

Práctica para el Parcial 2

Lea atentamente el siguiente texto y realice las actividades a continuación

Web Development Trends & Technologies to Follow in 2023

Machine learning in cybersecurity

"So where do I think AI will be in five to ten years? While the possibilities are endless, I believe the most consequential will be the secure application development". This is how Sridhar Muppidi, the Chief Technology Officer for IBM Security, assesses the prospects of AI.

Today, 100% of IBM security solutions use AI technology. IBM is not the only one to see AI as beneficial for security: Cisco, Microsoft, Siemens, McAfee, and many others are also actively using it.

This is not surprising, as the capabilities of AI technologies far exceed those of standard cybersecurity methods.

Firstly, AI tools can automate detection, response, and remediation processes that typically require human intervention when using traditional methods.

Secondly, traditional tools rely on signature-based detection methods, which can only detect and respond to known threats, whereas AI tools can assess and respond to unknown and complex threats using machine learning algorithms.

Another significant advantage of AI tools is their ability to analyze and predict potential security risks — an area where traditional methods are also inferior.

Here are some of the top AI solutions for web development:

- Managed detection and response (MDR) is a type of cybersecurity service that offers ongoing monitoring and threat detection, incident response, and remediation services for web security. MDR also provides comprehensive threat intelligence and analysis to help organizations understand the nature of threats and identify vulnerabilities in their web infrastructure.
- Cloud-based detection works by analyzing website traffic and data in real-time using advanced algorithms and machine-learning models hosted in the cloud. A cloud-based detection service compares website traffic against known attack patterns, identifies anomalies, and alerts owners or security teams of potential threats. This approach allows for quick and efficient threat detection without impacting website performance or requiring on-premises hardware or software.
- User and entity behaviour analytics can provide improved security, fraud detection, compliance, and operational efficiency as well as better business insights for websites. It analyzes user behaviour patterns to detect anomalies, personalize the user experience, and automate routine tasks while reducing the risk of cyber-attacks and potential financial losses.

Use it for your business


Leading market players have already implemented AI into their security systems. You can learn from how they have adopted this web development trend to achieve success with your website.

However, setting up an in-house team and developing AI cybersecurity solutions is time-consuming and

expensive. The most cost-effective and fastest way to provide advanced security to your project is to use ready-made tools.


Puntos: 10/10

✓ **Correcto** 1/1 Puntos

1. En el fragmento "While the possibilities are endless (...)", la palabra **possibilities** es un ejemplo de palabra con: 


- ☐ Sufijo
- ☐ Prefijo
- ☒ Sufijo y flexión
- ☐ Prefijo y flexión

✓ **Correcto** 1/1 Puntos

2. En el fragmento "Firstly, AI tools can automate detection, response, and remediation processes (...)", la palabra **tools** es un ejemplo de palabra con: 

- ☐ Sufijo
- ☐ Prefijo
- ☐ Sufijo y prefijo
- ☒ Ninguna de las opciones anteriores es correcta


✓ **Correcto** 1/1 Puntos

3. En el fragmento "This is not surprising, as the capabilities of AI technologies far exceed (...)", la palabra **surprising** es un ejemplo de flexion -ING de: 

- ☐ Sustantivo


- ☒ Adjetivo
- ☐ Verbo conjugado
- ☐ Verbo no conjugado

✓ **Correcto** 1/1 Puntos

4. En el fragmento "(...) a type of cybersecurity service that offers ongoing monitoring and threat detection (...)", la palabra **offers** es un sustantivo 


- ☐ Simple
- ☐ Derivado
- ☐ Compuesto
- ☒ No es un sustantivo

✓ **Correcto** 1/1 Puntos

5. En el fragment "Cloud-based detection works by analyzing website traffic and data (...)", la palabra **works** es un ejemplo de: 


- ☒ Verbo en presente simple
- ☐ Sustantivo plural
- ☐ Sustantivo singular
- ☐ Sustantivo en caso posesivo

✓ **Correcto** 1/1 Puntos

6. En el fragmento "(...) AI tools can assess and respond to unknown and complex threats using machine learning algorithms.", la palabra **threats** es un: 

- ☐ Verbo núcleo
- ☒ Sustantivo núcleo
- ☐ Sustantivo modificador
- ☐ Adjetivo

✓ **Correcto** 1/1 Puntos

7. Indique en cuál de los siguientes fragmentos puede encontrar un verbo copulativo y un adjetivo con función predicativa. 


- ☒ "(...) developing AI cybersecurity solutions is time-consuming and expensive."
- ☐ "(...) I believe the most consequential will be the secure application development".
- ☐ "Secondly, traditional tools rely on signature-based detection methods (...)"
- ☐ "Another significant advantage of AI tools is their ability to analyze and predict potential security risks (...)"

✓ **Correcto** 1/1 Puntos

8. Indique en cuál de los siguientes fragmentos puede encontrar un adverbio modificando a un verbo. 


- ☐ "(...) 100% of IBM security solutions use AI technology."
- ☐ "This is how Sridhar Muppidi, the Chief Technology Officer for IBM Security, assesses the prospects of AI."
- ☒ "(...) Cisco, Microsoft, Siemens, McAfee, and many others are also actively using it."
- ☐ "The most cost-effective and fastest way to provide advanced security to your project is to use ready-made tools."

✓ **Correcto** 1/1 Puntos

9. En "Another significant advantage of AI tools is their ability to analyze and predict potential security risks — an area where traditional methods are also inferior" encontramos los siguientes bloques nominales 

- ☐ Another significant advantage of AI tools /potential security / risks / an area / traditional methods / inferior"
- ☒ Another significant advantage /of AI tools / their ability / potential security risks / an area / traditional methods /
- ☐ "Another significant advantage /of AI tools/their ability / predict / potential security risks /an area / traditional / methods / inferior"

✓ **Correcto** 1/1 Puntos

10. En "A cloud-based detection service compares website traffic against known attack patterns, identifies anomalies, and alerts owners or security teams of potential threats" encontramos los siguientes bloques verbales 

- ☐ /service / compares / known / identifies / alerts /threats
- ☐ /compares / attack / identifies / alerts
- ☒ /compares /identifies / alerts

Conserve la información guardando su respuesta.

[Guardar mi respuesta](#)



Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial [Crear mi propio formulario](#)

