Stage 1: SANS 20 - AI Based Threat

1) SANS 20 Framework Overview

The SysAdmin, Audit, Network, and Security (SANS) Institute is one of the leading organizations providing cybersecurity training, research, and certification. Their decades of experience in the field led them to publish their cybersecurity framework, the Incident Handler's Handbook, in 2012. The SANS CIS Critical Security Controls (SANS CIS) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

Since its release, the SANS framework has been recognized as one of the most comprehensive incident response approaches and has been implemented by many influential organizations worldwide.

The SANS 20 Security Controls, published by the Center for Strategic International Studies (CSIS), are prioritized mitigation steps that your organization can use to improve cyber security. They include a set of 20 controls that will help you counter common threat pathways and remediate potential vulnerabilities. The SANS Top 20 CSCs are often used by organizations that have yet to develop a comprehensive security information program. Learn more about the 20 critical security controls and what they mean for your organization.

The 20 critical security controls include:

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Cyber attackers will typically scan address spaces waiting for new and unprotected IT assets to be added to the system. The first control encourages companies to use an inventory discovery tool to automatically log and track all devices that exist in the company’s IT infrastructure. Many organizations do not have a complete list of all assets that need protection.

Critical Control 2: Inventory of Authorized and Unauthorized Software

SANS encourages companies to include authorized and unauthorized software in their IT asset inventory database. Most cyber attacks are carried out using a combination of social engineering, phishing emails and, vulnerabilities — Java, Adobe Flash and Acrobat, Firefox and Chrome plugins, 0-day client-side / browser vulnerabilities. The vulnerability discovery tool should automatically include both types of software into the scanning process to ensure that these assets are protected as well.

SANS Critical Control 3: Secure Configurations

Control 3 focuses on ensuring companies set up and install the proper security configurations on all workstations, laptops, servers, and mobile devices. Individuals can use a configuration review scanner and authenticated scans to monitor the security of their operating systems automatically and make sure they aren’t affected by malware.

Critical Control 4: Continuous Vulnerability Assessment and Remediation

The fourth control focuses on the value of continuous vulnerability management and remediation. Many companies will only scan their assets for potential vulnerabilities every three to six months, which may be the bare minimum for

compliance purposes. Still, SANS urges companies to monitor their assets continuously. Hackers are waiting for potential vulnerabilities to pop up online. Companies simply can't afford to wait every few weeks to perform an audit. The latest vulnerability assessment and remediation software will scan assets every few seconds for continuous monitoring. The system will then alert the IT department, so they can remediate vulnerabilities by patching the system as soon as possible.

Critical Control 5: Malware Defenses

Malware remains a dangerous threat to organizations of all sizes. Companies can use the last vulnerability management software to automatically scan assets for malware before it can spread to other parts of the network.

Critical Control 6: Application Software Security

Web and mobile applications can often be the weakest link in the security chain. This control encourages companies to install web application firewalls to protect these applications while including them in the VRM scanning process.

Critical Control 7: Wireless Device Control

Wireless networks and the devices that use them often lack the necessary security protocols to ward off a potential attack. Control 7 outlines the ways in which organizations can test, monitor, and analyze their wireless networks for potential vulnerabilities while encrypting sensitive information and setting administrative privileges.

Critical Control 8 and 9: Data Recovery Capability & Security Skill Assessment

Control 8 refers to an organization's ability to recover data in the event of a breach or attack. This often includes storing a secure backup outside of the company's IT system.

Control 9 refers to an organization's ongoing security training program and security skill improvement. Employees need to regularly improve their skills to keep up with the latest trends in cyber security.

Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

This control speaks to the importance of setting security configurations for network devices, including internet routers, which often lack the necessary cyber security protections.

Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

Control 11 focuses on limiting access to network ports, protocols, and other services. The latest VRM software will analyze production systems for unauthorized ports, protocols, and services while blocking unauthorized users using the application firewall.

Critical Control 12: Controlled Use of Administrative Privileges

This control deals with an organization's ability to track and control the use of administrative privileges.

Critical Control 13: Boundary Defense

Boundary defenses are cybersecurity tools that automatically differentiate networks based on their trustworthiness such as firewalls, intrusion detection and prevention systems, web content filtering, network access controls, routers/switches, and proxy servers that can help organizations prevent attacks.

Critical Controls 14 and 15: Audit Logs and Controlled Access

Control 14 refers to audit logs for firewalls, network devices, servers, and hosts. They are usually the only way to

determine whether the host has been compromised. The logs need to be aggregated, safeguarded, and correlated with other relevant security events. Control 15 deals with controlling access to data from people with the appropriate need to know, based on their level in the organization. This can help organizations prevent sensitive information from falling into the wrong hands.

Critical Control 16: Account Monitoring and Control

This control talks about the need to the protect privileged user and administrative accounts. Automatic scanning tools will automatically identify potential access control vulnerabilities, including expired or weak passwords and outdated lockout policies.

Critical Controls 17, 18 and 19: Data Loss Prevention, Incident Response and Management, Secure Network Engineering

These controls focus on how companies can prevent potential data breaches, improve their incident response times, and avoid permanent data loss.

Critical Control 20: Penetration Tests and Red Team Exercises

The last control talks about the importance of penetration testing and how companies can hire ethical hackers to conduct simulated attacks on the system without disrupting operations. The organization can then patch the system before a real attack occurs.

Download the full SANS 20 Critical Security Controls Whitepaper from NopSec to understand each control and how features in Unified VRM map to the respective control.

2) AI-Based Threat Identification Within SANS 20

AI can enhance threat identification within the SANS Top 20 Critical Security Controls by employing machine learning algorithms to analyze patterns, anomalies, and known attack vectors. It can assist in real-time detection, behavioral analysis, and automated response, improving the overall security posture of an organization.

AI and machine learning can be integrated into the SANS 20 framework in the following ways:

- **Data analysis and visualization**: AI and machine learning can help analyse and visualize large and complex data sets, such as network logs, security events, or threat intelligence, to identify patterns, trends, anomalies, or correlations that may indicate potential or ongoing attacks. AI and machine learning can also help present the data in an intuitive and interactive way, such as dashboards, charts, or graphs, to facilitate the understanding and communication of the security situation and status.
- **Anomaly and intrusion detection**: AI and machine learning can help detect and alert any abnormal or suspicious activities or behaviours on the network or the system, such as unauthorized access, data exfiltration, malware infection, or denial of service, that may signify an intrusion attempt or a breach. AI and machine learning can also help classify and prioritize the alerts based on the severity, impact, or likelihood of the threat, and provide recommendations or actions to respond or mitigate the threat.
- **Threat intelligence and prediction**: AI and machine learning can help collect and analyse information from various sources, such as open source, commercial, or proprietary, to provide relevant and actionable intelligence on the current or emerging threats, such as threat actors, tactics, techniques, or procedures, that may target or affect the organization. AI and machine learning can also help predict the future or potential threats, based on the historical or current

data, and provide proactive or preventive measures to protect the organization.

- **Automation and orchestration**: AI and machine learning can help automate and orchestrate various security tasks or processes, such as scanning, patching, backup, or recovery, to improve the efficiency and effectiveness of the security operations. AI and machine learning can also help integrate and coordinate various security tools or systems, such as firewalls, antivirus, or SIEM, to provide a holistic and consistent security view and response.

- **Examine AI Algorithms: Explore various AI algorithms and techniques employed in threat identification, such as anomaly detection, behaviour analysis, and predictive analytics, as per SANS 20's guidelines.**

SANS 20 provides guidance and best practices for implementing various AI algorithms and techniques for threat identification, such as:

- Behaviour analysis: Behaviour analysis is the technique of monitoring and analysing the patterns and trends of the network or system users, devices, or applications, to understand their normal or expected behaviours, and to identify any deviations or changes that may indicate malicious or compromised activities. AI algorithms, such as machine learning or natural language processing, can help automate and enhance the behaviour analysis process, by extracting and processing various features, such as user profiles, device attributes, or application logs, and by applying various methods, such as association, correlation, or sentiment analysis, to analyse and interpret the behaviours.
- Anomaly detection: Anomaly detection is the technique of identifying and alerting any abnormal or suspicious activities or behaviours on the network or the system, such as unauthorized access, data exfiltration, malware infection, or denial of service, that may signify an intrusion attempt or a breach. AI algorithms, such as machine learning or deep learning, can help automate and enhance the anomaly detection process, by learning from the historical or current data, and by applying various methods, such as clustering, classification, or regression, to detect and classify the anomalies. For example, one of the web search results1 shows how a deep learning model based on convolutional neural networks (CNNs) and long short-term memory (LSTM) networks can be used to detect anomalies in network traffic.
- Predictive analytics: Predictive analytics is the technique of using data and statistics to forecast and anticipate the future or potential threats, based on the historical or current data, and to provide proactive or preventive measures to protect the organization. AI algorithms, such as machine learning or deep learning, can help automate and enhance the predictive analytics process, by learning from the data and applying various methods, such as regression, classification, or neural networks, to generate and evaluate the predictions.

- **Study Integration Practices: Investigate best practices and recommended methodologies for integrating AI-driven threat identification into the SANS 20 framework.**

Some of the best practices and recommended methodologies for integrating AI-driven threat identification into the SANS 20 framework are:

- **Model development**: Model development is the core of AI-driven threat identification, as it is used to create, train, and test the AI models, as well as to provide outputs and predictions for the threat identification process. Therefore, model development is crucial for ensuring the

robustness, effectiveness, and reliability of the AI models. Some of the model development practices include:

- Model selection: Select the appropriate AI technique and algorithm for the threat identification task, based on the data, the objective, and the criteria. For example, machine learning techniques, such as supervised, unsupervised, or reinforcement learning, can be used to learn from the data and provide outputs or actions. Deep learning techniques, such as convolutional neural networks, recurrent neural networks, or generative adversarial networks, can be used to learn from complex and high-dimensional data and provide outputs or actions. Natural language processing techniques, such as natural language understanding, natural language generation, or sentiment analysis, can be used to process and analyse textual data and provide outputs or actions. Computer vision techniques, such as image recognition, face detection, or object detection, can be used to process and analyse visual data and provide outputs or actions.
- Model training: Train the AI model using the pre-processed and analysed data, and adjust the model parameters, such as weights, biases, or hyperparameters, to optimize the model performance and minimize the model error. Use appropriate methods and tools, such as gradient descent, backpropagation, or cross-validation, to train the AI model. Ensure that the model training process avoids overfitting or underfitting, and balances the trade-off between bias and variance.
- Model testing: Test the AI model using the unseen or new data, and evaluate the model performance and accuracy using various metrics, such as precision, recall, F1-score, or ROC curve. Use appropriate methods and tools, such as confusion matrix, error analysis, or A/B testing, to test the AI model. Ensure that the model testing process validates the model generalization and robustness, and identifies the model strengths and weaknesses.
- Model deployment: Deploy the AI model into the production environment, and integrate the model with the security controls and systems, such as firewalls, antivirus, or SIEM, to provide threat identification outputs and predictions. Use appropriate methods and tools, such as containers, APIs, or microservices, to deploy the AI model. Ensure that the model deployment process ensures the model scalability and compatibility, and monitors the model performance and feedback.

- **Data management**: Data is the foundation of AI-driven threat identification, as it is used to train, test, and validate the AI models, as well as to provide inputs and outputs for the threat identification process. Therefore, data management is crucial for ensuring the quality, security, and privacy of the data. Some of the data management practices include:

  - Data collection: Collect relevant and reliable data from various sources, such as network logs, security events, or threat intelligence, to provide comprehensive and diverse information for the threat identification process. Use appropriate methods and tools, such as web scraping, APIs, or sensors, to collect the data. Ensure that the data collection process complies with the legal and ethical requirements, such as consent, transparency, or anonymization.
  - Data preprocessing: Preprocess the data to remove any noise, outliers, errors, or inconsistencies, and to transform the data into a suitable format and structure for the AI models. Use appropriate methods and tools, such as cleaning, filtering, normalization, or encoding, to preprocess the data. Ensure that the data preprocessing process preserves the integrity and validity of the data.
  - Data storage: Store the data in a secure and accessible location, such as a database, a cloud, or a data lake, to enable the data retrieval and usage for the AI models. Use appropriate methods and tools, such as encryption, authentication, or backup, to store the data. Ensure that the data storage process protects the confidentiality and availability of the data.
  - Data analysis: Analyse the data to understand its characteristics, patterns, trends, anomalies, or correlations, and to extract useful and meaningful insights and features for the AI models. Use appropriate methods and tools, such as statistics, visualization, or feature selection, to analyse the data. Ensure that the data analysis process enhances the accuracy and performance of the AI models.

- **Model governance**: Model governance is the oversight of AI-driven threat identification, as it is used to monitor, audit, and improve the AI models, as well as to provide accountability and transparency for the threat identification process. Therefore, model governance is crucial for ensuring the explain ability, ethics, and security of the AI models. Some of the model governance practices include:

    - Model monitoring: Monitor the AI model during and after the deployment, and track the model performance, behaviour, and impact, using various indicators, such as accuracy, reliability, or fairness. Use appropriate methods and tools, such as dashboards, alerts, or logs, to monitor the AI model. Ensure that the model monitoring process detects and reports any model anomalies, errors, or failures, and provides feedback and improvement suggestions.
    - Model auditing: Audit the AI model periodically or on-demand, and review the model design, development, and deployment, using various standards, such as SANS 20, NIST, or ISO, to ensure the model compliance and quality. Use appropriate methods and tools, such as checklists, reports, or certifications, to audit the AI model. Ensure that the model auditing process verifies and validates the model correctness and effectiveness, and identifies and mitigates any model risks or issues.
    - Model improvement: Improve the AI model continuously or iteratively, and update the model data, parameters, or outputs, based on the model feedback, evaluation, or auditing, to enhance the model performance and accuracy. Use appropriate methods and tools, such as retraining, fine-tuning, or transfer learning, to improve the AI model. Ensure that the model improvement process adapts and evolves the model to the changing data, environment, or requirements, and maintains the model relevance and value.
    - Model explanation: Explain the AI model to the stakeholders, such as users, customers, or regulators, and provide the model rationale, logic, or evidence, for the model outputs and predictions, to ensure the model transparency and trustworthiness. Use appropriate methods and tools, such as feature importance, decision trees, or saliency maps, to explain the AI model. Ensure that the model explanation process clarifies and justifies the model decisions and actions, and addresses any model uncertainties or biases.
    - Model ethics: Ethically design, develop, and deploy the AI model, and consider the model impact and consequences, on the stakeholders, such as individuals, groups, or society, to ensure the model fairness and responsibility. Use appropriate methods and tools, such as ethical principles, frameworks, or guidelines, to ethically guide the AI model. Ensure that the model ethics process respects and protects the stakeholder rights and values, such as privacy, dignity, or diversity.

3) Practical Application and Simulation

- **Hands-On Simulations: Utilize cybersecurity simulation tools or platforms that demonstrate AI-driven threat identification aligned with the SANS 20 framework. Engage in hands-on exercises to understand the practical application of AI in threat detection.**

SANS stands for **S**ysAdmin, **A**udit, **N**etwork, and **S**ecurity.

1. **SANS Category:- CWE-119**: **Memory Buffer Error**
   Description:-
   This buffer overflow happens when an application process tries to store more data than it can hold in the memory. The data flows to another memory location which can corrupt the data already contained in that buffer.This could be disastrous, as this can erase data, steal confidential information, and even the whole application could crash because of this buffer overflow.

Business Impact:-
Memory buffer errors can cause applications to crash lead to system downtime. Exploitation of memory buffer errors disrupts the business operations and impact the continuity of services. If the affected system provides services to customers, the exploitation of memory buffer errors can lead to service outages, inconveniencing and frustrating users.

2. **SANS Category:- CWE-79: Cross-site Scripting**
   Description:-

   Cross-site Scripting (XSS) is an injection attack that usually happens when a malicious actor or an attacker injects malicious or harmful script into a web application which can be executed through the web browsers. Once the malicious script finds its way into the compromised system, it can be used to perform different malicious activities.

   Business Impact:-
   Cross-Site Scripting (XSS) attacks can harm a business by stealing user data, damaging its reputation, causing financial losses, and leading to legal consequences. Fixing these vulnerabilities involves implementing secure coding practices to protect websites and applications from malicious script injections.

3. **SANS Category:- CWE-20**: **Unvalidated Input Error**

   Description:-

   The application receives input, but fails to validate the input, whether it has all necessary details needed for it to be accepted into the system for processing.When there is input sanitization, this can be used to check any potentially dangerous inputs in order to ensure that the inputs are safe to be processed with the source code or when it's an input that is needed to communicate with other components.

   Business Impact:-
   Unvalidated Input Errors (CWE-20) pose a risk of security breaches, financial losses, and reputation damage by allowing malicious data input, necessitating robust input validation measures to safeguard against unauthorized access and maintain data integrity.

4. **SANS Category:- CWE-200**: **Sensitive Information Exposure Error**
   Description:-

This happens when the application knowingly and unknowingly exposes information that is confidential and sensitive to an attacker who does not have the authorization to access these information.Different errors lead to this information being exposed to an attacker.

Business Impact:-
Sensitive Information Exposure (CWE-200) can result in severe business impact, including compromised data confidentiality, loss of customer trust, and potential legal consequences, necessitating robust security measures to protect sensitive information and maintain regulatory compliance.

5. **SANS Category:- CWE-125**: **Out-of-bounds Read Error**
   Description:-

   This usually occurs when the application reads data past the normal level, either to the end or before the beginning of the buffer. This gives unprivileged access to an attacker to read sensitive information from other memory locations, which can as well leads to a system or application crash.A crash will certainly happen when the code reads data and thinks there is an indicator in place that stops the read operation like a NULL that is applied to a string

   Business Impact:-
   Out-of-bounds Read Error (CWE-125) can lead to security vulnerabilities, system crashes, and unauthorized access, posing a risk of data breaches and significant business disruption, emphasizing the need for thorough code reviews and preventive measures to ensure secure software development.

6. **SANS Category:- CWE-89: SQL Injection**
   Description:-

   SQL injection is a form of security vulnerability whereby the attacker injects a Structured Query Language (SQL) code to the Webform input box in order to gain access to resources or change data that is not authorized to access.This vulnerability can be introduced to the application during the design, implementation, and operation stages.What this SQL query does is to make an unauthorized request to the database for some information.

   Business Impact:-

   SQL Injection (CWE-89) can result in unauthorized access, data breaches, and manipulation of databases, causing severe business impact such as compromised data integrity, reputational damage, and potential legal consequences, necessitating strict input validation and parameterized queries to mitigate risks.

7. **SANS Category:- CWE-416: Free Memory Error**
   Description:-

   This issue is caused by the referencing of memory after it has been released, which can seriously lead to a program crash. When you use a previously freed memory, this can have adverse consequences, like corrupting of valid data, arbitrary code execution which is dependent on the flaw timing.

Business Impact:-
Free Memory Error (CWE-416) can lead to application crashes, data corruption, and potential security vulnerabilities, posing a risk of system instability, service disruption, and exploitation by attackers, emphasizing the importance of proper memory management practices for business continuity and security.

8. **SANS Category:- CWE-190: Integer Overflow Error**
Description:-

When a calculation is processed by an application and there is a logical assumption that the resulting value will be greater than the exact value, integer overflow happens. Here, an integer value increases to a value that cannot be stored in a location.

Business Impact:-
Integer Overflow Error (CWE-190) can result in unexpected behavior, crashes, or security vulnerabilities, posing a risk of system instability, data corruption, and potential exploitation, highlighting the need for secure coding practices to prevent business disruptions and safeguard against malicious activities.

9. **SANS Category:- CWE-352: Cross-Site Request Forgery**
Description:-

This is when a web application does not sufficiently verify the HTTP request, whether the request was actually coming from the right user or not. The webservers are designed to accept all requests and to give a response to them.

Business Impact:-

Cross-Site Request Forgery (CWE-352) can lead to unauthorized actions on behalf of users, compromising data integrity, user accounts, and potentially causing financial losses, emphasizing the importance of anti-CSRF tokens and secure web application design to mitigate business risks.

10. **SANS Category:- CWE-22**: **Directory Traversal**
Description:-

Directory traversal or file path traversal is a web security vulnerability that allows an attacker to read arbitrary files on the server that is currently running an application.

Business Impact:-

Directory Traversal (CWE-22) can result in unauthorized access to sensitive files, compromising data confidentiality, and potentially leading to data breaches, emphasizing the need for input validation and secure file access controls to prevent business-critical information exposure.

11. **SANS Category:- CWE-78**: **OS Command Injection**
Description:-

It is about the improper sanitization of special elements that may lead to the modification of the intended OS command that is sent to a downstream component. An attacker can execute these malicious commands on a target operating system and can access an environment to which they were not supposed to read or modify.

Business Impact:-
OS Command Injection (CWE-78) can lead to unauthorized execution of arbitrary commands, compromising system integrity and potentially causing data breaches or service disruptions, highlighting the critical need for input validation and secure command execution practices to mitigate business risks.

12. SANS Category:- CWE-787: Out-of-bounds Write Error
Description:-

This happens when the application writes data past the end, or before the beginning of the designated buffer.

Business Impact:-

Out-of-bounds Write Error (CWE-787) can result in data corruption, system crashes, and potential security vulnerabilities, posing a risk of unauthorized access and service disruption, underscoring the importance of robust bounds checking to ensure business continuity and prevent malicious exploitation.

13. SANS Category:- CWE-287: Improper Authentication Error
Description:-

This is when an attacker claims to have a valid identity but the software failed to verify or proves that the claim is correct.A software validates a user's login information wrongly and as a result, an attacker could gain certain privileges within the application or disclose sensitive information that allows them to access sensitive data and execute arbitrary code.

Business Impact:-

Improper Authentication (CWE-287) can lead to unauthorized access, compromising sensitive data and system integrity, posing a risk of data breaches, reputational damage, and potential legal consequences, emphasizing the need for robust authentication measures to safeguard business assets.

14. SANS Category:- CWE-476: Dereferencing NULL Pointer
Description:-

Dereferencing a null pointer is when the application dereferences a pointer that was supposed to return a valid result instead returns NULL and this leads to a crash. Dereferencing a null pointer can happen through many flaws like race conditions and some programming error.

Business Impact:-

Dereferencing NULL Pointer (CWE-476) can result in application crashes, system instability, and potential security vulnerabilities, posing a risk of service disruption, data corruption, and unauthorized access, emphasizing the importance of rigorous error checking to ensure business continuity and prevent exploitation.

15. SANS Category:- CWE-732: Incorrect Permission Assignment
Description:-

This vulnerability happens when an application assigns permissions to a very important and critical resource in such a manner that exposed the resource to be accessed by a malicious user.

Business Impact:-

Incorrect Permission Assignment (CWE-732) can lead to unauthorized access, data breaches, and potential compromise of sensitive information, posing a risk of reputational damage, legal consequences, and business disruption, highlighting the need for proper permission controls to ensure data security.

16. SANS Category:- CWE-434: Unrestricted File Upload
Description:-

This vulnerability occurs when the application does not validate the file types before uploading files to the application. This vulnerability is language independent but usually occurs in applications written in ASP and PHP language.

Business Impact:-

Unrestricted File Upload (CWE-434) can result in malicious file execution, compromising system integrity and potentially leading to data breaches, reputational damage, and service disruption, emphasizing the importance of secure file upload controls to mitigate business risks.

17. SANS Category:- CWE-611: Information Exposure through XML Entities
Description:-

When an XML document is uploaded into an application for processing and this document contains XML entities with uniform resource identifier that resolves to another document in another location different from the intended location. This anomaly can make the application to attach incorrect documents into its output.

Business Impact:-

Information Exposure through XML Entities (CWE-611) can lead to unauthorized access to sensitive data, posing a risk of data breaches, reputational damage, and potential legal consequences, emphasizing the need for secure XML processing and input validation to safeguard business-critical information.

18. SANS Category:- CWE-94: Code Injection

Description:-

The existence of code syntax in the user's data increases the attacker's possibility to change the planned control behavior and execute arbitrary code. This vulnerability is referred to as "injection weaknesses" and this weakness could make a data control become user-controlled.

Business Impact:-

Code Injection (CWE-94) can result in the execution of arbitrary code, leading to unauthorized access, data breaches, and potential system compromise, posing a risk of reputational damage, financial losses, and legal consequences, highlighting the critical need for secure coding practices to mitigate business risks.

19. SANS Category:- CWE-798: Hard-coded Access Key

Description:-

This is when the password and access key is hard coded into the application directly for inbound authentication purpose and outbound communication to some external components and for encryption of internal data. Hard-coded login details usually cause vulnerability that paves the way for an attacker to bypass the authentication that has been configured by the software administrator.

Business Impact:-

Hard-coded Access Key (CWE-798) can lead to unauthorized access, compromise of sensitive information, and potential security breaches, posing a risk of reputational damage, legal consequences, and business disruption, emphasizing the importance of secure key management practices to protect business assets.

20. SANS Category:- CWE-400: Uncontrolled Resource Consumption

Description:-

This vulnerability happens when the application does not control the allocation properly and maintenance of a limited resource, this allows an attacker to be able to influence the amount of resources consumed, which will eventually lead to the exhaustion of available resources.Part of the limited resources includes memory, file system storage, database connection pool entries, and CPU.

Business Impact:-

Uncontrolled Resource Consumption (CWE-400) can result in system performance degradation, service disruptions, and potential denial-of-service attacks, posing a risk of business downtime, customer dissatisfaction, and financial losses, emphasizing the need for resource usage controls to maintain operational stability.