Cat Scan II Big Dog

Author: Sukhvir Kaur Sahota

**Executive Summary**

In today's era securing the Organisation from Cyber Threats is very important. This report details recommendations for Big Dog, a company aiming to bolster their network monitoring practices. The report acknowledges the growing prevalence of cyberattacks and emphasizes the importance of robust monitoring solutions. The BIG Dog Organization was recommended to use the PRTG (Paessler Router Traffic Grapher) to observe and analyze what is happening in their Organization. Based on sensor analysis data they can take required measures to enhance the Organisation’s security and protect the critical assets from the Cyber Threats.

This report is made by taking key assets of the Big Dog organization in consideration. The company decides to go with 20 sensors to start with. All sensors can help the Big Dog to get notified on different types of attacks that could be happening on those sensors. SIL Should be a major consideration for the security team so that they can plan and implement the best approaches to prevent the attack. SQL Database is mainly stored on Windows servers which make it more vulnerable and main priority to protect followed by the Linux system. Both Windows and Linux are used for the development purpose so it is important to maintain the Confidentiality, Integrity and Availability of both in every possible way so that BIG DOG do not have to face Data and Reputation loss.

This report also contains the examples of past vulnerability from NVD, (“The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP).”(12) ) to get more understanding on how attacks happened in past on Organizational assets. The company can use those examples and their details for better monitoring and training purposes.

To enhance website security, it is important to implement measures to prevent various types of attacks. After understanding all aspects related to assets' Risk, Vulnerability, IoC and SILA at last I have provided some recommendations to make the Big Dog organization more secure. The most important suggestion is to apply as many security and verification steps as possible in budget to avoid any kind of Access attack. Data Encryption, use of parameterized queries and traffic filtering can also save the organization from losing so much. Along with that, it is also very important to invest in training the employees so that they do know whom to contact and where to report if they notice any unusual activity.

**Introduction**

Wth advancement of technology the Cyber attacks are increasing every day. In 2023 itself 3205 data compromise cases were reported in the USA only(1). According to the IBM’s Cost of Data Breach report, The average cost of a data breach was $4.45 million in 2023, the highest average on record(2). To avoid these kinds of attacks the organizations use different data monitoring tools/softwares which help them with tracking of critical IT applications, networks,and infrastructures.

The purpose of this report is to develop monitoring solutions for Big Dog Organisation as they understand the Importance of monitoring the Network Traffic to rapidly detect anomalous activity and malicious behavior. There are various network monitoring tools available in the market, Big Dog decided to go with PRTG (Paessler Router Traffic Grapher) tool which is known for monitoring the entire IT infrastructure of a company.

Further, this report will explain that with detailed assessment of the different sensors on the servers of the Big Dog Organisation how they can know about the Vulnerabilities and Risks of the activities happening in their system.

**Key Assets**

Let's start with what we know about Big Dog. The Big Dog is securing a large network and their key assets are Windows Server, Linux, Kali, and Windows Workstations. The main focus should be on the Windows server as it contains the SQL database which plays a very Important role in Maintaining CIA Triad for the Organisation. Second main focus should be on Windows Workstation and Linux systems as they are used for development, also the Linux system is mainly used by the developers to create important proprietary intellectual property (IP) for the company.

The Big Dog Organisation decided to use a set of pre-selected sensors. Based on those sensors we will provide the information on how they can be set up for rational prioritization. The assumptions/monitoring recommendations are based on how asset being monitored, vulnerabilities, threats, tactics, techniques, and risk severity to the organization

**Tools and Technologies**

For this analysis I have used the CVE MITRE tool and NVD NIST tool to find out research about the type of Vulnerabilities associated with endpoint systems. My IoCs details and Rationale is based on the research from these tools. Also I used Cyber Kill chain and MITRE ATTACK framework for understanding the attackers point of view while doing the research.

CVE MITRE : <https://cve.mitre.org/>

NVD NIST : <https://nvd.nist.gov/>

MITRE ATT&CK : <https://attack.mitre.org/>

Cyber Kill Chain: <https://www.lockheedmartin.com/>

**Table**

For this table the Columns indicates the following information ( The column detail data is from the project instructions(3))

* *Sensor*: Generic sensor name
* *Description*: A short non-technical description of the sensor
* *System*: The endpoint that the sensor will be monitoring
* *IoCs*: The Indicators of Compromise that the sensor is expected to monitor
* *Rationale*: Why this sensor may have been chosen, linked to MITRE or some other framework information
* *Priority*: Based on the nature of Risk/IoC/SIL, etc.
* *Thresholds/ Assumption*s: Based on what is monitored. This column can also be used to specify any assumptions made.

| **Sensor** | **Description** | **System** | **IoCs Associated (May be more than 1)** | **Rationale** | **Priority** | **Thresholds /Assumptions** |
| --- | --- | --- | --- | --- | --- | --- |
| HTTP Load Time | Monitors the time it takes for the page to load. | Winserver | May be used to indicate Malicious Redirects, DDoS Attacks or Content Injection | Unexpected changes in load time can indicate anomalies or performance-related issues that could be indicative of a security breach or compromise | Medium (SIL 7) | Changes of 20% over the average load. SIL base on the fact that BIG DOG does NOT have a large Web Presence, the linux web server being internal and this one outward facing(Assumption) There is a relatively low impact on CIA (specifically A) but a higher chance of compromise I have assigned an SIL of 7 |
| HTTP Load Time | Monitors the time it takes for the page to load. | Linux | Maybe used to Indicate Content Injection in OS command,  Unauthorized access | Unexpected changes in load could indicate the injection of vulnerability in web applications. | High (SIL of 8) | SIL is based on the fact that Linx web server is the internal server in the case study and play very important role as it is Used by developers to create important proprietary intellectual property (IP) for the company |
| MySQL Database Query Sensor | Monitors and track the queries sent to My SQL Database server | Linux | Maybe use to indicate SQL Injection, Shall command injection and Database Abuse | Anomalies in query execution times may indicate potential SQL injection attacks or abusive database usage. | Medium(SIL of 7) | SIL is based on the assumption that the main Database is stored on the Windows server and Linux just has an internal MySQL Database , which is likely to have less Data stored. |
| MSSQL Database Query Sensor | Monitors and track queries to identify performance issue, security risk and optimized resource usage | Winserver | Unauthorized access or use of untrusted input and access of sensitive information | Anomalies in the query could be showing a vulnerability that untrusted user access to sensitive information which could lead to Database crash. | High( SIL of 9) | SIL is High based on the assumption that Winserver is the main server where the major Database sits. This server contains the information of the combined system and will act as a central system so it needs more security. |
| SSH Sensor | SSH is a protocol used to securely access remote systems over an unsecured network | Winserver/Linux | Unauthorized Access, Brute Force Attacks and Data Exfiltration | Monitoring SSH activity helps detect unauthorized access attempts or potential brute force attacks, which could lead to data exfiltration or system compromise | High  (SIL of 8) | Considering the assumption/data from case study both Linux and windows server are used by the developers to write codes. They both need major protections towards all 3 CIA trades. |
| Antivirus Status Sensor | Monitors the status of antivirus software | All | Malware Infections which could cause DOS | Will help to ensure that antivirus is running properly. Disruption in this sensor can indicate Malware threat such as Denial of services | High(SIL of 8) | Antivirus plays an important role for each and every type of system. Antivirus are capable of protecting systems from many attacks without even bothering the security team. |
| File Sensor |  | Winserver/Linux | Weak file permission results in unauthorized Access, Data Exfiltration | Change in Access pattern can indicate unauthorized access to sensitive files, unusual file modifications | High (SILof 8) | The SIL is based on the assumption that both these servers are mainly used for coding purposes so the files need to be more secure as they may contain the scripting and other sensitive information which could cause reputation damage in wrong hands. |
| Windows Event Log Sensor |  | Winserver | Could be use to find Improper Privileges, DoS attack | Anomaly in this sensor could indicate modification in the files which could also lead to Denial of services if accessed by attacker | High (SIL of 8) | This SIL -8, it is based on assumption that Windows server is outdoor main server and if the they logs get compromise from here then chances are it can impact the other servers as well |
| Windows Event Log Sensor |  | Windows1 and 2 | Maybe used to find unauthorized Modifications. | Anomaly in this sensor can be helpful for finding if a local user made any changes to events prior to them being sent to the main server. | Medium  (SILof 7) | The SIL is based on the assumption that Windows 1 and 2 will be used internally by employees who have limited access to logs, however, if they manage to get access then they can change the logs which can generate false vulnerabilities. |
| Bandwidth Usage Sensor |  | All | Maybe used to find DDoS Attacks, Network Intrusions | Unusual spikes or drops in network bandwidth usage can indicate DDoS attacks, data exfiltration, or unauthorized network intrusions, necessitating further investigation | Medium  (SILof 7) | SIL is medium based on the assumption that for any kind of Bandwidth attack the attacker might need to be present locally. This kind of attack can slow down the operation so it is still very Important to observe. |

**IoC explained**

In Cyber security IoC (Indicator of Compromise) is a term that refers to the evidence that points out security breach on the device(4). It is a very common practice to check IoC data for suspicious incidents which can further be used to detect the system vulnerabilities. With security tools such as PRTG, the security team of the Organisation can work fast on issues notified by sensors on Ioc and can contain them before they spread and cause harmful breach. The Data in the table is based on the search from NIST NVD and MITRE CVE. I took the following steps to get details.

1. Search for server in CVE.mitr.org
2. Filter with sensor
3. Pick the one you want to work with
4. Copy the CVE in NVD (advance search)
5. This will help you to find IoC and Rationale
6. Priority and Threshold should be based on what we think is important for a Big dog.
7. **Http Load time sensor for Windows Server**

**IoC**: This sensor is to monitor IoC Vulnerabilities for Malicious Redirects, DDoS Attacks or Content Injection.

**Rationale***:* In the tool/software, unexpected changes in load time can indicate anomalies or performance-related issues that could be indicative of a security breach or compromise.

**Example from NVD and MITRE CVE**

* [**CVE-2023-41266**](https://nvd.nist.gov/vuln/detail/CVE-2023-41266) : A path traversal vulnerability, allows an unauthenticated remote attacker to generate an anonymous session. This allows them to transmit HTTP requests to unauthorized endpoints.(12)
* **CVE-2020-13938** : Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows.(12)

**Risk and Vulnerabilities**

* ***Malicious redirects*** : Malicious redirects are caused by hackers injecting scripts into infected sites that send visitors to destinations where they usually get scammed or infected with malware.(5)

*Risk associate to it could be:*

* Phishing
* Malware distribution
* Identify theft
* Financial loss
* Reputation Damage
* ***DDoS Attacks***: A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic(6)

*Risk associate to it could be:*

* Service Disruption
* Data Breach
* Collateral Damage
* Regulatory Compliance Violation

1. **Http Load time sensor for Linux**

**IoC**: This sensor is to monitor IoC Vulnerabilities for Content Injection in OS command, DDoS Attacks.

**Rationale***:* In the tool/software, unexpected changes could indicate the injection of vulnerability in web applications. DDoS attacks can be observed by noticing performance related issues.

**Example from NVD and MITRE CVE**

* **CVE-2023-37477** :1Panel is an open source Linux server operation and maintenance management panel. An OS command injection vulnerability exists in 1Panel firewall functionality. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.(12)
* **CVE-2019-1853:** A vulnerability in the HostScan component of Cisco AnyConnect Secure Mobility Client for Linux could allow an unauthenticated, remote attacker to read sensitive information on an affected system. The vulnerability exists because the affected software performs improper bounds checks. An attacker could exploit this vulnerability by crafting HTTP traffic for the affected component to download and process. A successful exploit could allow the attacker to read sensitive information on the affected system.(12)

**Risk and Vulnerabilities**

* ***Content Injection*** : An“arbitrary text injection” or virtual defacement, is an attack targeting a user made possible by an injection vulnerability in a web application.(7)

*Risk Associated:*

* Data Integrity
* Cross-site Scripting (XSS)
* Server Compromise
* Reputation Damage
* ***Unauthorized access***: Gaining access to an organization's data, networks, endpoints, applications or devices, without permission needed or required. Unauthorized access to an Operational Technology (OT) environment poses significant risks and vulnerabilities due to the critical nature of these systems.

*Risk Associated:*

* Data Theft
* Supply chain risk
* Long Term Persistence
* Disruption of Operations

1. **MySQL Database Query Sensor for Linux**

**IoC**: This sensor is to monitor IoC Vulnerabilities for SQL Injection, Shall command Injection and Database abuse.

**Rationale***:* Anomalies in query execution times may indicate potential SQL injection, Shell command injections attacks or abusive database usage.

**Example from NVD and MITRE CVE**

* **CVE-2023-26034**: A user with the View or Edit permissions of Events may execute arbitrary SQL. The resulting impact can include unauthorized data access (and modification), authentication and/or authorization bypass, and remote code execution.(12)
* **CVE-2017-14478:** A specially crafted MMM protocol message can cause a shell command injection resulting in arbitrary command execution with the privileges of the mmm\\_agentd process. An attacker that can initiate a TCP session with mmm\\_agentd can trigger this vulnerability.(12)

**Risk and Vulnerabilities**

* ***SQL Injection*** : SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques(8).

*Risk Associated:*

* Data Exposure
* Data Manipulation
* Complete Denial of service
* Application Compromise
* ***Shall command Injection***: It allows an attacker to execute operating system (OS) commands on the server that is running an application, and typically fully compromise the application and its data.(9)

*Risk Associated:*

* Data Exfiltration
* Complete Denial of service
* Remote Code Execution
* Data Manipulation

1. **MSSQL Database Query Sensor for Winserver**

**IoC**: This sensor could be used for observing unauthorized access or use of untrusted input and access of sensitive information.

**Rationale***:* Anomalies in the query could be showing a vulnerability that untrusted user access to sensitive information which could lead to Database crash.

**Examplefrom NVD and MITRE CVE**

* **CVE-2023-1574** : Information disclosure in the user creation feature of a MSSQL data source in Devolutions Remote Desktop Manager 2023.1.9 and below on Windows allows an attacker with access to the user interface to obtain sensitive information via the error message dialog that displays the password in clear text.(12)
* **CVE-2007-2079** : Uses untrusted input for the database server hostname, which allows remote attackers to trigger a library buffer overflow and execute arbitrary code via a long host parameter, or have other unspecified impact. NOTE: it could be argued that this is an issue in mssql\_connect (CVE-2007-1411.1) in PHP, or an issue in the ADOdb Library, and the proper fix should be in one of these products; if so, then this should not be treated as a vulnerability in XAMPP. (12)

**Risk and Vulnerabilities**

* **Unauthorized access**: Gaining access to an organization's data, networks, endpoints, applications or devices, without permission needed or required. The unauthorized access to Microsoft SQL Server databases pose significant risks and vulnerabilities, particularly concerning data confidentiality, integrity, and availability.

*Risk Associated:*

* Data Breach
* Data Manipulation
* Data Exfiltration
* Credential Theft
* Reputation Damage

1. **SSH Sensor for Winserver/Linux**

**IoC**: SSH sensor likely refers to a sensor that monitors Secure Shell (SSH) activity. SSH is a protocol used to securely access remote systems over an unsecured network. An SSH sensor could track various aspects of SSH connections, such as unauthorized Access, Brute Force Attacks and Data Exfiltration.

**Rationale***:* Monitoring SSH activity helps detect unauthorized access attempts or potential brute force attacks, which could lead to data exfiltration or system compromise.

**Example from NVD and MITRE CVE**

* **CVE-2021-44151 :** An issue was discovered in Reprise RLM 14.2. As the session cookies are small, an attacker can hijack any existing sessions by brute forcing the 4 hex-character session cookie on the Windows version (the Linux version appears to have 8 characters). An attacker can obtain the static part of the cookie (cookie name) by first making a request to any page on the application (e.g., /goforms/menu) and saving the name of the cookie sent with the response. The attacker can then use the name of the cookie and try to request that same page, setting a random value for the cookie. If any user has an active session, the page should return with the authorized content, when a valid cookie value is hit.(12)
* **CVE-2021-38931**: IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and 11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from.(12)

**Risk and Vulnerabilities**

* **Brute Force Attacks** :A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys (10).

*Risk Associated:*

* Credential Theft
* Data Breach
* Account Takeover
* Reputation Damage

1. **Antivirus Status Sensor for All**

**IoC**:This sensor could be used to find Malware Infections which could cause DOS attacks.

**Rationale***:* An Antivirus status sensor is a component of antivirus software that monitors the real-time status of antivirus protection on a computer system. It checks whether the antivirus software is active, up-to-date with the latest virus definitions, and functioning properly. The sensor typically provides feedback to users or administrators about the security status of the system, helping to ensure that the system is adequately protected against malware threats.

**Example from NVD and MITRE CVE**

* **CVE-2009-1783:** Multiple FRISK Software F-Prot anti-virus products, including Antivirus for Exchange, Linux on IBM zSeries, Linux x86 File Servers, Linux x86 Mail Servers, Linux x86 Workstations, Solaris Mail Servers, Antivirus for Windows, and others, allow remote attackers to bypass malware detection via a crafted CAB archive.(12)
* **CVE-2007-1281**: Kaspersky AntiVirus Engine 6.0.1.411 for Windows and 5.5-10 for Linux allows remote attackers to cause a denial of service (CPU consumption) via a crafted UPX compressed file with a negative offset, which triggers an infinite loop during decompression.(12)

**Risk and Vulnerabilities**

* **A denial-of-service (DoS**): This attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.(11)

Indicators of Compromise (IoC) related to Denial of Service (DoS) attacks targeting the antivirus status pose specific risks and vulnerabilities, particularly concerning the security and operability of endpoint protection systems.

*Risk Associated:*

* Endpoint protection Disruption
* Malware Propagation
* Exploitation of other inside vulnerabilities
* Regulatory Compliance Violation

1. **File Sensor for Winserver/Linux**

**IoC**: If the file permission are too weak and easy to change, this results in unauthorized Access and Data Exfiltration.

**Rationale***:* Anomaly in this sensor could be an indication of unauthorized access to sensitive files, unusual file modifications, or ransomware activity, helping prevent data exfiltration or file encryption.

**Example from NVD and MITRE CVE**

* **CVE-2019-17388**: Weak file permissions applied to the Aviatrix VPN Client through 2.2.10 installation directory on Windows and Linux allow a local attacker to execute arbitrary code by gaining elevated privileges through file modifications.(12)
* **CVE-2023-4554**: Improper Restriction of XML External Entity Reference vulnerability in OpenText AppBuilder on Windows, Linux allows Server Side. Request Forgery, Probe System Files. AppBuilder's XML processor is vulnerable to XML External Entity Processing (XXE), allowing an authenticated user to upload specially crafted XML files to induce server-side request forgery, and to disclose files local to the server that processes them.(12)

**Risk and Vulnerabilities**

* ***Data Exfiltration*** : The unauthorized transfer of information from an information system. In this case data is stored in the form of files.

*Risk Associated:*

* Loss of sensitive Information
* Intellectual Property theft
* Business Espionage
* Operational Disruption

1. **Windows Event Log Sensor for Winserver**

**IoC**: The Event log sensor could be used to find Improper Privileges to files which could lead toDoS attack.

**Rationale**: Anomaly in this sensor could indicate modification in the files which could also lead to Denial of services if accessed by an attacker.

**Example from NVD and MITRE CVE**

* **CVE-1999-1361:** Windows NT 3.51 and 4.0 running WINS (Windows Internet Name Service) allows remote attackers to cause a denial of service (resource exhaustion) via a flood of malformed packets, which causes the server to slow down and fill the event logs with error messages.(12)
* **CVE-2020-1371**: An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'.(12)

**Risk and Vulnerabilities**

* **Improper privileges/DoS :** This refers to a situation where outside users/Hacker manage to go inside a system with insufficient permissions and then are able to access event logs.

*Risk Associated:*

* Data Exfiltration
* Service Disruption
* Can cause Denial of services

1. **Windows Event Log Sensor for Windows 1 and 2**

**IoC**: This event log sensor coils be used for Internal users to find unauthorized Modifications to the logs.

**Rationale***:* Anomaly in this sensor can be helpful for finding if a local user made any changes to events prior to them being sent to the main server.

**Example from NVD and MITRE CVE**

* **CVE-2021-31839:** Improper privilege management vulnerability in McAfee Agent for Windows prior to 5.7.3 allows a local user to modify event information in the MA event folder. This allows a local user to either add false events or remove events from the event logs prior to them being sent to the ePO server.(12)
* **CVE-2011-2779**: Windows Event Log SmartConnector in HP ArcSight Connector Appliance before 6.1 uses world-writable permissions for exported report files, which allows local users to change or delete log data by modifying a file.(12)

**Risk and Vulnerabilities**

* **Unauthorized modifications form Internal users :** This refers to a situation where internal users try to manipulate the system by modifying logs.

*Risk Associated:*

* Insider Threat
* Data Tampering
* Loss of Forensic Evidence

1. **Bandwidth Usage Sensor for All**

**IoC**: Maybe used to find DDoS Attacks, Network Intrusions.

**Rationale***:* Unusual spikes or drops in network bandwidth usage can indicate DDoS attacks, data exfiltration, or unauthorized network intrusions, necessitating further investigation.

**Example from NVD and MITRE CVE**

* **CVE-2024-1185 :** A vulnerability classified as problematic has been found in Nsasoft NBMonitor Network Bandwidth Monitor 1.6.5.0. This affects an unknown part of the component Registration Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252675. NOTE: The vendor was contacted early about this disclosure but did not respond in any way**.**(12)
* **CVE-2020-5982 :** NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) scheduler, in which the software does not properly limit the number or frequency of interactions that it has with an actor, such as the number of incoming requests, which may lead to denial of service.(12)

**Risk and Vulnerabilities**

* **Network Intrusions :** network intrusion based on bandwidth usage can have significant implications for an organization's network infrastructure, security posture, and operational continuity.

*Risk Associated:*

* Operational Cost
* Denial of service
* Network Congestion
* Service disruption

**SIL Priority**

SIL (Safety Integrity Level) is a measure of the reliability and availability of system functions. In simple terms we can say that the more you require to reduce risk from the asset, the more SIL needs for it.

To Measure the SIL, an SC question can play an important role , it is based on the CIA Triad to calculate how important the assets/system to organization based on protection level needed for its Confendinatilay, Integrity and Availability.

**SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}**

Let's break down each component to understand its purpose, who uses it, and how it is assessed:

***Confidentiality*** ensures that information is accessible only to those authorized to have access. It's about protecting personal information or proprietary data from unauthorized individuals or systems.

***Integrity*** involves maintaining the accuracy and consistency of data over its entire lifecycle. This means that the data cannot be altered in an unauthorized or undetected manner.

***Availability*** refers to ensuring timely and reliable access to and use of information or resources. This component is about making sure that data and systems are available to authorized users when they need it.

By keeping in mind the above Equation, I assume the SIL Level is given in table the SIL Level. I arrange the Sensors from High to low.

1. ***HTTP Load Time for Linux*** : {(confidentiality, High), (integrity, Medium to High), (availability, High)}
2. ***MSSQL Database Query for Winserver*** = {(confidentiality, High), (integrity,High), (availability, Medium to High)}
3. ***Windows Event Log Sensor for Winserver*** = {(confidentiality, High), (integrity,High), (availability, Medium)}
4. ***File sensor for Winserver/Linux*** = {(confidentiality, High), (integrity, High), (availability, Medium)}
5. ***SSH Sensor for Winserver/Linux*** = {(confidentiality, High), (integrity,High), (availability, Medium)}
6. ***Antivirus Status Sensor for All servers*** = {(confidentiality, Medium), (integrity,Medium), (availability, Medium)}
7. ***MySQL Database for Linux*** = {(confidentiality, Medium), (integrity, Medium to High), (availability, Medium to High)}
8. ***HTTP Load Time for Winserver*** = {(confidentiality, Medium), (integrity, Medium), (availability, High)}
9. ***Bandwidth Usage Sensor for all system*** ={(confidentiality, Medium), (integrity,Medium), (availability, Medium)}
10. ***Windows Event Log Sensor for Windows 1 and 2*** = {(confidentiality, Medium), (integrity,Medium), (availability, Medium)}

As you can see some of the SIL have an impact on CIA triads, by implementing some of the recommendations below in the recommendation the BIG DOG can make their Organisation more secure.

**Recommendations**

In search of IoC and vulnerabilities I found various types of Attacks that could be caused by system vulnerabilities. The list below gives information on what can be done to make the BIG DOG more secure.

1. ***Malicious Redirects***:

* Implement URL filtering and validation mechanisms.
* Regularly monitor website traffic for suspicious patterns.
* Keep web servers and applications updated with the latest security patches.

1. ***DDoS Attacks:***

* Use a DDoS mitigation service.
* Implement rate limiting and traffic filtering techniques.
* Distribute server infrastructure geographically to avoid regional attacks.

1. ***Content Injection:***

* Implement input validation and sanitization techniques.
* Use parameterized queries to prevent SQL injection attacks.
* Implement web application firewalls (WAFs) to detect and block injection attempts.

1. ***Unauthorized Access:***

* Enforce strong authentication mechanisms such as multi-factor authentication (MFA).
* Implement access controls and role-based permissions.
* Audit user accounts and access logs for anomalies.

1. ***SQL Injection:***

* Use parameterized queries or ORM frameworks to prevent direct SQL manipulation.
* Employ WAFs to detect and block SQL injection attempts.
* Regularly review and sanitize database inputs.

1. ***Shell Command Injection:***

* Avoid using user input directly in shell commands.
* Implement proper input validation and sanitization.
* Limit the use of system commands to only necessary operations.

1. ***Brute Force Attacks:***

* Implement account lockout mechanisms after multiple failed login attempts.
* Use CAPTCHA or reCAPTCHA challenges to deter automated brute force attacks.
* Monitor login attempts and block IP addresses with suspicious behavior.

1. ***Denial-of-Service (DoS):***

* Implement rate limiting and traffic filtering.
* Utilize a content delivery network (CDN) to distribute traffic and absorb attacks.
* Configure firewalls to block traffic from known malicious sources.

1. ***Data Exfiltration:***

* Encrypt sensitive data both in transit and at rest.
* Implement data loss prevention (DLP) solutions such as Google Cloud Data Loss Prevention to monitor and prevent unauthorized data transfers.
* Enforce strict access controls to limit data access to authorized users.

1. ***Improper Privileges/DoS:***

* Implement the principle of least privilege.
* Regularly review and update user roles and permissions.
* Monitor privilege escalation attempts and unauthorized access.

1. ***Unauthorized Modifications from Internal Users:***

* Implement version control systems to track changes made by internal users.
* Utilize file integrity monitoring (FIM) solutions to detect unauthorized modifications.
* Educate employees on security best practices and enforce policies regarding data handling.

1. ***Network Intrusions:***

* Implement intrusion detection and prevention systems (IDPS).
* Utilize network segmentation to isolate critical assets.
* Regularly audit network configurations and monitor for unauthorized devices or connections.

**Video Presentation Link**

<https://drive.google.com/file/d/13HL91yKol-NcMk6bCjm22zEueNw7pKI2/view?usp=sharing>

**PPT Link**

<https://docs.google.com/presentation/d/122Z8ho0efL2d0dl0ucF4c5Itttg3JdZt1Tu5pErNQyo/edit#slide=id.g2cc9c886abe_0_96>

**References**

1. Statista. (2024, February 12). Number of data compromises and impacted individuals in U.S. 2005-2023. <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>
2. Cost of a data breach 2023 | IBM. (n.d.). <https://www.ibm.com/reports/data-breach>
3. Welcome to Compass. (n.d.). <https://web.compass.lighthouselabs.ca/p/14/projects/risks-report?day_number=w02d5>
4. What is IOC in Cyber Security? - Logsign. (n.d.). Logsign. <https://www.logsign.com/blog/what-is-ioc-in-cyber-security/>
5. Martori, A. (2020b, May 22). Understanding & stopping malicious redirects. Sucuri Blog. <https://blog.sucuri.net/2020/05/malicious-redirects.html#:~:text=Malicious%20redirects%20are%20caused%20by%20hackers%20injecting%20scripts,or%20redirect%20%E2%80%94%20visitors%20from%20their%20intended%20websites>.
6. What is a DDoS attack? (n.d.). https://www.cloudflare.com/. <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>
7. Content spoofing | OWASP Foundation. (n.d.). <https://owasp.org/www-community/attacks/Content_Spoofing#:~:text=Content%20spoofing%2C%20also%20referred%20to,vulnerability%20in%20a%20web%20application>.
8. SQL injection. (n.d.). <https://www.w3schools.com/sql/sql_injection.asp#:~:text=SQL%20injection%20is%20a%20code,statements%2C%20via%20web%20page%20input>.
9. What is OS command injection, and how to prevent it? | Web Security Academy. (n.d.). <https://portswigger.net/web-security/os-command-injection#:~:text=OS%20command%20injection%20is%20also,the%20application%20and%20its%20data>.
10. What is a Brute Force Attack? | Definition, Types & How It Works. (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/brute-force-attack#:~:text=A%20brute%20force%20attack%20is,and%20organizations'%20systems%20and%20networks>.
11. What is a denial-of-service (DoS) attack? (n.d.). CloudFlare. <https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/>
12. NVD - Home. (n.d.). https://nvd.nist.gov/