Chapter 14: Oversight & Operations

Governance

- **Governance** refers to the structures, systems, and practices an organization has in place to do the following:
  - **Assign** decision-making responsibilities, defining how decisions are to be made, and establishing the organization’s strategic direction
  - **Oversee** the delivery of its services; the implementation of its policies, plans, programs, and projects; and the monitoring and mitigation of risks
  - **Report** on performance toward achieving intended results and use performance information to drive ongoing improvements

Governance

Principle	Explanation
Accountability	The obligation of an individual, a group, or an organization to answer for a responsibility that has been conferred
Leadership	“Setting the tone,” which plays a crucial role in encouraging an organization’s personnel to embrace good governance practices
Integrity	Acting in a way that is impartial and ethical, reflected in part through compliance with legislation, regulations, and policies, as well as through the instilling of high standards of professionalism at all levels of an organization
Stewardship	The act of responsibly looking after resources on behalf of the organization and is demonstrated by maintaining or improving an organization’s capacity to serve the public interest over time
Transparency	Achieved when decisions and actions are open, meaning that stakeholders, including the public and employees, have access to full, accurate, and clear information on public matters

Governance

- Governance bodies can be either internal to the organization or external
  - Those that cover the immediate area are a **local/regional body**
  - Those that cover an entire nation are a **national body**
  - Those that are worldwide in scope are a **global body**
- In a **centralized** body, all authority is vested into a single group
- In a **decentralized** body, planning and decision making are distributed to smaller groups within it

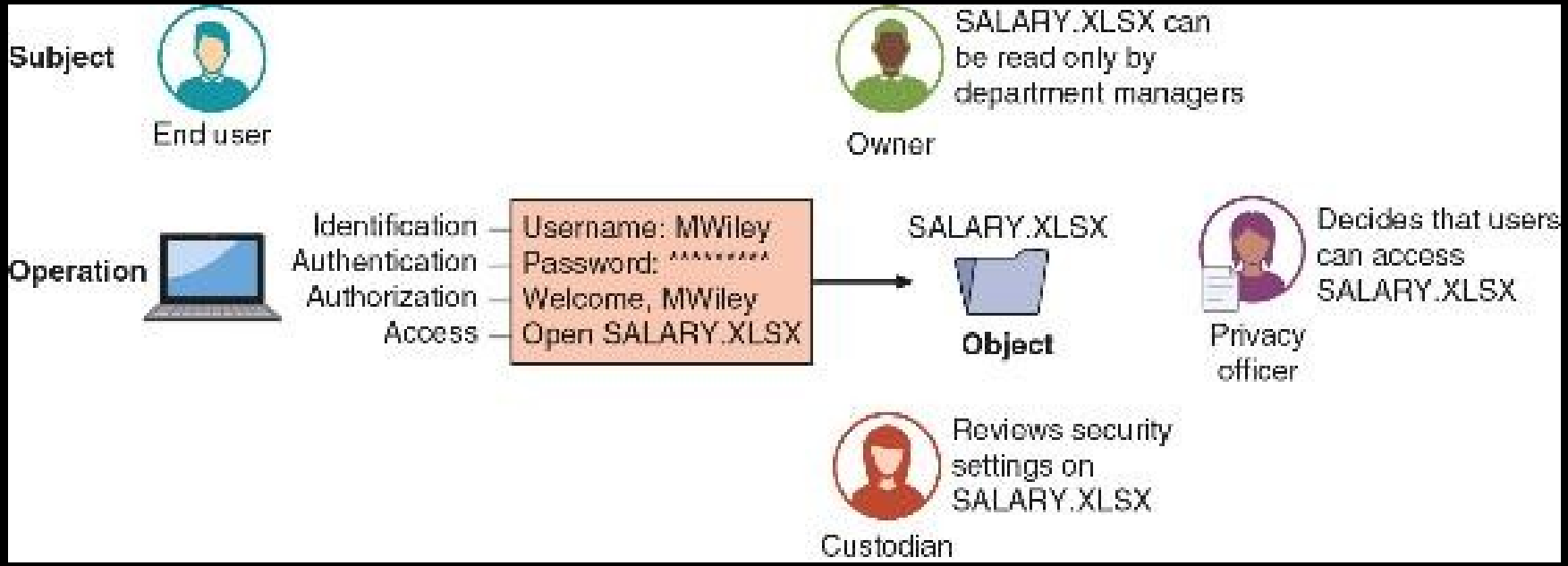
Governance

Name	Scope	Description
Board	Internal	Composed of internal directors who approve strategic organizational goals and policies
Committee	Internal	The board of governance committee is a subset of the board of directors that manages governance issues
Government entity	External	National governments direct organizations through governance directives
Regulatory	External	Regulatory agencies are responsible for distributing and enforcing government directives
Legal	Internal	Internal corporate legal departments interpret internal and external governance policies
Industry	External	Different industries create and audit governance policies for organizations that make up that industry

Governance

Role	Description	Duties	Example
Data privacy officer (DPO)	Manager who oversees the data privacy compliance and manages data risk	Ensures the enterprise complies with data privacy laws and its own privacy policies	Decides that users can have permission to access the file SALARY.XLSX
Custodian/ Steward	Individual to whom day-to-day actions have been assigned by owner	Periodically reviews security settings and maintains records of access by end-users	Sets and reviews security settings on SALARY.XLSX
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that the file SALARY.XLSX can be read only by department managers
Controller	Principal party for collecting the data	Acquire user's consent, store the data, and manage consent or revoking access	Gathers data for SALARY.XLSX and identifies where it is stored
Processor	Proxy who acts on behalf of data controller	Person or agency that hold and processes personal data for a third party but does not make decisions about using the data and is not responsible for the data	Manages the SALARY.XLSX file on behalf of data controller

System and Data Roles



Governance

- A **policy** is a formal statement that outlines specific requirements or rules that must be met based on a decision by a governing body
- An **acceptable-use policy** (**AUP**) defines the actions users may perform while accessing systems and networking equipment
- Other security policies include business continuity policies, disaster recovery policies, incident response policies, and a **software development lifecycle** (**SDLC**) **policy**

Governance

- A **procedure** provides detailed mandatory steps that a user needs to follow to comply with a policy
- An incident response **playbook** lists specific actions to take for threats
- An example of a procedure is employee **onboarding**, or the tasks associated with hiring a new employee
- Employee **offboarding** entails actions to be taken when an employee leaves an enterprise

Governance

- A **standard** specifies the uniform uses of specific technologies or settings for secure configurations
- An example of a standard is the **Payment Card Industry Data Security Standard (PCI DSS)**
  - Other examples include password standards, access control standards, physical security standards, and encryption standards
- A **guideline** provides general guidance and support for policies, standards, or procedures
  - It is voluntary while policies, standards, and procedures are mandatory

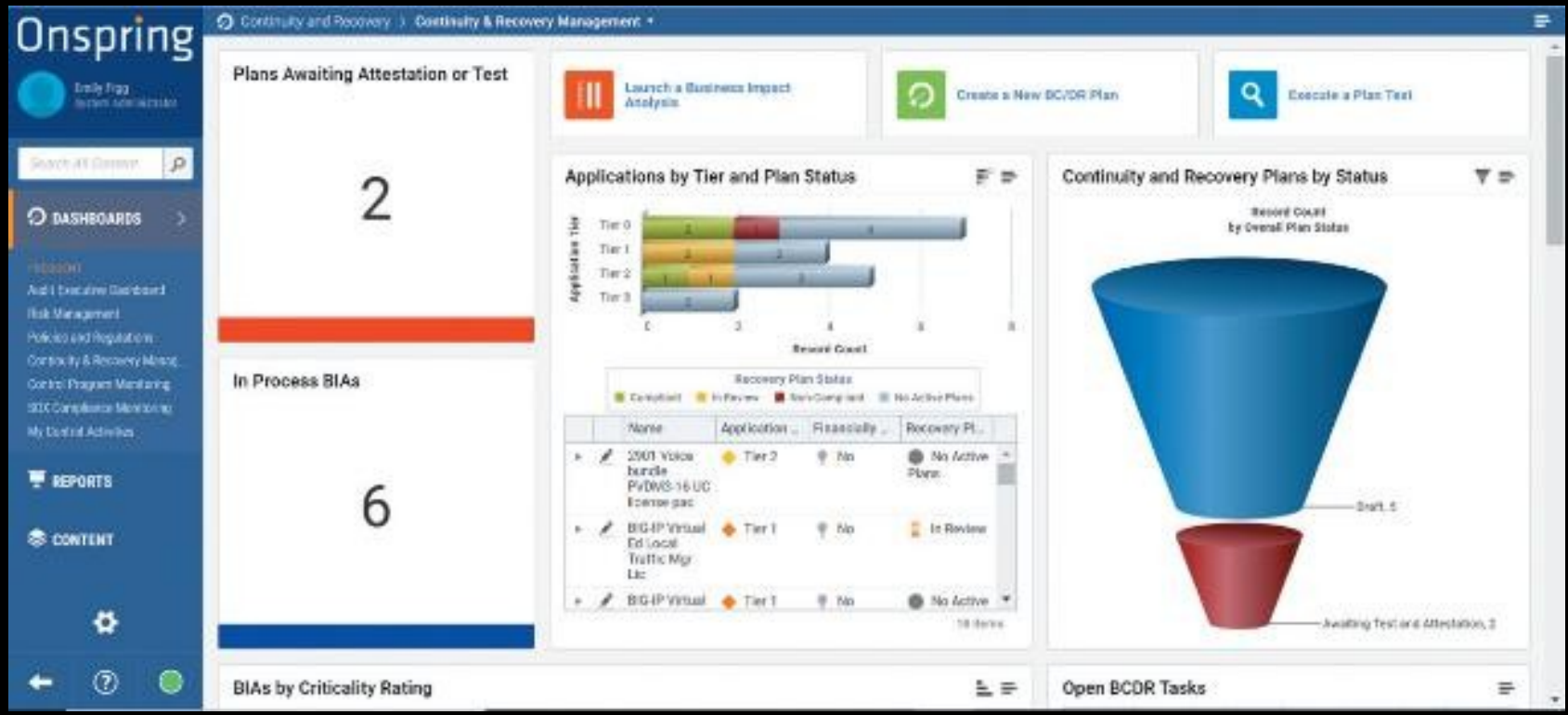
Compliance

- **Compliance** is the process of ensuring that an organization adheres to laws and regulations related to information security and user data privacy
- It relies on penalties for **noncompliance** or not following compliance standards
  - Penalties includes fines, sanctions, reputational damage, loss of license, or contractual impacts

Compliance

- **Compliance monitoring** refers to the quality assurance tests that organizations perform to determine how well their business operations meet security regulations and standards
  - It involves having a process to verify conformity and generating appropriate analysis
- Compliance monitoring can be performed by the organization itself (**internal compliance monitoring**)
- **Automation compliance tools** can generate an **internal compliance report** that can be provided to an auditor that verifies compliance

Automation Compliance Tool



Compliance

- Compliance monitoring can also be performed by a professional third party (**external compliance monitoring and reporting**)
- An external compliance report can serve as an official **attestation** of compliance monitoring
- Reports typically require a statement of the **acknowledgement** of the organization’s responsibility for establishing and maintaining effective internal controls as they relate to compliance

Compliance

- There are two types of data collections of user private data that occur:
  - An overt and legitimate gathering of this data by an organization
  - A concealed and questionable collection of user data
- Many organizations today take advantage of the fact that every time a user interacts with technology, they leave behind a “data trail”
- Data is predominantly collected by using tracking features (trackers) that are embedded in virtually every app on a smartphone

Compliance

- Different legal protections are in place to protect data privacy
- Currently there are no universal protections (**global data protections**) to which all nations adhere
  - There are protections that apply to a country (**national data protections**)
- In the US, ownership or legal possession and control of data has not been firmly established
  - U.S. data protections primarily are those established as industry regulations that an organization follows to be in compliance

Security Operations

- Information security defenders make up the **security operations center (SOC)**
- Members of a SOC team are responsible for multiple tasks, including proactive monitoring, incident response and recovery, remediation activities, compliance, and coordination
- Tools used by a SOC include:
  - Automation, orchestration, threat hunting, and artificial intelligence

Automation

- Information security has traditionally been more manual than automated for many years
- In recent years, a shift has occurred in which more automation is becoming available to security personnel
- This helps to streamline and speed up security processes to provide needed insights in a timely fashion

Benefits of Automation

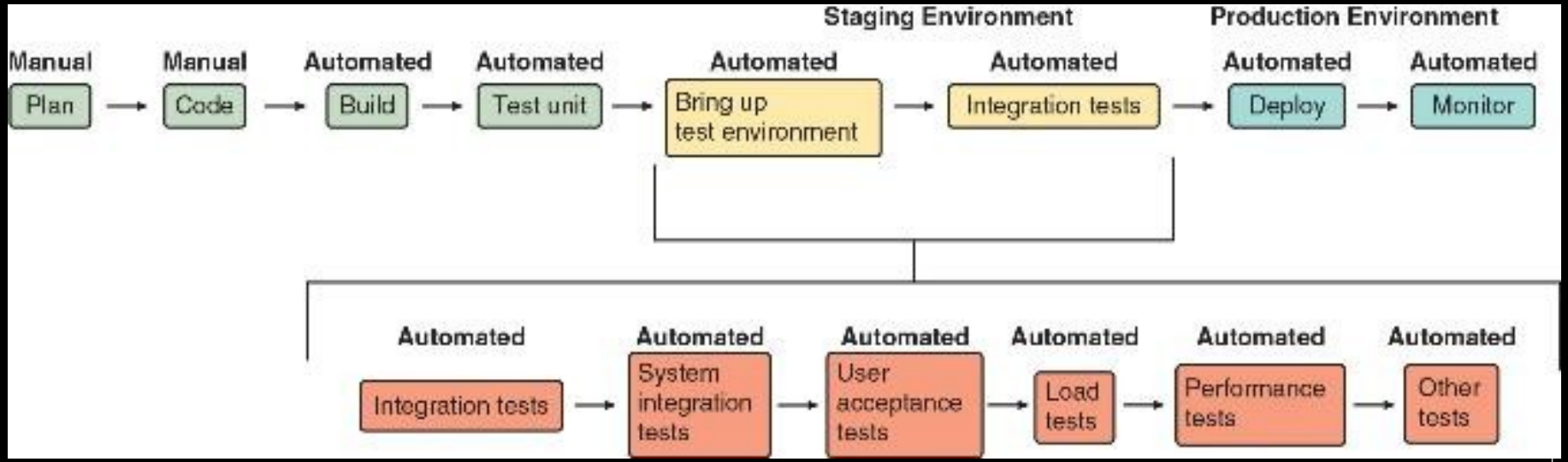
Benefit	Explanation
Produce time efficiency	Automation can improve productivity by reducing the needed time to complete a task
Enforce baselines	Security automation can ensure that required baselines are imposed
Distribute standard infrastructure configurations	Unlike a technician who can easily miss a configuration setting when performing a task manually, automation can distribute infrastructure configurations to all devices
Securely scale	Adding additional appliances to scale operations can be performed more securely through automation
Improve staff retention	Due to the laborious nature of sifting through massive amounts of data, security automation can reduce the stress and “burnout” fatigue of workers and improve retention
Reduce reaction time	Automation can dramatically decrease the time needed to react to an attack
Generate workforce multiplier	Security automation gives staff the ability to be more productive

Use Cases for Security Automation

- Security automation can be used to enhance software development to create more secure code
  - Implementing an automated process can not only produce code more quickly, but the code will be more secure
- **Application programming interfaces (APIs)** is a link provided by an operating system (OS), web browser, or other platform that allows a developer access to resources at a high level
  - Use of APIs has led to what is called **integration platform as a service (IPaaS)**

Use Cases for Security Automation

- Continuous integration, continuous deployment, and continuous development



Use Cases for Security Automation

- A script (snippet of code) is ideal for automation
  - They often have features not found in formal programming languages
  - These features include simple mechanisms for invoking other programs, less strict language requirements, and no requirement to declare variables
- Security **guardrails** are “automations” that constantly watch cloud deployments, find deviations from desired baselines, and automatically remediate issues

Use Cases for Security Automation

- **Provisioning** is the process of creating and setting up an IT infrastructure
  - It includes the steps required to manage user and system access to various resources
- **Automated provisioning** automatically grants and manages users' access to the systems, applications, and resources of an organization
  - Grants access based on employee positions and permission levels
  - Can provision for individuals (**user automation provisioning**) or system (**resource automation provisioning**)

Use Cases for Security Automation

- In cloud computing, automated **security groups** function like a virtual firewall that allows control over all inbound and outbound traffic to a particular cloud resource
- Security groups are associated with network interfaces so that any changes are reflected immediately and automatically once the configuration is completed
  - It can quickly deny ingress traffic from threat actors (**disabling services and access**)

Use Cases for Security Automation

- The following are additional use cases for security automation:
  - **Escalation –** Information security automation allows for the rapid detection of threat incident so that its importance can immediately be elevated
  - **Continuous integration and testing –** Automation can help security personnel perform continuous integration and testing
  - **Ticket creation –** A **ticket** is a special document or record that represents an incident, alert, request, or event that requires action
    - Ticket creation can be automated

Orchestration

- **Security orchestration** involves the automation and combination of many different individual tasks and processes
  - This coordination involves hardware, software, middleware, and services
- **Security orchestration, automation, and response (SOAR)** platform is a combination of software programs and tools that allow organization to synthesize and automate a range of security operations, threat intelligence, and incident response in a single platform

SOAR Dashboard

Threat Hunting

- **Threat hunting** is an emergent activity that combines a proactive, repetitive (iterative), and predominantly human identification of a cyber invasion to an IT network or endpoints
- Threat hunting assumes that the network is already infected, and attackers are not trying to enter form the outside but are currently inside

Threat Hunting

Title	Role	Goal	Task	Driving force	Timeframe
Incident responder	Reactive	Secure environment after alarm has been raised	Minimize impact of attack on the organization through formal process	Business continuity	Immediate
Penetration tester	Proactive	Secure environment through controlled offensive exercises	Mimic actions of threat actors to test and validate security posture	Uncover vulnerabilities	Soon
Threat hunter	Proactive	Identify suspicious activity before alarm has been raised	Seek evidence of malicious behavior	Prevent infection from spreading	Longer

Levels of Threat Hunting

Threat-hunting level	People	Processes	Tools
Initial (Level 1)	Existing SOC personnel	Ad-hoc hunts with little data collected	Standard SOC reactive tools with little automation
Managed (Level 2)	Threat hunting performed by volunteer	Uses basic threat feeds with indicators of compromise; hunts only occasionally	Searching for text strings and automatic matching of IoC
Defined (Level 3)	Dedicated threat hunter	Formal hunting process that occurs regularly with data collection from key areas	Uses statistical analysis techniques
Quantitatively Managed (Level 4)	SOC analysts rotated into threat hunting team	Hunts occur frequently with moderate data collection	Use of dashboards and visualization tools
Optimized (Level 5)	Threat-hunting teams integrated across a SOC with proper resources integration into process	Hunts occur continuously and data shared across security community	Takes advantage of machine learning

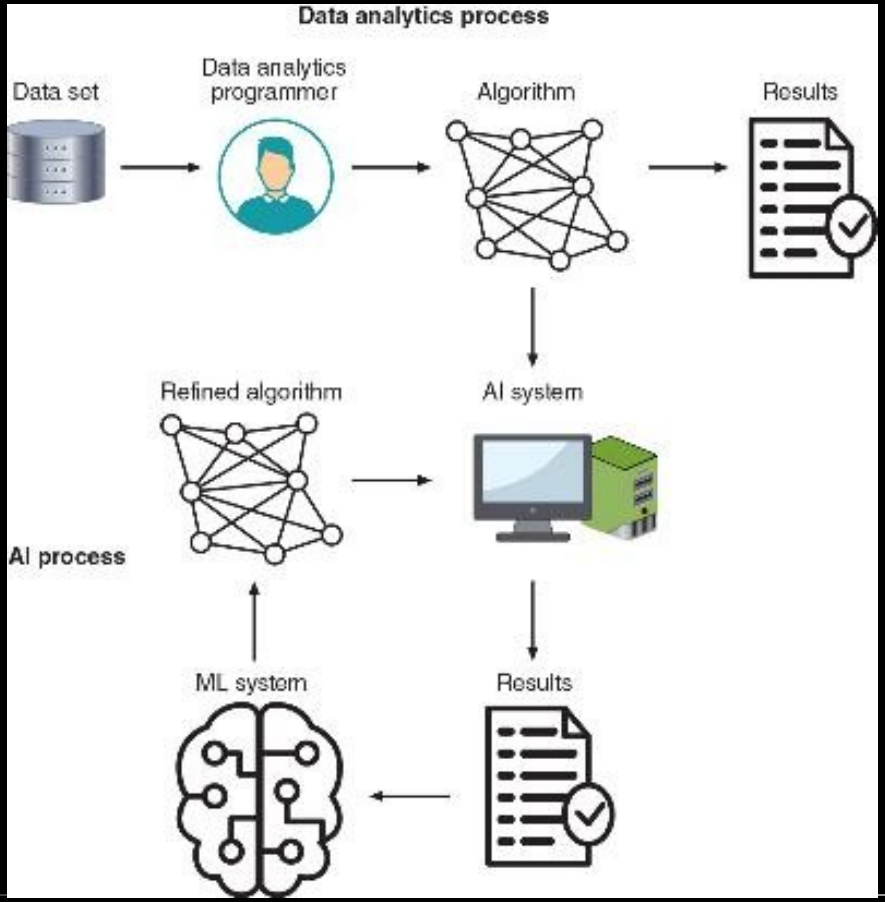
Threat Hunting Process & Tactics

- The following are the steps in the process of threat hunting:
  - Select the attack model
  - Identify the most concerning threats
  - Create a calendar
  - Generate a hypothesis
  - Investigate the hypothesis
  - Act on results

Artificial Intelligence

- **Data analytics** is a fixed process that examines large data sets to draw conclusions about the information they contain
- A subset of data analytics is **artificial intelligence (AI)**
  - Data analytics creates algorithms designed to learn patterns and correlations from data, which AI can then use to create predictive models
- **Machine learning (ML)** is a subset of AI that uses statistical techniques to give computer systems the ability to “learn” or progressively improve their performance using data

Data Analytics, AI, and ML



Artificial Intelligence

- The following are three types of AI systems:
  - **Assisted intelligence –** Improves what people and organizations are already doing
  - **Augmented intelligence** – Enable people and organizations to do things they could not have done otherwise
  - **Autonomous intelligence** – Features machines that act entirely on their own (self-driving vehicles)

Artificial Intelligence

- The birth of AI can be traced back to the beginning of digital computers
- AI exploded onto the scene with the release of ChatGPT in November 2022
- Microsoft is now infusing its popular workplace software, Microsoft 365, with the technology behind ChatGPT, called Microsoft 365 Copilot

Artificial Intelligence

- Organizations face many challenges relating to information security, such as:
  - Hundreds, thousands, or hundreds of thousands of endpoint devices per organization
  - Large numbers of daily vulnerabilities including unknown zero-day vulnerabilities
  - Massive amounts of security-related data that is generated hourly
  - A serious shortage of trained security personnel

Artificial Intelligence

- The following are risks associated with using AI in security:
  - AI needs huge volumes of high-quality data to function accurately
  - AI tends to generate too many false positives
  - It can be hard to “tune” an AI system for the specific needs of individual customers
  - There is a lack of transparency in how AI systems make decisions
  - The algorithmic models can degrade over time if they are not properly maintained by data analytics experts

Artificial Intelligence

- Threat actors can attack AI systems and take advantage of AI
- This is called adversarial artificial intelligence and includes the following:
  - **Compromise the algorithm**
  - **Taint ML training data**
  - **Use AI maliciously**