### **Intelligent Threat Detection And Response:**

### **AI Integration In Cybersecurity Frameworks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Collage** | **Mail\_id** | **Contact** |
| Sheeja Pon Chakravarthy | Coimbatore Institute of Technology | sheeja.cse@cit.edu.in | ☏8754237819 |

### **“SANS 20 - AI Based Threat”,** this is stage 1, where we understand various critical security controls. we took help from **OWASP top10 vulnerabilities** to understand them.

Prepared by, Verified by,

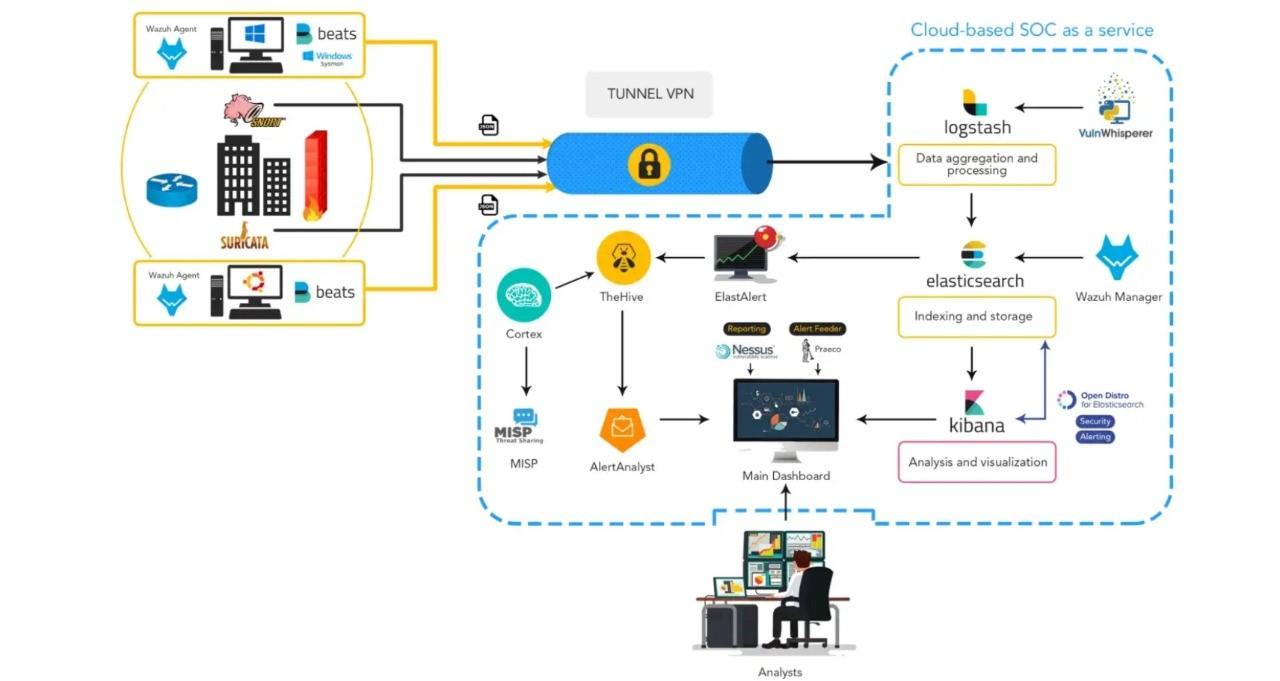
[Ms. SHEEJA PON CHAKRAVARTHY] [Mr. MANOJ]

**Overview:-**

The integration of artificial intelligence (AI) in cybersecurity frameworks has emerged as a transformative and crucial element in combating the ever-evolving landscape of cyber threats. Intelligent Threat Detection and Response, driven by the integration of artificial intelligence (AI) in cybersecurity frameworks, represents a paradigm shift in the way organizations safeguard their digital assets against sophisticated and dynamic threats. AI technologies, such as machine learning and advanced analytics, are at the forefront of this evolution, empowering cybersecurity frameworks to move beyond traditional rule-based methods.

Furthermore, the integration of AI enables intelligent automation in threat response. AI-driven cybersecurity frameworks can autonomously assess the severity of threats, prioritize alerts, and initiate predefined responses, reducing the response time and minimizing the impact of security incidents. Behavioral analytics, a subset of AI, aids in understanding the typical behavior of users and systems, enabling the identification of anomalies that may indicate malicious activities. As cyber threats become more sophisticated and diverse, the adaptability and continuous learning capabilities of AI contribute to a more dynamic defense posture.

A SOC, or Security Operations Center, is a centralized unit within an organization responsible for monitoring, detecting, and responding to security incidents. It is the primary point of contact for security-related issues and typically includes a team of security analysts, incident responders, and other security personnel who work together to protect the organization's assets and data. SOCs may also be responsible for managing security technologies, such as firewalls, intrusion detection systems, and security information and event management (SIEM) systems, as well as developing and implementing security policies and procedures.

****

### **SANS 20 - AI Based Threat**

* **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
* **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
* **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
* **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
* **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
* **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
* **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
* **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
* **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn’t well represented in the CVE/CVSS data.
* **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it’s not illustrated in the data at this time

**List of Vulnerability Table**

|  |  |  |
| --- | --- | --- |
| **S.no** | **Vulnerability Name** | **CWE – No** |
| **1** | **A01:2021-Broken Access Control** | CWE-284 |
| **2** | **A02:2021-Cryptographic Failures** | CWE-327 |
| **3** | **A03:2021-Injection** | CWE-89 |
| **4** | **A04:2021-Insecure Design** | CWE-657 |
| **5** | **A05:2021-Security Misconfiguration** | CWE-520 |
| **6** | **A06:2021-Vulnerable and Outdated Components** | CWE-1104 |
| **7** | **A07:2021-Identification and Authentication Failures** | CWE-290 |
| **8** | **A08:2021-Software and Data Integrity Failures** | CWE-353 |
| **9** | **A09:2021-Security Logging and Monitoring Failures** | CWE-117 |
| **10** | **A10:2021- Server-Side Request Forgery** | CWE-918 |

**Vulnerability Name: - Broken Access Control**

## **CWE: - CWE-284**

**OWASP/SANS Category: - A01:2021**

**Description: -** The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

**Business Impact: -** CWE-284, categorized as "Improper Access Control (IAC)," can have significant business impacts as it introduces vulnerabilities related to inadequate access control measures. This weakness may allow unauthorized users to exploit system functionalities, leading to unauthorized access to sensitive information, unauthorized modifications, and potential data breaches. The business consequences may include compromised data integrity, regulatory non-compliance, reputational damage, and financial losses associated with remediation efforts and potential legal actions. Operational disruptions and a loss of customer trust further underscore the importance of implementing robust access controls and security measures to mitigate the potential risks associated with CWE-284, safeguarding the organization's overall security posture and business continuity.

**Vulnerability Name: - Cryptographic Failures**

## **CWE: - CWE-327**

**OWASP/SANS Category: - A02:2021**

**Description: -** The product uses a broken or risky cryptographic algorithm or protocol.

**Business Impact: -** CWE-327, centered around the "Use of a Broken or Risky Cryptographic Algorithm," can have severe business impacts by exposing sensitive information to vulnerabilities. The use of compromised cryptographic algorithms can lead to data breaches, unauthorized access, and the compromise of confidentiality and integrity. This weakness may result in reputational damage, eroding customer trust and loyalty. Non-compliance with regulatory standards mandating secure cryptographic practices can lead to legal consequences and financial penalties. Remediation efforts, including system updates and security patches, may cause operational disruptions and increased security costs. Overall, the business impact of CWE-327 extends to potential financial losses, competitive disadvantage, and a compromised position in the market due to a diminished reputation for secure practices. Proactive measures, such as staying informed about cryptographic vulnerabilities and implementing secure algorithms, are crucial to mitigate these risks effectively.

**Vulnerability Name: - Injection**

## **CWE: - CWE-89**

**OWASP/SANS Category: - A03:2021**

**Description: -** The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

**Business Impact: -** CWE-89, commonly known as "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')," carries substantial business impacts as it enables attackers to manipulate and exploit database queries. This vulnerability can lead to unauthorized access, data breaches, and exposure of sensitive information, jeopardizing customer trust and triggering legal consequences. The compromise of data integrity through SQL injection attacks may result in financial losses, operational disruptions, and reputational damage. Non-compliance with regulatory standards, especially in industries with strict data protection requirements, can lead to legal actions and fines. The need for extensive remediation efforts, including patching and code reviews, adds to the associated costs. The overarching impact of CWE-89 encompasses compromised security, potential customer attrition, and a negative market perception, emphasizing the critical importance of implementing secure coding practices and robust input validation to mitigate these risks effectively.

**Vulnerability Name: - Insecure Design**

**CWE: - CWE-657**

**OWASP/SANS Category: - A04:2021**

**Description: -** The product violates well-established principles for secure design.

**Business Impact: -** CWE-657, focusing on "Violating Secure Design Principles," can have substantial business impacts by introducing vulnerabilities that compromise the foundational security of software systems. This weakness undermines the integrity and confidentiality of sensitive information, potentially leading to data breaches and unauthorized access. The violation of secure design principles may result in systemic weaknesses, allowing attackers to exploit vulnerabilities, causing reputational damage and eroding customer trust. The business consequences extend to regulatory non-compliance, as compromised security designs may violate industry and data protection standards, leading to legal repercussions and financial penalties. Addressing these vulnerabilities requires extensive remediation efforts, potentially causing operational disruptions and increased security costs. In essence, CWE-657 highlights the critical need for organizations to adhere to secure design principles to protect their assets, maintain customer confidence, and avoid the severe business ramifications associated with compromised system security.

**Vulnerability Name: - Security Misconfiguration**

**CWE: - CWE-520**

**OWASP/SANS Category: - A05:2021**

**Description: -** Allowing a .NET application to run at potentially escalated levels of access to the underlying operating and file systems can be dangerous and result in various forms of attacks.

**Business Impact: -** CWE-520, which pertains to ".NET Misconfiguration," can have significant business impacts by exposing vulnerabilities in the configuration of .NET applications. Such misconfigurations may allow unauthorized access, data breaches, and compromise the confidentiality and integrity of sensitive information. The exposure of internal resources and critical data due to misconfigured .NET applications can lead to reputational damage, eroding customer trust and potentially causing legal consequences. Non-compliance with regulatory standards, particularly those related to data protection, may result in financial penalties. Addressing the misconfigurations requires remediation efforts, potentially causing operational disruptions and increased security costs. The overall business impact of CWE-520 encompasses compromised security, regulatory non-compliance, reputational harm, and financial repercussions, underscoring the critical need for organizations to implement secure configuration practices in .NET applications to mitigate these risks effectively.

**Vulnerability Name: - Vulnerable and Outdated Components**

**CWE: - CWE-1104**

**OWASP/SANS Category: - A06:2021**

**Description: -** The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

**Business Impact: -** CWE-1104, highlighting the "Use of Unmaintained Third-Party Components," can have significant business impacts by introducing vulnerabilities associated with outdated or unsupported software elements. Relying on unmaintained third-party components may lead to security weaknesses, making systems susceptible to known exploits and vulnerabilities that have not been addressed. This can result in unauthorized access, data breaches, and compromised system integrity, potentially causing reputational damage and eroding customer trust. The overall business impact of CWE-1104 includes compromised security, potential legal liabilities, and reputational harm, underscoring the importance of diligent third-party component management to mitigate these risks effectively.

**Vulnerability Name: - Identification and Authentication Failures**

**CWE: - CWE-290**

**OWASP/SANS Category: - A07:2021**

**Description: -** This attack-focused weakness is caused by incorrectly implemented authentication schemes that are subject to spoofing attacks.

**Business Impact: -** CWE-290, centered around "Authentication Bypass by Spoofing," presents significant business impacts by enabling attackers to impersonate or spoof their identity, potentially leading to unauthorized access and exploitation of sensitive systems or data. Authentication bypass vulnerabilities may result in unauthorized users gaining entry to protected resources, compromising data integrity, and possibly leading to data breaches. The business consequences extend to reputational damage, as customers, partners, and stakeholders may lose trust in the organization's ability to secure access to its systems. This type of weakness can also result in regulatory non-compliance, leading to legal consequences and fines. Remediation efforts, including implementing stronger authentication mechanisms and conducting thorough security reviews, may incur operational disruptions and increased security costs. The overall impact of CWE-290 encompasses compromised security, potential legal liabilities, reputational harm, and financial repercussions, highlighting the critical need for robust authentication practices to effectively mitigate these risks.

**Vulnerability Name: - A08:2021-Software and Data Integrity Failures**

**CWE: - CWE-353**

**OWASP/SANS Category: - A08:2021**

**Description: -** The product uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum.

**Business Impact: -** CWE-353, focusing on "Missing Support for Integrity Check," introduces significant business impacts by leaving systems vulnerable to undetected alterations or tampering. Without proper support for integrity checks, malicious actors may exploit vulnerabilities to compromise the integrity of critical data or system components, leading to misinformation, unauthorized changes, and potential operational disruptions. This weakness can result in data breaches, unauthorized access, and the compromise of sensitive information, causing reputational damage and eroding customer trust. Non-compliance with regulatory standards that mandate integrity protection may result in legal consequences and financial penalties. Addressing this vulnerability necessitates implementing robust integrity checking mechanisms, potentially leading to increased security costs and operational disruptions during remediation efforts. In essence, CWE-353 underscores the importance of ensuring the integrity of data and systems to mitigate the risks associated with compromised security, regulatory non-compliance, reputational harm, and financial repercussions.

**Vulnerability Name: - Security Logging and Monitoring Failures**

## **CWE: - CWE-117**

**OWASP/SANS Category: - A09:2021**

**Description: -** The product does not neutralize or incorrectly neutralizes output that is written to logs.

**Business Impact: -** CWE-117, involving "Improper Output Neutralization for Logs," poses significant business impacts by creating vulnerabilities that allow attackers to manipulate log entries, potentially leading to misinformation, unauthorized access, and exploitation of sensitive data. If logs are not properly neutralized, attackers may inject malicious content into log files, compromising the integrity of recorded events and impeding the ability to accurately detect and respond to security incidents. This weakness can result in data breaches, reputational damage, and eroded customer trust. Non-compliance with regulatory standards that mandate secure logging practices may lead to legal consequences and financial penalties. Addressing CWE-117 requires implementing proper output neutralization techniques, potentially leading to increased security costs and operational disruptions during remediation efforts. In essence, CWE-117 highlights the importance of secure logging to mitigate the risks associated with compromised security, regulatory non-compliance, reputational harm, and financial repercussions.

**Vulnerability Name: - Server-Side Request Forgery**

**CWE: - CWE-918**

**OWASP/SANS Category: - A10:2021**

**Description: -** The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

**Business Impact: -** CWE-918, which involves "Server-Side Request Forgery (SSRF)," presents significant business impacts by allowing attackers to manipulate a web application into making unintended requests to internal resources or external systems. This vulnerability can lead to unauthorized access, data breaches, and potential exposure of sensitive information. Attackers may exploit SSRF to probe internal networks, facilitating reconnaissance for further attacks. The compromise of external systems or cloud services may result in financial losses, operational disruptions, and reputational damage. Non-compliance with data protection regulations and industry standards may lead to legal consequences and fines. Remediation efforts, including securing input validation and implementing proper network controls, may incur operational disruptions and increased security costs. The overall impact of CWE-918 encompasses compromised security, potential legal liabilities, reputational harm, and financial repercussions, emphasizing the critical need for robust security measures to effectively mitigate these risks.