?id=CVE-2024-0126

CVE-2024-0117 (2024, October 26) CVE
https://www.cve.org/CVERecord?id=CVE-2024-0117

Best Practice Citations:

M. Souppaya, K. Scarfone(2022, April) *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
NIST https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

What are indicator of compromise (IoCs)(n.d.) Microsoft
Retrieved November 3 2024,
https://www.microsoft.com/en-ca/security/business/security-101/what-are-indicators-of-compromise-ioc#examples-of-IOCs