Microsoft 365 Security, Compliance, and Identity Concepts

by Vlad Catrinescu

With your data in the cloud, it’s important that you configure the right security settings to protect it. This course will teach you the different security, compliance, and identity solutions for Microsoft 365.

Course Overview

Course Overview

Hello everyone. My name is Vlad Catrinescu, and welcome to my course, Microsoft 365 Security, Compliance, and Identity Concepts. I'm a Microsoft MVP from Montreal, Canada. As more users work from home, coffee shops, and many other places outside the corporate network, security has become an even bigger concern for many organizations. Even with all of your workloads in a cloud environment, such as Microsoft 365, you are still responsible for many security and compliance configurations. In this course, you will learn the basic concepts around Microsoft 365 security, compliance, and identity. Some of the major topics that we will cover include security concepts and methodologies for Microsoft 365, identity and access management solutions for Microsoft 365, threat protection solutions for Microsoft 365, as well as compliant solutions for Microsoft 365. By the end of this course, you'll understand what you are responsible of securing in the Microsoft Cloud, as well as have an overall view of the different security, compliance, and identity products available to secure Microsoft 365. Before beginning this course, you should be familiar with what Microsoft 365 is and the services inside. I hope you'll join me on this journey to learn how to secure Microsoft 365 with the Microsoft 365 Security, Compliance, and Identity Concepts course at Pluralsight.

Security Concepts and Methodologies for Microsoft 365

Module Introduction

Hello, and welcome to this Microsoft 365 Security, Compliance, and Identity Concepts course. My name is Vlad Catrinescu, and I'll be your instructor for this course. I'm a Microsoft MVP from Montreal, Canada, and you can find me on Twitter @vladcatrinescu or follow my blog at VladTalksTech.com. In this first module, we will learn some of the fundamental security concepts and methodologies for Microsoft 365. We will start this module by one of the most fundamental concepts of security in the cloud, which is the shared-responsibility model, or as I like to call it, the who secures what. Afterwards, we will cover some common security threats that we need to defend ourselves from, even if our services are in the cloud. And finally, we will learn about the Zero Trust methodology. By the end of this module, you'll understand some of the most important fundamental concepts of security in the cloud.

Microsoft Product Name Updates

Hello there. My name is Vlad Catrinescu, and in our goal to keep this course up to date, I wanted to share with you a few quick updates that Microsoft did to their product names. First of all, Yammer is now called Microsoft Viva Engage. It still has the same features, purpose, and goal inside Microsoft 365, but instead of only part of Yammer being called Viva Engage, the Yammer branding is going away and all the product will now be called Microsoft Viva Engage. Our next product rename is that Azure Active Directory is now called Microsoft Entra ID. Azure AD has been part of the Microsoft Entra suite for a while now, and the new name fully confirms the position in the suite. But don't worry, the admin center and settings did not change. Our last rename is that Microsoft 365 Defender is now called Microsoft Defender XDR. Only the name of the suite has changed and not the name of the products inside. So for example, inside Microsoft Defender XDR, we still have Microsoft Defender for Office 365, Microsoft Defender for Endpoints, and so on. The product name changes we just talked about have no impact on the features that you will learn about in this course. The impact is really from a marketing point of view, but the features are the same. Many internal resources that you might consume, such as maybe training, old project documentation, or blog posts that you see on the web might still reference the old product names, but just again so you are sure, the features did not change. Microsoft simply rebranded the products. This is it for this quick course update on the product renames, and I hope you enjoy the course.

The Shared Responsability Model

Let's start by talking about the shared responsibility model, or who secures what in a cloud environment. If we take a step back and look at cloud computing in general, there are multiple types of computing services. The three main ones are Infrastructure as a Service, Platform as a Service, and Software as a Service. What really differs between those deployment models is how much you manage versus how much the cloud vendor manages. Let's start with on-premises where it's pretty easy. You're the one that manages everything from storage, to the data center, to networking, virtualization, and applications on top of it. Infrastructure as a Service delivers cloud-computing infrastructure to organizations including things such as servers, networks, and storage through virtualization technology. You, as the client, still manage the operating system, the applications, the data, and all of that. Platform as a Service provides cloud components to certain software while being used mainly for applications. Platform as a Service provides a framework for developers that they can build upon to create customized applications. All of the servers, storage, and networking is managed by the cloud provider, while the developer can maintain management of the applications and data on top of it. Our last option is Software as a Service in which you simply enjoy the service, pay a fee, but you don't really manage anything at all. Everything is managed by the vendor. A majority of Software as a Service applications run directly through web browsers and don't even require any downloads or installations from the client. Something to also be aware of is while we separate the workloads into different service types, most organizations will actually use products from each service type. For example, your organization might be using Azure Virtual Machines and Azure storage, which would be in Infrastructure as a Service. You're also probably using Azure Logic

Apps, Azure Functions, Azure Web Apps, or Azure Automation, which are Platform as a Service solutions. And if your company also uses productivity solutions such as SharePoint Online, OneDrive for Business, Microsoft Teams, you're also leveraging Software as a Service solutions, all while in the Microsoft Cloud. Now, why is this important for security? Security in the cloud is a partnership between the cloud provider and you. At a high level, the cloud provider operates and secures the base infrastructure, and most of the time, the host operating system layers. While you control and secure identities, as well as additional application settings, for example, turning on multi-factor authentication or turning it off, this is not a set-in-stone list. Really, the responsibility highly depends on the service type that you have hosted. For example, in Infrastructure as a Service, the customer has more responsibilities than in Software as a Service. So let's take a look at who secures what in the cloud, based again on the three cloud service types that we talked about. This is, again, also called the shared responsibility model. Let's start with on-premises, which is the easiest one because basically, on-premises, the customer is responsible for securing everything, from the physical data center, to the network, hosts, applications, all the way to the information and data. If we move onto Infrastructure as a Service, the cloud provider now takes care of the physical data center, the physical network and host; however, everything over it such as the operating system, applications, accounts, and identities, falls under your responsibility as a client. Moving onto Platform as a Service, the customer has less things to worry about, and some of them, as you can see, are even a split responsibility. Remember that Platform as a Service allows customers to put their own code on the platform run by the provider. So for the application part, it's split if the code that you add on there contains vulnerabilities, will it's your responsibility, the customer's responsibility, not the cloud provider. Different things such as accounts and identities, devices and information, and data are still the responsibility of the customer. Lastly, Software as a Service, where the cloud provider hosts and is therefore responsible for most security settings. Even in this service type, security will always be a partnership, and the customer is responsible for accounts and identities, devices, and data governance, and information, as well as the data. As you can see, even if from a hosting perspective earlier, Software as a Service was the one where the cloud provider hosted everything. From a security perspective, it's still a partnership. To give you an example, if an employee gets their device stolen and it doesn't have a password, and then the person that steals the device, while they have access to the data, that is your responsibility, not the cloud provider's. Same thing if somebody clicks a ransomware link and accidentally gives their password away to a bad actor, it's not the cloud provider's responsibility that the user got hacked and sensitive data was accessed; it's your responsibility. Of course, cloud providers will offer you multiple ways to help you secure your cloud workloads such as multi-factor authentication, but it's your responsibility to turn those features on for your users. If there's something important to remember it's that it's really your duty to understand and know what are your security responsibilities for each type of product and workload that you leverage in the cloud. The shared responsibility model is your guide to who secures what, but never forget that some things will always be your own responsibility.

Common Security Threats

Now that we have learned about the shared-responsibility model, let's talk about common security tricks that we want to defend ourselves from. There are many types of security tricks out there. Some aim to steal data, some aim to extort money, and others to disrupt normal operations. In this course, we will focus really on the six main ones, but this is in no way a full list. Let's start talking about data breaches. A data breach is when data is stolen, and this can include either proprietary data, trade secrets, or also the ones that often make the news, which is personal data. When we talk about personal data, we talk about any information related to an individual that can be used to identify them directly or indirectly. If personal data is stolen, this can also result in identity attacks, such as phishing, or spear phishing, or even the famous tech support scams that I'm sure a lot of you have heard about or even experienced yourself. Next up, let's talk about dictionary attacks. A dictionary attack, also often called a brute-force attack, is a common identity attack where a hacker attempts to steal an identity by trying a large number of known passwords. Each password is automatically tested against a known username. Another common identity attack is the password spray. Most password spray attacks submit a small number of the known weakest passwords against each of the accounts in an enterprise. This technique allows the attacker to quickly search for an easily-compromised account and avoid potential detection thresholds. Unlike a brute-force attack, where you can really try and submit thousands of combinations, attackers know that most enterprises will lock your account after, let's say, five failed attempts. So password spray is really about trying the most common passwords, maybe one or two per account, but on a large number of accounts, and trying to find the easiest way in. Next up is ransomware, which is part of the malware family. Ransomware is a type of malware that encrypts files and folders, preventing access to important files. Ransomware attempts to extort money from the victims, usually in the form of cryptocurrencies, in exchange for the decryption key. Our next common security threat is disruptive attacks, or you might also have heard about the term distributed denial-of-service, or DDoS attack. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. Next up, we have worms. A worm is a type of malware that can copy itself and often spreads through a network by exploiting security vulnerabilities. It can spread through email attachments, text messages, filesharing programs, social-networking sites, network shares, removable drives, and software vulnerabilities. The last one, which we will talk about, is coin miners or crypto jacking. This is a fairly new form of malware that either installs software or runs directly in the browser of an affected computer to use the computer's resources and power to mine for cryptocurrency. Most affected computers only notice a decrease in performance, so it can take a while until the user notices their PC has been infected.

Zero Trust Methodology

Now that we know the threats out there, let's talk about the Zero Trust methodology. The Zero Trust methodology, or simply Zero Trust, is a cybersecurity model with a very simple premise, eliminate the concept of trust from your network. But what exactly does that mean? To better understand what this means, let's take a look at a traditional network design at a high level. First of all, I will really split this up into corporate resources, internet, and then the DMZ part of your network where certain client-facing resources might be stored. The way that networks have been designed before is that everything that was inside your corporate perimeter or internal was trusted. The internet was untrusted, and the DMZ is where you would have a lot of different rules on what has access to what. But the big problem was that always, by default, once something was inside your corporate network, it was trusted and it was free to move laterally. That might have worked a long time ago, but with today's modern workforce, the corporate perimeter has changed. We now have things such as cloud technology, which is accessed from the internet from anywhere in the world, and with all sorts of devices, as people now don't only work from desktop PCs, they work from tablets, laptops, smartphones, from anywhere in the world, really, whether it's in a train, a plane, or a hotel, something else that has changed is that the bad actors and threats have also evolved so we cannot rely on that trusted corporate perimeter anymore. Now that we have seen a bit more, let's take a look at the definition from the National Institute of Standards and Technology, which has a standard for Zero Trust. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely under physical or network location, or based on an asset ownership. So, is the device personally owned or an enterprise device? it doesn't mean that if it's a company laptop we will trust it automatically. Zero Trust follows three guiding principles. The first one is verify explicitly, the second one is least-privileged access, and the third one is assume breach. Let's take a look at them in detail. The first one is verify explicitly, which advises to always authenticate and authorize based on the available data points including user identity, location, device, service, or workload, data classification, and anomalies. This means that we will not only accept the user's authentication as a token of trust, but we will verify all of the other signals mentioned and what the user is allowed or authorized to do, depending on them. If you see that a user is logged in from, let's say, Canada, and then one hour later the same user is logged in from Germany, it should trigger an anomaly in your system, and then you need to make a decision if you still allow the user to do what they request or not. The next one is least privileged access. In a Zero Trust model, we should limit user access with just-in-time and just-enough access, which you will often see abbreviated as in the slides. This means that a user should not simply always have administrator permissions on everything all the time, as that can be a security risk. Instead, when the user needs to do something with an elevated permission, they can request it, and it can be approved based on risk-based adaptive policies that evaluate the signals that you have. Those elevated permissions should be just enough for what the user needs to do and should be only for the time that the user needs to do the task, not forever. By implementing just-in-time and just-enough-access, you can really protect both data and productivity. The last one, but not the least, is assume breach, and this one is important, as it really frames the whole mindset with which you should approach your security. By doing so, you reduce the attack surface and prevent lateral movement by segmenting your network, users, and devices when threats are detected. You should ensure that all the sessions are encrypted, and you should use analytics to get visibility of threats and improve threat detection. The last one is important, as even once somebody is authenticated, you must keep monitoring them and see what do, and if any threats are detected, assume breach and take corrective action. In a Zero Trust model, we need all the elements to work together to provide an end-to-end security. When we talk about elements, we talk about six elements that are, again, foundational pillars of the Zero Trust model. The first one is identities. Identities might be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication and follow least-privilege access principles. Second is devices. Devices create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is a very important part of security. Third is applications. Applications are the way that data is consumed, and this includes discovering old applications being used, sometimes called shadow IT because not all applications are managed centrally. This pillar also includes permissions and access. Fourth is data. Data should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data and ensuring that it remains safe when it leaves devices, applications, infrastructure, and networks that organization controls. Fifth is infrastructure. Your infrastructure, whether on-premises or cloud-based, represents a threat vector. To improve security, you must assess for version, configuration, and just-in-time access, and use telemetry to detect attacks and anomalies. This allows you to automatically block or flag risky behavior and take protective actions. Sixth is networks. Networks should be segmented, including deeper in-network microsegmentation, real-time threat protection, end-to-end encryption, monitoring, and analytics.

Module Conclusion

To finish off this module, let's review what we have learned. We have first done an overview of the types of cloud-computing services, and afterwards we have looked at the shared responsibility model, or who secures what in the cloud. Depending on the service type, the responsibilities are split differently, and super important to remember, some responsibilities are always retained by the customer, such as information and data, devices, as well as accounts and identities. Next up, we have learned the most common security threats in the cloud that we need to defend ourselves from. And finally, we have learned about Zero Trust, a cybersecurity model with a very simple premise, eliminate the concept of trust from your network. Zero Trust follows three guiding principles. First one is verify explicitly, second one is least-privileged access, and the third is assume breach. We have looked at each one of those three in detail. This is it for this module, which was all about concepts. In the next modules of this course, we will start diving into the more specific products that actually help us achieve Zero Trust and protect from common threats, starting with the next module on Identity and Access Management Solutions for Microsoft 365.

Identity and Access Management Solutions for Microsoft 365

Module Introduction

Hello, and welcome to this Microsoft 365 Security, Compliance, and Identity Concepts course. My name is Vlad Catrinescu, and I'll be your instructor for this course. In this module, we will learn about the identity and access management solutions for Microsoft 365. We will start this module by covering some identity concepts, such as authentication and authorization, as well as what modern authentication is in the Microsoft world, and also learn about the role of the identity provider. We will then talk about Microsoft's Active Directory, and, of course, Azure Active Directory as well, and even learn what a hybrid identity is. Next up, we will learn about the different Azure Active Directory authentication methods and learn about the value of implementing things such as multi-factor authentication and passwordless. And finally, we will learn about conditional access, a very important tool towards our goal of implementing Zero Trust inside our Microsoft 365 deployment. After listening to this module, you will understand the key products that help us provide identity services in Microsoft 365.

Identity Concepts

Let's start by learning some identity concepts for Microsoft 365, and we'll start by talking about authentication and authorization. While they might sound similar and sometimes a lot of nontechnical users interchange them, authentication and authorization are very distinct security processes in the world of identity and access management. In short, authentication is the act of validating that users are who they claim to be. Authorization in the system security is the process of giving the user permission to access a specific resource or function. Let's take a look in a bit more detail. Authentication is when you go to a website or application, and it asks you for your identification, which most of the time is a username and password. By the way, when you sign in in an application anywhere and you only need a username and password to log in, we call this single-factor authentication, as you only need to know one thing, the username and password in order to log in. The authentication process, really what it does is it validates that you are who you say you are, and if you're only using single-factor authentication, so username and password, you enter those and they match, authentication is confirmed. You are you because you knew those pieces of information. Authentication is always the first thing that is done, and it's really important to remember that authentication is always done before authorization. Now, after you are authenticated and the system knows that Vlad is signed in, now after you are authenticated and the system knows that, okay, Vlad is signed in and passed all of the required tests, we go to the authorization stage. Authorization is what determines what permissions you have. I might log in on a site and authorization process will determine, am I only allowed to view documents, or am I allowed to edit them? What permissions do I have on this application? So just to recap again, as this is a very important concept, and it will also come up on the exam if you decide to get certified, authentication is done first, and it's confirming users are who they say they are. Authorization is done afterwards and checks if a user is allowed to access a certain resource. Now let's talk about the concept of modern authentication. Modern authentication is a Microsoft umbrella term for authentication and authorization methods between client and server. I really want to emphasize that this is mostly a Microsoft term, rather than an industry methodology like Zero Trust, for example. To better understand modern authentication, let's take a step back and look at what we did before modern authentication. When accessing a resource, you usually have a client and a server, and when you wanted to access, you needed to provide your username and password to the server. If you had multiple servers, you would need to log in to each one of them. You could even have multiple usernames and passwords in each one, and each server would also need to know each username and password. This is not only a bad user experience, but it can be less secure. Now, let's talk about modern authentication. In a modern authentication scenario, we add a new component to our diagram, which is the identity provider. When a user signs in, they will send their authentication information to the identity provider, which can be, of course, a username and password. It could be a smart card, or however it's configured. The identity provider will return a token back, and when the client wants to authenticate to a resource, it can send over that token. Since the server has a trust relationship with the identity provider, it trusts that token to be valid from an authentication point of view. Another advantage of a modern identity provider is single sign-on, meaning that our client can log into other servers that trust that identity provider without having to enter their username and password again. They say signed in once, and they can access everything that trusts that identity provider. This is, of course, a bit of an over simplified diagram, but it really showcases the benefits of modern authentication, as well as the role of the identity provider.

The identity provider is really at the center of modern authentication. A modern identity provider offers authentication, authorization, and auditing services, as well as single sign-on, which is often abbreviated as SSO. Single sign-on is really a key part of today's identity systems. As we're using so many systems daily, it's a requirement, not only for productivity, but also for security.

Introduction to Microsoft Active Directory

Our next topic for this module is Microsoft Active Directory. Before we talk about Microsoft specific, let's take a step back and talk about directory services in general. A directory service is a customizable information store that functions as a single point from which users can locate resources and services distributed throughout the network. When we talk about resources, it includes, of course, users and groups, devices, printers, and more. It's also a single point for administrators to manage all of those objects. Now let's talk more about Microsoft specific and talk about Active Directory Domain Services, which you will often see as AD DS in different documentation. Active Directory is a set of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks. Active Directory Domain Services stores information about members of the domain, including devices, end users, verifies their credentials, and defines their access rights, and it's really a central component in organizations with on-premises IT infrastructure. However, as it has been released well over 20 years ago, it's not the most modern identity system, and by default, it doesn't support the latest innovations in identity technology. For the cloud solutions, Microsoft has created Azure Active Directory, which is really the next evolution in Microsoft identity solutions, and it's a cloud-based solution. Now let's talk more about Azure Active Directory. Azure Active Directory, which you will often see written as Azure AD, is Microsoft's cloud-based identity and access management service, and from a branding perspective at Microsoft, it's part of their Microsoft Entra suite of services. The goal of Azure AD is to provide a single identity system for all of your cloud and on-premises applications. Azure AD can be used for both your internal and external users to access your cloud and custom applications. In fact, each Microsoft cloud subscription uses Azure Active Directory in the back end, whether you're getting a subscription for Microsoft 365 or Office 365, Azure, or Dynamics 365 and the Power Platform, Azure AD is provisioned with it. When we talk about identities in Azure Active Directory, we're not only talking about users. There are five main types of identities that can be managed by Azure Active Directory. The first one is of course users, such as employees and guests. Often, you might need to give the same permissions to multiple users, and that's when it's a lot easier to use groups. Azure Active Directory allows you to create different types of groups in which you can add members and assign permissions, or even licenses to those groups. Our next type of identity is a Service Principal. A Service Principal is a security identity used by an application or service to access a specific resource. You can think of it as an identity for an application. Another type of identity can be a managed identity. Managed identities eliminate the need for developers to manage credentials. Managed identities provide an identity for an application to use when connecting to resources that support Azure AD authentication. Our last type of identity that we will find in Azure AD are devices. A device is a piece of hardware, such as a mobile device, laptop, server, or printer. Device identities can be set up in different ways in Azure AD, which determine properties such as who owns the device. Managing devices in Azure AD allows an organization to protect its assets by using tools such as Microsoft Endpoint Manager to ensure standards for security and compliance are met. Before going further, I want to do a quick note on licensing. Azure Active Directory has multiple licensing tiers or editions, and some of the features we will talk about in this course do require premium licensing. Licensing also always changes, so make sure that you always check the latest information, and I have added a link in the slides. Remember, you can download the slides from the Exercise Files tab, so you can easily copy and paste the link. We talked a lot about the cloud, however, many enterprises in the Microsoft ecosystem have started with an on-premises IT infrastructure, so they used Active Directory Domain Services for their identity needs. Most enterprises today still have an on-premises infrastructure, whether it's for file shares, collaboration apps, such as SharePoint Server, or line of business applications. Hybrid identities is what allows their users to be productive, whether they work with applications on-premises or online. Let's take a look at a high-level diagram, what are hybrid identities. So we have our on-premises Active Directory that the company has been using for over a decade, where all of our identities are. We also have Azure Active Directory as we're using Microsoft 365 and cloud workloads. The first part of a hybrid identity is that Microsoft offers a tool called Azure Active Directory Connect, or Azure AD Connect for short, which allows you to synchronize all of the properties of your users and groups from on-premises to the cloud. It can also synchronize the hash of the password, which makes it possible for a user to authenticate and be authorized to work with files and applications, both on-premises and online, with the same username and password. If I look at an example of a hybrid user in Azure Active Directory, you can see that even if we're in Azure Active Directory, we have all of the properties of that user, and under the source we see that it's Windows Server Active Directory. I'm in edit mode in the screenshot, but as the user originated on-premises, I cannot make any changes to the user in Azure AD, I need to make the changes in the on-prem Active Directory, and then those changes will be synced by Azure AD Connect to the cloud. Now that we know the basics, I just want to cover some terminology, this way when you read documentations or forums, or have questions about hybrid identity in a certification exam, you know exactly what it references. For accounts that only exist in Azure Active Directory, so they have been created in the cloud and only exist in the cloud, you will often see this called Cloud-Only accounts. Other terms that I have seen in Microsoft documentation are Cloud-Sourced and Cloud-Mastered accounts. So, if you see those terms, it means that those accounts have been created directly in Azure AD. Now for accounts that are synchronized from on-premises, we will often see the term directory synchronized user.

Azure AD Authentication Methods

Now that we know what Azure Active Directory is, let's dig deeper and learn about the different types of authentication methods that it can provide. We have already established that authentication is the process of verifying an identity to be legitimate. In order to verify identities, we have traditionally used the username and password combination, but the truth is that passwords are not perfect. I've even heard at a conference in the past that the only people who love passwords are the hackers. Some of the main problems with passwords are that users reuse passwords across multiple services, meaning that if one of those gets hacked, it opens the door for the hacker to many other services for that user. Also, good secure passwords are difficult to remember, which can decrease productivity. To further show you why passwords are not the most secure authentication method anymore, let's take a look at three different statistics that show it. First of all, according to the Verizon 2020 Data Breach investigation Report, 80% of breaches in 2019 were caused by a password compromise. In 2018, it was 81%, so it's not an odd year. This is unfortunately the hard truth. The second statistic might explain it. According to Google in partnership with a Harris poll, 65% of people reuse passwords across multiple sites, and 13% of people just the same password for all of their passworded accounts and devices. So now that we saw why passwords are not the the most secure form of authentication, what can we do better? The first thing you can enable as an organization to be more secure is multi-factor authentication. Multi-factor authentication requires more than one form of verification. So it can ask you for something that you know, for example, a PIN or a password, something that you have, like a phone or a hardware key, or something that you are, so like a fingerprint or a facial scan. Multi-factor authentication is the combination of having at least two of those methods required. Microsoft internal studies show that enabling multi-factor authentication can reduce the risk of identity compromise by as much as 99.9%, so that is huge. As I said at the beginning of the slide, but I want to emphasize it again, enabling multi-factor authentication is always the first thing to enable in an environment in order to provide greater protection to user identities. Now, if we talk Azure Active Directory more specifically. There are four ways that Microsoft supports an additional factor in addition to the password. You can use the Microsoft Authenticator app, an OAuth hardware token, a text message or SMS, or finally a voice call. Administrators can disable certain methods if they want to. The most often disabled are usually the SMS and voice call, as they are considered the least secure. Without going into too much detail, the SMS and voice calls are transmitted in clear text, and if a hacker really targeted a person, there are open-source out there that could intercept those details. Don't get me wrong, having multi-factor authentication with SMS or voice is still way better than not having multi-factor authentication at all. However, if your organization wants to take it to the next level, disabling SMS and voice from your multifactor authentication options would be the next step. Our next authentication method, which is recommended by Microsoft as the most secure is passwordless. Passwordless authentication is based on something you are rather than something you know. Some options can be a fingerprint scan in Microsoft Authenticator, a FID02 security device, which some of the latest keys actually have a fingerprint scanner on them, or it can be a face scan in Windows Hello. So it would automatically default to a something-you-are option rather than something you know. So how does it work? After the initial setup, when you log in, you enter your username, and instead of asking you for a password, it will automatically default to the passwordless option you have set up initially. In the screenshot above, it asks the user to confirm the number under Microsoft Authenticator app, which means the user needs access to their phone, as well as the capability to unlock it, select the right number, and in addition, authenticator can request a fingerprint confirmation, depending on how it's set up. So the user can effectively log in without entering their password. If we look at how Microsoft positions the three authentication methods we have talked about so far, first of all, at the bottom right, we have Passwords alone, which are convenient, but low security. On the top left, we have Password and Two-Factor Authentication, or MFA, which is high security, but inconvenient. And finally, we have Passwordless Authentication, which is seen as the most convenient, as well as the most secure option of all three.

Demo: MFA and Passwordless Authentication

Now that we have seen the theory, let's go in the lab and check out what multi-factor authentication and passwordless authentication look like for end users. We are now in the lab. Let me open up the browser here, where for the first demo for MFA, we will log in with the user called MFAUser@globomantics.org. Now, I will click on Next, so I enter my username. Then it will ask me for my password. Let me enter that in. So I have my first factor of authentication, my password. Let's click on Sign in, and it will say, hey, you know what? This account is enabled for multi-factor authentication, so we need another thing to verify your identity. Right now with this account, I have set up only my phone number. So what it does, it says I can either text you at the number ending with 02, and you see, it doesn't actually put the full number on there, just the last digits, so you should know the phone number, or I can call you. Let's do a text here, and let's wait for a few seconds. Usually, it's pretty fast, and let's see what happened. So let me go to the other tab, and here, I'm logged in on my phone, and what happened is we got a text message saying, hey, use the verification code 657333 for Microsoft authentication. So let's take it, 657333. Let's hope I will not forget it. There we go, click on Verify, and we did good. We were able to sign in by using multi-factor authentication using a text message, or SMS, as your second factor of authentication. The code you get by text message is always different. That's why I didn't mind sharing it with you on the screen, because every time Microsoft sends you a code, it will be a different code, so that code by now is already expired. Great! So let me close this now that we have looked at multi-factor authentication. Let's take a look at passwordless authentication. So I went back to a guest profile in Edge, this way I'm not logged in anymore, and this time we're going to log in with another account that is configured for passwordless authentication. The account, well, I named it NoMorePasswords@globomantics.org. This way, this account should not have to put a password. Let's check it out. So now, I only entered my username. Watch what happens when I click Next. It will not ask me for an actual password. Instead, it says, Hey, Vlad, open your Authenticator app and enter the number shown below to sign in. So, let me just open up the Authenticator app, and let's go back to my phone over here. What happened is you see I have a pop-up on my phone by Authenticator, saying, hey Vlad, are you try trying to sign in, because we got a signing request from the globomantics.org organization. The user is NoMorePasswords@globomantics.org, and if it's you, enter the number. So we should enter 28. Let me enter 28 here and say yes, I am the one trying to sign in. Let's answer it. Now the screen went black over here. This is because it's asking me for my fingerprint. So, in addition to having the phone, knowing the number, I also need the fingerprint to confirm that, yes, it's me. So I have approved it, and it looks like we were too slow, because if we explained everything, of course, it would be a lot faster, usually. Let's do it again, but faster. Let's go here, New sign-in request, enter 40 for yes, it's me. This time, I'm sure we're fast enough, and we managed to log in to this account without ever entering a password. This is it for this quick demo showcasing multi-factor authentication, as well as passwordless authentication from an end-user perspective. Now, let's head back to the slides and talk about conditional access.

Azure AD Conditional Access

Next up on our list of access management capabilities is Conditional Access. Conditional Access is an additional layer of security that organizations can enable after a user is authenticated and before they are able to access data or other assets. So technically, it sits between the authentication and authorization layer. Conditional Access policies evaluate every access attempt and decide if access is granted, access is blocked, or if it requires one or more conditions to be met before access is granted, such as requiring MFA, or requiring the device to be marked as compliant. Azure Active Directory Conditional Access is implemented through policies that each organization creates, and you can think of it as a bunch of if statements. Conditional Access policies can be applied to users or even applications. So you can, let's say, apply a Conditional Access policy to every user that tries to access a specific SharePoint site. Let's take a look at a high-level diagram of Conditional Access. The first thing that happens is that the user must enter their first factor of authentication, and, of course, that needs to be valid before Conditional Access kicks in. After the first authentication, Azure Active Directory Conditional Access will analyze multiple signals based on your policies. Things it will look at are who are you, what permissions do you have, what country or network are you logging in from? It can also calculate the sign-in risk. So, is this the first time you sign in from this PC or IP, or is it one that you use often? Conditional Access verifies every access attempt, so your user risk or real-time risk can vary during the same session. Depending on all those signals and your policies, it will make one of three choices: whether access is granted, whether more conditions need to be met, such as multi-factor authentication prompt, or block your access. Conditional Access is really a key part of the verify-everything principle of the Zero Trust methodology. The goal of Azure AD Conditional Access is really to allow you to find a balance between productivity and security inside your organization, which is really one of the toughest things to balance as you create your security policies. On one hand, you want everything to be as closed down as possible, and I mean think of all the action movies you've seen where you need to pass like 10 different authentication methods to access information, like a voice, a fingerprint, an eye scan, a face scan, a card, and everything, and of course, that makes it super secure. But imagine if you implemented this many barriers for users that just want to find a document on the intranet, their productivity would tank, as they would spend so much time validating their identity. Conditional Access allows you to find that balance of using all of the available signals at your disposal and Microsoft's advanced algorithm to detect user risk and sign-in risk detection, and depending on the content they want to access, apply different security policies. This ensures that your data and identities stay secure while your users stay productive. By verifying all of those available data points and continuously checking all of the the signals for every access request, Conditional Access fits the verify explicitly and assume breach mentality of the Zero Trust methodology. So what are some examples of Conditional Access policies that we can create? Let's say, if a user wants to access SharePoint Online from a trusted network after authenticating on a compliant device, grant access. However, if a user wants to access a collaboration SharePoint site from an untrusted network, an action must be done, which is prompting for multi-factor authentication. You can also do it based on admin roles, so you can say that for any user that logs in that has an admin role, always prompt for multi-factor authentication. Let's take a look at a few other examples. Let's say that a user authenticates at home on a managed device and is connected via VPN, so a trusted network, and browses the intranet. That's allowed. However, if that user tries to access the SharePoint site where employees' files are stored, we can ask for an MFA prompt. This is due to Conditional Access allowing us to apply policies even to specific sites. As a last example, let's say that I have a user that tries to access SharePoint from another country. I can block access to that user.

Demo: Azure AD Conditional Access

Now that we have seen the theory, let's head over to the lab environment and check out Azure Active Directory Conditional Access in action. We are now in the demo environment. First of all, let me show you a bit of what the admin view looks like. With Azure Active Directory Conditional Access, we create multiple policies. Right now, I created one that is called Block Canada! So let's check it out. So first of all, I have the name. Then it will ask me, okay, Vlad, what users does this policy apply to? In this example, I only apply it to Vanessa, but I could apply it to Directory roles, so everybody that has a certain Azure Active Directory admin role. So I could base it on directory roles. I can also say, okay, you know what? This applies to all of my external users and guests, or I can say, you know what? This applies to all my users. But right now, we only want to apply it to Vanessa. After that, I can select what cloud apps this applies to. I can say this applies to all of the apps, or I can select to say, hey, this only applies to SharePoint Online, for example. I also have have a warning here saying that, hey, be careful, don't lock yourself out because if I'm from Canada and then I say block Canada from logging in all cloud apps, I can't log in as an admin anymore to fix my mistake, so I do have that warning there. After that, it's asking me for the condition. What condition do I base this policy on? You see, I have the user risk and sign-in risk level, I have my device platforms, my locations, which in this case, I actually configured it to say, you know what, apply this only when the selected location is Canada, and this will be based on the IP address. But if you want to, for example, you could also base it on the GPS coordinates of the device, so that is an option as well. Great! Then it will say, okay, Vlad, if the user you specified is trying to access the app you specified in Canada in our case, what do you want to do? And in my case, I'm saying, block access, but I could also say, grant access and require multi-factor authentication. So that's another option I have, but let me leave it to block access for this demo. Yes, I don't want to save anything, and then I can say, do I want to enable this policy only as a report only, so log everything, but don't necessarily actually block the users, turn it on, which is what it is right now, or keep it save, but do not apply it yet. Something else that is cool that you have as an admin, let me go back to my conditional policies, you actually have a what if. So you can enter a bunch of combinations. Let's say I will say, what happens if Vanessa logs from Mexico? Then it will tell me all of the different policies that would be applied and would Vanessa be able to sign in or not. So you do have a ton of different tools as an admin to make sure you configure them exactly the way you want to. So for this demo, we know that we blocked Canada. This virtual machine that I'm on right now is actually in the United States, so if everything goes well here, I will go on Next, type in the password, and say yes, stay signed in, and I successfully logged in to Microsoft 365 from the US. Now, let me close this and let me go to this other virtual machine that I have, and this one is in Canada here. That's why I have the closest shade of red I could find for the background, but this one is from Canada, so logging in with the same user, let me put the password in there. Let's try and sign in again. I had it there too long. You see, I have an error message, and let's zoom in a bit. It says, you cannot access this right now; your sign-in was successful, but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin. So it's telling me, hey, you logged in with the right username and password, you passed the authentication stage; we know you are Vanessa, but we can't allow you to access anything. So this is where Conditional Access jumps in, in-between the authentication and authorization stages. I'm authenticated, but I'm not allowed to access anything. Then, if I click on More details, I actually have a ton of different things that I can send to my admin. My admin can then go and say, hey, let me go in Conditional Access, what if, type all of the different details in here and probably with the IP address, the admin can say, hey, you know what, it's because you're logging in from Canada, and this is the policy that is blocking you. So this is it for this demo on Azure Active Directory Conditional Access, a tool that we have in our tool belt in order to balance productivity and security and help us towards our goal of implementing Zero Trust. This is the last demo of this module. So let's head back to the slides and finish the module.

Module Conclusion

To finish off this module, let's review what we have learned. We have first started this module by learning some identity concepts starting with authentication and authorization. Remember that authentication is done first and it's confirming that users are who they say they are. Authorization is done afterwards and checks if a user is allowed to access a certain resource. We have then talked about modern authentication and the role of the identity provider. Next up, we have introduced the concept of directory services and talked about Microsoft Active Directory Domain Services, as well as Azure Active Directory, which is in the cloud. We have also learned how Azure Active Directory can manage hybrid identities. Afterwards, we have learned the different authentication methods for Azure AD and learned about multi-factor authentication and passwordless authentication. We learned what they are and how they can help us secure our identities. Finally, we have learned about Conditional Access, which allows us to balance security and productivity by only prompting for certain actions depending on many signals that are evaluated for each access request. This is it for this module. Up next, we will learn about the threat protection solutions for Microsoft 365.

Threat Protection Solutions for Microsoft 365

Module Introduction

Hello, and welcome to this Microsoft 365 Security, Compliance, and Identity course. My name is Vlad Catrinescu, and I'll be your instructor for this course. In this module, we will learn about the threat protection solutions for Microsoft 365. We will start this module by introducing some industry terms and set of security solutions, which are SIEM, SOAR, and XDR, and understand what Microsoft product fits in which category. We will then introduce Microsoft 365 Defender and then dive into the three main products, part of it which are Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Defender for Endpoint. After we find out how those tools work together to help us secure Microsoft 365, we will learn about Microsoft Sentinel, a single solution for attack detection, threat visibility, proactive hunting, and threat response. By the end of this module, you'll be able to describe the threat protection solutions for Microsoft 365.

Introduction to SIEM, SOAR, and XDR

Let's start by introducing three very important security terms, SIEM, SOAR, and XDR. Those three are actually a set of security tools used by enterprises across the world to secure their environment. SIEM stands for Security Incident and Events Management, SOAR stands for Security Orchestration Automated Response, and finally, XDR stands for Extended Detection and Response. Let's take a look at what each one of them does. First, a Security Incident and Event Management system is a tool that organizations use to collect data from across the whole digital estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents. Next up, a security orchestration automated response system collects data from many sources, similar to a SIEM system, however, the SOAR system can do something more. It can trigger action-driven automated workflows and processes to run security tasks that mitigate the issue. Our last but not least tool is the extended detection and response category. An extended detection and response system is designed to deliver intelligent, automated, and integrated security across an organization's domain. It helps prevent, detect, and respond to threats across identities, endpoints, applications, email, IoT, infrastructure, and of course, cloud platforms. Now, if we take a look at the Microsoft products for each category. In the Security Incident and Event Management category, we have Microsoft Sentinel, which is also a security orchestration automated response system. In the extended detection and response category, we have Microsoft 365 Defender. Now that we know where those products sit from an industry solutions point of view, let's dive into the details for both of them.

Microsoft 365 Defender

The first product we will talk about is Microsoft 365 Defender. So what is Microsoft 365 Defender? Microsoft 365 Defender is a unified pre and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. Microsoft 365

Defender has four main services, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity, and last, but not least, Microsoft Defender for Cloud Apps, which was previously called Microsoft Cloud App Security. One of the big selling points of Microsoft 365 Defender is that it's an integrated, cross-domain solution that stitches together signals from endpoints, identity, data, and applications. Instead of each one of those domains having its own tool that is isolated, with Microsoft 365 Defender, you can group signals from all domains in entities called incidents, which really allow security teams to see the full picture of a breach, instead of each one of them focusing on a single domain and working to manually stitch it together. When looking at an incident, which we can see an example of in the screenshot, you can see that the scope shows how many devices, users, and mailboxes have been affected, and we also have a group timeline in details from an attack in a single location, allowing us to focus on the bigger picture and make sure that we remediate that bridge completely, not just part of it. Before we deep dive into the different Microsoft Defender products, I want to talk about the Microsoft 365 Defender portal. The Microsoft 365 Defender portal is the central location or home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure. You can access the Microsoft 365 Defender portal at security.microsoft.com. One of the cool things we will also find in the Microsoft 365 Defender portal is the Microsoft Secure Score. The goal of the Microsoft Secure Score is to provide you a quick way to understand your security posture. One of the nicest features, in my opinion, is that it also helps prioritize actions based on potential to reduce risk by using gamification in a way, as the bigger the security impact, the more points it gives you towards your secure score. By doing the high-point, high-reward action items first, you're also taking the biggest steps, so it's really a win for everyone. And also, in my opinion, a nice way to present your security progress to management and non-technical executives. The Microsoft Secure Score will show you recommendations around multiple cloud services and security tools such as Microsoft 365, Azure Active Directory, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps.

Demo: Microsoft 365 Defender Portal and the Secure Score

Now that we have seen the theory, let's head over to the lab and check out the Microsoft 365 Defender portal, as well as what the Microsoft Secure Score looks like in action. We are back in the demo environment. Let me open up the browser here where I'm in the Globomantics tenant, and I already navigated to security.microsoft.com. On the left side, I will see all of the different apps and services that I have access to. This is really your go-to place for all of the different threat protection solutions for Microsoft 365, and in the middle I will see my Home page, which remember, is customizable. So, for example, if I don't care for the Security news feed, I can just remove it and then I can rearrange the rest of cards or even some of the cards that maybe I do not have, and customize the Home page to fit the things that I need. Of course, if you don't have a lot of devices in a demo tenant, this might look a bit boring, however, I do have another tenant open over here which has a bit more action. Using cards, I can really see a highlight from all the different Defender services, for example, how many devices lack protection from Defender for Endpoint. I can also see information on high-impact threats, emerging threats, things like that. I can also see, for example, how many discovered devices I have, and more. So this is the Microsoft 365 Defender portal. Now let me go back to my Home tenant and let's talk about the Secure Score. As you can see in my demo tenant, I'm not doing the best job. My Secure Score is only at 34.22%. We have a highlight over here that says, Vlad, you're doing really bad on Identity, only 5.63%. However, on data you're doing a pretty good job with 77% and on Apps you're still below average with 46%. Let's take a look if we go on Improve your score. Let me go into the Overview first of all. Here you see again I see my Secure Score, I see the Breakdown by category, and then the part that I really love is the Recommended actions. You can see right now today if I require multifactor authentication for admin roles, I would add a 6% impact to my score. If I create a Safe Links policy for email messages, I add another 5.39%. So this way I really have a list of things that I should implement as an admin in order to increase security inside the tenant. The more that you do, the better your score will be and you actually have a history that you can show. This way, again, if you ever need to show your progress to executives, the Secure Score is an easy way to do it. You can also go in the Recommended actions here to see really all of the different recommendations, even the ones that do not add a lot. But, again, for me the thing that I like the most is that they are sorted by priority, and the bigger the security impact, the bigger the score. So this is the Defender portal and the Microsoft Secure Score. Now, let's head back to the slides and talk about the different Microsoft Defender services.

Microsoft Defender for Identity

Let's start deep diving into each product, starting with Microsoft Defender for Identity. Let's start with a nice overview from Microsoft. Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions detected at your organization. Microsoft Defender for Identity has four key areas, monitor and profile user behavior and activities, protect user identities and reduce the attack surface, identify suspicious activities and advanced attacks across the cyber-attack kill-chain, and investigate alerts and user activities. Let's take a look at each one of those four key areas in detail. First, Microsoft Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership. This will create a behavioral baseline for each user. After it has that baseline, it uses its analytics capabilities to identify anomalies in user behavior and provide you with insights into suspicious activities and events. Another key area of Microsoft 365 Defender for Identity is to protect user identities and reduce the attack surface. Defender for Identity can provide insights on identity configurations and suggested security best practices that you can implement. This will really enable you to reduce your organizational attack surface. Another great feature is the visual lateral movement paths, an easy way to see how attackers can move laterally inside your network so you can prevent those risks in advance. Defender for Identity can also provide you reports so you can identify users and devices that are, for example, authenticating using clear-text password, which can be a big risk, so this way you can remediate it before it becomes the source of a breach. Our next area is identifying suspicious activities and advanced attacks across the cyber-attack kill-chain. We usually split this into four different parts. First of all, reconnaissance, where Defender for Identity can help you identify rogue users and attackers' attempts to gain information. Attackers are searching for information about usernames, users' group membership, IP addresses assigned to devices, resources, and more using a variety of information. The next stage is the compromised credentials, where Defender for Identity can help you identify attempts to compromise user credentials using brute-force attacks, failed authentication, user group membership changes, and other methods. Afterwards, we have the lateral movements phase, where Defender for Identity can help detect attempts to move laterally across the network to gain further control of sensitive users by using things such as pass the ticket, pass the hash, overpass the hash, and really other attacker techniques. Lastly, Identity Defender can help highlight attacker behavior if domain dominance is achieved through remote code execution on the domain controller. Our last pillar is that Defender for Identity is designed to reduce the general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline. The Defender for Identity attack timeline view allows you to easily stay focused on what matters, leveraging the intelligence of smart analytics.

Microsoft Defender for Office 365

Our next Microsoft Defender product is Microsoft Defender for Office 365. Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links, collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients. We can really split its functionality into four key areas, threat protection policies, reports, threat investigation, and response capabilities, as well as automated investigation and response capabilities. Let's start with the threat protection policies that we can implement. The first one is called safe attachments. This policy provides zero-day protection to safeguard your messaging system by checking email attachments for malicious content. It routes all of the messages and attachments that do not have a virus or malware signature to a special environment, and then uses machine learning and analysis techniques to detect malicious intent. If no suspicious activity is found, the message is forwarded to the mailbox. The second one is called safe links. This provides time-of-click verification of URLs, for example, in email messages and Office files. Protection is ongoing and applies across your messaging and Office environment. Links are scanned at each click, and then safe links remain accessible and malicious links are dynamically blocked. Third, we have anti-phishing protection. With this policy, Defender for Office 365 can detect attempts to impersonate your users and internal or custom domains. It applies machine learning models and advanced impersonation detection algorithms to avert phishing attacks. Last, but not least, we have safe attachments for SharePoint, OneDrive, and Teams. This protects your organization when users collaborate and share files by identifying and blocking malicious files in team sites and document libraries. Now let's talk about Microsoft Defender for Office 365 reports. Defender for Office 365 comes with multiple real-time reports to measure its performance, such as URL protection report, threat protection status for content and email, as well as user reported messages to see email messages that have been marked as spam or malicious by users. Next up, we have the threat investigation and response capabilities, which first of all includes threat trackers, Threat trackers provide the latest intelligence on prevailing cybersecurity issues. For example, you can view information about the latest malware and then take countermeasures before it becomes an actual threat to your organization. Next up, we have the threat explorer, which is also called real-time detection, which is a real-time report that allows you to identify and analyze recent threats. Lastly, we have a really interesting feature, which is the attack simulator. This allows you to run realistic attack scenarios in your organization, such as spare phishing, attachment attack, password spray, and brute force. This way you can educate and test users before a bad actor succeeds. Our last key area of Microsoft Defender for Office 365 is Automated Investigation and Response. This includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or you can launch them manually as well. The playbook will recommend actions to remedy the situation, and your security team can approve or reject the actions. This makes it easier for your security team to focus on more advanced attacks while keeping in line with security best practices.

Microsoft Defender for EndPoint

Our next Microsoft Defender product is Microsoft Defender for Endpoint. Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. With Microsoft Defender for Endpoint, we have six key areas, threat and vulnerability management, attack surface reduction, next-generation protection, endpoint detection and response, automated investigation and remediation, as well as Microsoft threat experts. So let's take a look at all six of them in detail. First of all, the threat and vulnerability area gives you a risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. Microsoft Defender for Endpoint uses sensors on devices for real-time discovery to avoid the need for agents or scans, making it easier for administrators and users at the same time. Microsoft Defender for Endpoint also enables you to reduce your attack surface and reduce places where your organization is vulnerable, which is really that first line of defense in the stack. Microsoft Defender for Endpoint will make sure that the device configurations are properly set and exploit mitigation techniques are properly applied. This also includes network and web protection, which regulate access to malicious domains, URLs, or IP addresses. Next up, we have next-generation protection, which sounds quite markety, but what it includes it's really Microsoft Defender antivirus, as well as behavior-based and real-time antivirus protection. This makes sure that you have real-time protection and always on scanning to keep devices safe. You also have cloud-delivered protection, which means near instant detection and blocking of new and emerging threats. Lastly, Microsoft offers dedicated protection and product updates to always keep Microsoft Defender up to date. Our fourth pillar is Endpoint detection and response, which provides advanced attack detection that are both near real-time and actionable. With that information, security teams can prioritize alerts and gain visibility into the full scope of a potential breach. Furthermore, Defender for Endpoint will automatically aggregate alerts with the same technique or attacker into an incident, making it easier to investigate and respond to a threat. Next up, we have the automated investigation and remediation, which uses inspection algorithm and processes used by analysts to examine alerts and take quick remediation action to resolve breaches. The goal of this is to significantly reduce the volume of alerts that must be investigated individually and allows your security team to really focus on more sophisticated threats. The remediation can occur either automatically or only after approval, depending on your organization's configuration. Last, but not least, we have the Microsoft threat experts, which is a managed threat hunting service that provides your security team with an expert level monitoring and analysis to help them ensure that critical threats in your unique environments don't get missed. This managed threat hunting service provide expert-driven insights and data through two main features, targeted attack notification and access to experts on demand. This is a feature that is available, but not included with Defender for Endpoint, as customers need to apply for the Microsoft threat experts managed threat hunting service, and this feature does require some add-on pricing.

Demo: Viewing a Microsoft Defender Incident

We have now seen the features of the full Microsoft 365 Defender suite. Now let's go to the lab and check out an incident that combines signals from all of them. I am now in the lab environment. Let me open up the browser over here where I'm in the Microsoft 365 Defender portal. What I will do now is on the left navigation, I will go under Incidents where I will see all of the different incidents with the filters applied, and you can apply filters on many things, from the status, severity, tags, and things like that. Let's go in the second one over here. It's called a multi-stage incident involving Initial access, Collection on one endpoint reported by multiple sources. If we take a look at this summary, you can see that right now we have 1 impacted device, 4 impacted users, 4 impacted mailboxes, and 1 impacted app. This is really the beauty of combining everything in a single incident. All of those signals that traditionally would be managed by four different tools and four security teams are now combined together because at the end of the day this is one attack you need to be able to contain and mitigate that attack because if you only take care of one pillar, let's say devices, all the other ones can still move laterally inside your organization. We can see what are the impacted entities. We have our workstation, the different users, as well as the email addresses, and then I also have a timeline. We can see that this happened on August 10, 2022 when a suspicious URL got clicked on workstation 15. A user accessed a link in a ZAP-quarantined email, and then we have a potential malicious URL click was detected from a mailbox. And we can really follow everything that happened inside this incident. We can see how did this attack gain access? How did it evolve? What are all the entities that actually got attacked, and what do we need to do to mitigate it? We can also see, for example, if we go into the affected apps, it had something to do with Office 365. I can click on it, and then I can go and see all of the different details of what happened to that service. But this is an incident in Microsoft Defender. Really the biggest advantage is that it's able to combine the timeline and the alerts from all those different Defender services that we learned about and were able to see it in one incident and deal with it all at the same time. This is it for this demo on Microsoft Defender. Now let's head back to the slides and learn about Microsoft Sentinel.

Microsoft Sentinel

With Microsoft 365 Defender covered, there is another tool that can help us protect our Microsoft 365 data, which is Microsoft Sentinel. If we take a high-level overview and really split Microsoft Sentinel into four main categories, its goal is to first of all collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. It can also help you detect previously uncovered threats and minimize false positives using analytics and threat intelligence. Microsoft Sentinel allows you to investigate threats using AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft. And finally, it enables you to respond to incidents rapidly with built-in orchestration and automation of common security tasks. Okay, so let's dive deeper into each one of them. First of all, the most important part of a SIEM and source system is to be able to connect to all of your data. A SIEM is nothing without actual data to analyze, so it's always the first part of the setup. Microsoft Sentinel has a great number of built-in connectors, whether it's a Microsoft service, such as Azure Active Directory, Microsoft 365 Defender, Office 365 services, as well as external solutions, such as F5 BIG-IP, Okta, Google Workspace, and more. In fact, there are over 100 built-in connectors at the time of recording this course, which includes, again, both Microsoft and third-party sources. If a system you want is not there, you can also use the common event format, syslog, or the REST API to connect your data sources with Microsoft Sentinel. Microsoft Sentinel also integrates with Azure Monitor Workbooks. Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. I really think of them as a dashboard that can help you be more productive by looking at the signals and information that matters most. Most connectors have one or more built-in workbooks, and you can also create your own using the information that matters to you. Here's an example of the built-in workbook example for Amazon Web Services called AWS User Activities. You can see things such as sign-in and login events, whether the success is a result or a failure, as well as even by user how many logins and failures they each had. Here's another built-in example for SharePoint and OneDrive. Built-in workbooks are a great way to get you started, and as your usage of Microsoft Sentinel progresses and your needs become more clear, you can customize them to what's important to you. Next up, we have analytics and incidents. For most connectors, you have built-in analytics rules templates, which are basically the rules that say this is suspicious, and it sends you a notification. Microsoft Sentinel can collate multiple connected alerts into incidents, allowing you to see the bigger picture and fix the threat as a whole instead of focusing on separate alerts. Microsoft Sentinel comes in with built correlation rules, and you can, of course, also create your own. This is what the Incidents dashboard looks like in Microsoft Sentinel. And in the Alerts column, you can see how many alerts each incident includes. Some of them might only include 1 alert, while some may combine over 20 alerts for you in a single incident. We have seen a lot of the SIEM part. Now let's talk about the security automation and orchestration part of Microsoft Sentinel. With Microsoft Sentinel, you can create automation rules that can do things such as tagging incidents, assigning them to the right personnel, changing the severity, or even running playbooks. And by doing those rules, you take some boring tasks off your security team, again, allowing them to focus on more important things. I mentioned playbooks. Playbooks are collections of procedures that can be run based on workflows built on Azure Logic Apps. There are over 200 connectors built in, and I estimate thousands of actions that allow you to really build workflows unique to your needs for your organization. This is what the Microsoft Sentinel playbook creation experience looks like. Some of you might be like, hey Vlad, isn't this Power Automate part of the Power Platform? Well, yes and no. This is Azure Logic Apps, which shares a lot of the same back end as Power Platform, so that's why they look almost exactly the same. As you can see in this example, Microsoft Sentinel can be your trigger, and then you can do things such as opening tickets in ServiceNow, posting a message in Teams, blocking a user in Azure AD, blocking an IP in Palo Alto, and more. The ability of automating different tasks across multiple systems is amazing for your security teams, productivity, and answer speed.

Module Conclusion

To finish off this module, let's review what we have learned. We have started this module by doing an introduction to SIEM, SOAR, and XDR, a set of security tools, part of your toolbelt, to keep an organization secure. We have then learned about Microsoft 365 Defender, an extended detection and response tool that helps us protect our Microsoft 365 data, and we have covered the features of three main products inside Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Defender for Endpoint. We have also learned about the Microsoft 365 Defender portal, as well as the Microsoft Secure Score. Next up, we have learned about Microsoft Sentinel, a SEIM and source solution that helps your security teams stay on top of incidents and automate tasks to increase productivity. This is it for this module on threat protection solutions for Microsoft 365. In next module, we will learn about the compliance solutions for Microsoft 365.

Compliance Solutions for Microsoft 365

Module Introduction

Hello, and welcome to this Microsoft 365 Security, Compliance, and Identity Concepts course. My name is Vlad Catrinescu, and I'll be your instructor for this course. In this module, we will learn about the compliance solutions for Microsoft 365. We will start this module by doing an introduction to regulatory compliance in general as a task for IT professionals. Afterwards, we will talk about Microsoft's privacy principles. Next up, we will talk about the Microsoft Service Trust Portal and how it can help us with our compliance goals. And finally, the most exciting part will be about the Microsoft Purview compliance solutions for Microsoft 365 where we will talk about what specific solutions and features Microsoft offers to make sure that we remain compliant. By by end of this module, you'll be able to describe Microsoft's compliance solutions.

Introduction to Regulatory Compliance

Let's start by doing a quick introduction to regulatory compliance and what it actually means. In IT, compliance is a set of digital security requirements and practices. Following compliance requirements is a way to ensure that a company's business processes are secure and that sensitive data, including customers' data, won't be accessed by unauthorized parties. While compliance is similar to security in that it drives a business to practice due diligence in the protection of its digital assets, the motive behind compliance is different. It's really centered around the requirements of a third party, such as a government, a security framework, or a client's contractual terms. If an organization wants to do business in a country with strict privacy laws or in a heavily regulated market, like healthcare, or finance, or maybe with a client that has high confidentiality standards, they must play by the rules and bring their security up to the required level. If we take a look at some popular standards, starting with the one most of you have almost for sure heard about, GDPR. GDPR protects the security and privacy of data belonging to EU citizens and residents. So if your company operates with such data, GDPR may be applied to you, even if your company isn't located in the European union. Another popular one is HIPAA. HIPAA is the IT compliance standard for the healthcare industry. HIPAA regulates how medical organizations protect the sensitive information of their patients. To be HIPAA compliant, you have to ensure that all health data is secure and confidential. Next one is NIST. Consulting firms, suppliers, and other businesses working with federal or state agencies need to follow NIST compliance. This standard highlights various aspects of data management, including access control, risk assessment, system integrity, and many others. Another one is the PCI-DSS standard. Payment processors and other financial services' providers may need to comply with the Payment Card Industry Data Security Standard. This standard helps to prevent credit card fraud and ensure that financial information is protected. If we take a look at a deeper level, what are some example compliance needs? It could be granting individuals the right to access their data at any time, or granting individuals the right to correct or delete data about them if needed. Another very common one is introducing retention periods that dictate the minimum or maximum amount of time that data should be stored. You might also need to enable governments and regulatory agencies the right to access and examine data when necessary. Another type of need might also be to define rules for what data can be processed and how it should be done. Before we start going into the specific tools that will help us follow those regulations, in one of the first modules of this course, we talked about how security in the cloud is a partnership between the cloud provider and the client. Well, so is compliance. Most regulatory standards will have requirements on the security of the data center and physical servers, for example, which will be done by Microsoft. So when you check a specific one, you might see that because you're in the cloud, some of them are Microsoft managed, and you can find the documentation for those in the Service Trust portal, about which we'll talk in just a few minutes. But it's important to remember that compliance in the cloud is a partnership, and even if you have all of the tools available, and we'll talk about those tools throughout this module, it's up to you to implement them, and you have a list of things to implement as well to follow the compliance standards.

Microsoft's Privacy Principles

Next up, let's learn about Microsoft's privacy principles. Something that is very important to remember is that when you use a cloud service, you're entrusting the cloud service provider with one of your most valuable assets, which is your data. Microsoft has six key privacy principles when making decisions around your data. The six privacy principles are first, control, which means putting you, the customer, in control of your privacy with easy-to-use tools and clear choices. Second one is transparency. Being transparent about data collection and use so that everyone can make informed decisions. Third one is security. Protecting the data that is entrusted to Microsoft by using strong security and encryption. Fourth one is strong legal protections, which is respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right. Fifth one is no-content based advertising. This means that Microsoft will not be using email, chat, files, or other personal content to target advertising. The sixth, and last one is benefits to you. When Microsoft does collect data, it is used to benefit you, the customer, and to make your experiences better.

The Microsoft Service Trust Portal

Next up, let's learn about the Microsoft Service Trust Portal. The Service Trust Portal is a single location where you can find audit reports, pen tests, security assessments, and more information on how Microsoft manages security, privacy, and compliance. You can easily access it at servicetrust.microsoft.com. The Service Trust Portal is a free offering. However, some documents do require you to sign in with your Microsoft 365 account in order to access them. Signing in with your Microsoft 365 account also gives you access to the My Library feature. This feature allows you to save certain documents in your virtual library. This way you can easily access them and receive updates when new versions are available without needing to download them or print them.

Demo: The Microsoft Service Trust Portal

Now that we have seen the theory, let's head over to the lab environment and check out the Microsoft Service Trust Portal. We are now in the lab environment, and let me open up the browser where I navigated to servicetrust.microsoft.com. Here, I can quickly find all of the different compliance documents, pen tests, things like that to ensure compliance from the Microsoft site. If I scroll down a bit, we have some audit reports as an example, and let's say that my organization needs to comply with the PSI/DSS standard. Let me click on it here. It will take a few seconds to load the documents. And here I can have, for example, the Office 365 PCI, Attestation of Compliance, AoC. And we can see that it has been updated on August 25th, 2022, so it's quite recent. At the top here, I also have other ones. For example, I can go and check out the FedRAMP Reports, the ISO Reports, things like that. You can also filter by industry, by cloud service, for example, only show me the Office 365 ones that have to do with the energy industry, for example, and then filter by that. If you want to, you can either download the files or save them to your library. This way, as well, if it gets up updated in the future, you can simply go to My Library here at the top, and you will have access to all of the different documents that you have saved in your library. If they get updated, you will have them here. This is it for this quick demo of the Service Trust Portal, your go-to place to get all of the different documents, pen tests, security assessments, Attestation of Compliance. This way, you have them if you ever have a compliance audit. You have all of the documentation to support the compliance requirements on the Microsoft site. Now let's go back to the slides and learn about the compliance solutions that we can use to make sure that we do our share of our responsibilities in Microsoft 365.

Microsoft Purview Compliance Portal and the Compliance Score

With the basics out of the way, let's start talking about the different Microsoft compliance solutions, part of the Microsoft Purview portfolio. The Purview name is actually pretty new, as Microsoft rebranded all of their compliance products in April 2022 and created this Microsoft Purview suite of compliance solutions. With this change, many existing products have been rebranded, mostly by adding Purview inside the name of the feature. If you want to see more about the announcement, you can read it at the link in the slides. In this course, we will cover over 6 different Microsoft Purview products that help us stay compliant in Microsoft 365. Before we get into the products, I want to introduce the Microsoft Purview compliance portal. The compliance portal is a central one-stop location for all of your compliance tools and settings, and it's available at compliance.microsoft.com. As it's a compliance tool, it's only available for administrators with the right roles. This is really where we will find all of the tools that we will talk about in this module. Talking about tools, let's actually already get started with our first one, which is the Microsoft Purview Compliance Manager. The Microsoft Purview Compliance Manager is one of the tools part of the compliance center. Its goal is to help administrators to manage an organization's compliance requirements with clear to-dos. It provides administrator's pre-built assessments for common industry and regional standards, or even custom assessments. It also provides step-by-step guidance to help achieve the compliance standard they're looking for. One of the nice features of the Compliance Manager is the compliance score. If we take a look at what the Compliance Manager looks like before we go into the demo, we have the compliance score, which is 58% right now in the screenshot, and the most interesting feature is really the improvement actions, which is the step-by-step guidance. What are the things that need to be done or enabled in order to achieve your compliance goals? By default, Microsoft has a compliance baseline standard, which takes actions that are most important across all compliance standards, but by going into the assessment templates, you can choose the ones that apply to your organization and see the tasks for you. If we dive deeper into the compliance score, its goal is to provide you with a quick way to understand your compliance posture. One of the nicest features in my opinion is that it also helps prioritize actions based on potential to reduce risk by using gamification in a way, as the bigger the compliance impact, the more points it gives you towards your compliance score. By doing the high-point, high-reward action items first, you're also taking the biggest steps, so it's a win for everyone. And also, in my opinion, a nice way to present your compliance progress to management and non-technical executives.

Demo: Compliance Manager and the Compliance Score

Now that we have seen the theory, let's head over to the lab environment and check out the Microsoft Compliance Manager, as well as the Microsoft compliance score. We are now in the lab environment. Let me open up the browser here where I'm in the Microsoft Purview compliance portal. Here is the central location for all of the different compliance solutions in Microsoft 365. Just to spend a few seconds on the portal, it's very similar to the Defender portal that we have seen in the previous module. You have the different cards that you want to bring in. You can even add some cards and customize where they are on your screen, so it's a very customizable experience. But in this demo, we will focus on the Compliance Manager. Here the first thing that I will see is my compliance score. This will tell me for a selected assessment template what my compliance score is, and, of course, our goal is to be as close to 100% as possible. As this is a demo tenant, you can see that right away I'm at 72%, which might seem really, really good. But if we go in the details, we can see that Microsoft has done most of the job for me, while my points achieved are at 0. So I haven't done a lot of work towards compliance in this tenant, and by default, I am evaluated on the Microsoft-provided baseline template. I also have all of the different tasks that I can do. My improvement actions that I have to do in order to achieve a better score, and again, they are shown in order of importance. So if I do the top ones first, those are the ones that will have the biggest impact on my score. I can also see them again here in Improvement actions at the top. I can see all of the different things that I need to do in order to achieve a greater compliance score. Now let me go into Assessments here. You will see by default, again, I'm assessed on the Data Protection Baseline. However, most organizations that focus on compliance will have a standard they need to adhere to. This is where the assessment templates come in. Microsoft comes in with 20 included templates, which include NIST 800, EU GDPR, FedRAMP Moderate, ISO 27001, and more. And we also have 716 premium templates. For example, for California specific here, we have the California SB-327 information privacy regulation. If you want to, under Assessments here, you can go and tell the Compliance Manager, hey, I want to know what are all the things I need to do in order to reach a specific standard? So I can go and say, okay, let me add an assessment, let me select the template. I'll do EU GDPR, for example, and then just add it in there, and then I will be assessed on that standard. This is it for this quick demo of the Compliance Manager and compliance score. Now, let's sit back to the slides and learn about Microsoft Purview information protection.

Microsoft Information Protection and Sensitivity Labels

Next up on our list of compliance tools is Microsoft Purview Information Protection. Let's start with a nice definition by Microsoft to set the stage. Microsoft Purview Information Protection discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization. It provides the tools to know your data, protect your data, and prevent data loss. Microsoft Information Protection divides its capabilities across four main areas. The first one is know your data, which means organizations can understand their data landscape and identify important data across on-premises, cloud, and hybrid environments. Next up is protecting your data, which enables organizations to apply flexible protection actions including encryption, access restrictions, and visual markings. Third is prevent data loss, which enables organizations to detect risk behavior and prevent accidental oversharing of sensitive information. Finally, we have the govern your data, which allows you to automate the retention and deletion of data for your compliance needs. Now let's talk features. There are four features of Microsoft Purview Information Protection that we will covering this module that are important for Microsoft 365, sensitivity labels, retention policies, data loss prevention, and records management. Let's dive into all of those in detail, starting with sensitivity labels. Sensitivity labels let you classify and protect your organization's data while making sure that productivity and their ability to collaborate isn't hindered. More concretely, sensitivity labels allow you to enforce protection settings such as encryption or watermarks on labeled content such as documents. It allows you to protect content in Microsoft 365 across different platforms and devices. And when integrated with other applications such as Defender for Cloud Apps, you can even protect content in third-party applications such as Salesforce Box or Dropbox. Sensitivity labels can also be applied at the container level, so for a full Microsoft 365 Group, a Microsoft Team, or a SharePoint, or OneDrive for Business site. Some of the container-level settings that you can apply is the group, for example, can it be public or private only? Are external users allowed or not? Is access to this container from unmanaged devices allowed or not? When configuring a sensitivity label, the administrator will be able to decide the scope of the label, if it's manually or automatically applied, as well as the different encryption, permissions, and content marking settings for content tagged with that label.

Retention Policies and Records Management

Next up, we have retention policies. Retention policies help you to more effectively manage the information in your organization. Use retention policies to keep data that's needed to comply with your organization's internal policies, industry regulations, or legal needs, and to delete data that's considered a liability or that you're no longer required to keep, or maybe it has no more legal or business value. Retention policies can be applied to multiple Microsoft 365 services, such as SharePoint Online, OneDrive for Business, Microsoft Teams, and of course, Microsoft 365 groups, which can be a container for multiple other services. If we go a bit more in depth in the retained data aspect of it with retention policies, you can ensure that data is retained for a specific period of time, regardless of what happens in the user app. So, even if a message is deleted by a user inside Microsoft Teams, that message will be held in the substrate and available for eDiscovery. You can also decide what to do with the data after the specified period of time with two choices. You can either do nothing, or delete the data. You can also use retention policies to simply delete data after a certain period of time, and this would permanently delete it from all of the storage locations on the service. Let's take an example with Microsoft Teams and see what we can do. There are three options for retention policies in Teams. First, retain Team chats and/or channel messages for a specified duration, and then do nothing. Second, retain Team chats or channel messages for a specific duration, and then delete the data. Or the last one, delete Team chats and/or messages after a specified duration. So those are kind of the three different combinations that you can do with retention policies to make sure that you keep the required data for as long as you're required to, and after that, if it becomes a liability or it has no more value, automatically delete it. Next up, we have records management. Records management is the supervision and administration of digital and paper records, regardless of format. Record management activities include the creation, receipt, maintenance, use, and disposal of records. Documentation may exist in contracts, memos, paper files, electronic files, reports, emails, and a ton of other both physical and digital records. Now, as you hear that, you might be thinking, wait, Vlad, isn't this kind of the same thing as retention policies? Well, it's close. And I mean from a technical point of view, Records Management and Microsoft 365 actually leverages retention policies. However, the behavior is different from a user experience and feature point of view. With retention labels, when something is deleted, for example, Microsoft keeps a copy of that content hidden from the user, either in the substrate or in a hidden folder where it's available for eDiscovery, but the user can still delete it from the end user interface. Records management also block actions in the user interface for the user so they simply cannot delete it. And in this module we're really doing an overview of the feature without diving too deep in the technical properties, but with records management, you can even make it so that even a global admin is not allowed to delete a record, and that global admin cannot even change the record settings to make that record delete faster. So you have quite a lot of power with records management in order to make sure that your compliance standards are followed no matter the permissions of the admin that's trying to do something.

Microsoft Purview Data Loss Prevention

Next up in our list of information protection tools, we have Microsoft Purview Data Loss Prevention. Data Loss Prevention, or DLP, is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. When we talk about sensitive data, we are talking about data such as credit card numbers, Social Security numbers, passport numbers, and so on. With Microsoft 365, you can also create custom sensitive information types that are relevant to your business, so maybe a client case number or a patient number, and be able to detect those.

Data Loss Prevention can identify information across multiple services, such as Exchange Online, SharePoint Online, OneDrive for Business, as well as Microsoft Teams. Microsoft Purview Data Loss Prevention is even able to find information outside Microsoft 365 services for things such as On-Premises SharePoint Server or file shares that you may still have on-premises. You can create multiple Data Loss Prevention policies inside your tenant and for each one, select the type of sensitive information that you want to detect, where to look for that information, and, of course, what action to take if sensitive information is found. You could simply show a pop-up warning to the user saying, like, hey, this seems to contain sensitive information, make sure it's okay that you're sharing this. You could also block the sharing of that content or even lock that content and move it to a safe quarantine location until it's checked by an administrator. You could, of course, have multiple policies with different actions depending on the type of sensitive information. If we take a look at an example inside Microsoft Teams, you can see that John Smith shared a list of credit card numbers inside the channel. However, because there was a DLP policy in place, this message got blocked right away. From the other user's point of view, we simply see that this message was blocked due to sensitive content. This is the goal of Data Loss Prevention, making sure that sensitive data is not shared in places where it shouldn't be. And if it is, you can block it automatically. The message owner can get it unblocked in case it's a false positive, but mainly the goal is to prevent the sharing of sensitive information and data leaks.

Microsoft Purview Insider Risk Management

Next up on our list of compliance solutions is Microsoft Purview Insider Risk Management. The goal of Insider Risk Management is to help detect, investigate, and take action to mitigate internal risks in your organization, from scenarios including data theft by employees, the intentional or unintentional leak of confidential information, offensive behavior, and more. Some insider risk scenarios that you need to protect yourself from can be leaks of sensitive data and data spillage, intellectual property theft, insider trading, fraud, confidentiality violations, or regulatory compliance violations. So, how does the general Insider Risk Management workflow look like? With Microsoft 365 Insider Risk Management, we usually split this into five steps. First, policies must be created. What do you want to protect yourself against or monitor? We then have the alerts that will come from those policies, which we then need to go into triage, really figure out which one is important, which one is not. Machine learning and artificial intelligence will always do a good job at evaluating risk levels and what should be an alert, but manual triage will always be needed. After triage, an investigation needs to happen. Maybe someone did download 100 documents from SharePoint, but they wanted them offline, as they needed to work on them during a long flight. This is, of course, something that will be a case-by-case basis, as is the action, which is our last step. The whole process isn't done by IT, but it's important that it's a collaboration between your compliance, human resources, legal, and security teams together. Things such as intellectual property theft, for example, can end up in courts, and the process on how proof is gathered is a very important part, so this should never be an IT-only task. If we take a look at a pre-built policy in Insider Risk Management in Microsoft 365, we have data theft by a departing user. It does have a few optional prerequisites in there, such as, for example, knowing when the employee is leaving by connecting it to your HR solution, or even knowing what physical locations the employee accessed. You can see the trigger event, as well as detected activities in Microsoft 365, such as downloading files from SharePoint, printing files, or copying information to, let's say, a personal Dropbox or USB key. Now, if we move to alerts, on this page, you will see all of the different alerts, and as you can see, you can even see the users as anonymous at this stage so there is no bias at all in the way that administrators handle alerts. We then have the triage where we analyze alerts, and if needed, create a case out of them. We can see what potential insider risk action was taken and the activities that triggered it. We can then group activities in a case and investigate it, and we have information on the user activities on the past six months, so we can see what activities they did that triggered the alert. We have case notes, and we can also explore the content that they interacted with. After we investigate, we can take multiple actions, which, again, remember to take together with your HR and legal team, as those can range between sending a notice to the employee to maybe sending them for refresher training, or you can transfer them to eDiscovery premium to start creating a legal case on that employee.

Microsoft Purview eDiscovery

The next compliance tool we will cover is Microsoft Purview eDiscovery. Before talking Microsoft specific, let's talk about eDiscovery, in general, as an industry term. Electronic discovery, mostly called eDiscovery, is the electronic aspect of identifying, collecting, and producing electronically stored information in response to a request for production in a lawsuit or investigation. Electronically stored information includes, but is not limited to, emails, documents, presentations, databases, voicemail, audio and video files, social media, and websites. Electronic discovery is made of six stages, first one being identification. The identification phase is when potentially responsive documents are identified for further analysis and review. Next up, we have the preservation stage. During preservation, data identified as potentially relevant is placed in a legal hold. This ensures that that data cannot be destroyed. Once documents have been preserved, collection can begin. Collection is the transfer of data from a company to their legal counsel who will determine relevance and disposition of data. Our fourth stage is the processing stage. During the processing stage, native files are prepared to be loaded into a document review platform. Often, this phase also involves the extraction of text and metadata from the native files. We then have our review stage where specific documents are reviewed, and only data that is relevant to the the case is kept. Lastly, the production phase is where documents are exported in their native format or in an industry-standard format and turned over to opposing counsel. Those are the basic stages of eDiscovery, but now let's see why that is relevant for us in the Microsoft World. Microsoft actually has three tools for eDiscovery, first one being Content search. Second one is eDiscovery (Standard), which was previously called Core eDiscovery. And the third one is eDiscovery (Premium), which was previously called Advanced eDiscovery. What is the big differences between them from a functionality purpose? It's all about the features. The Content search is the most basic one and can help you with the identification and collection stages. EDiscovery (Standard) helps you with the identification, preservation, and collection stages. And finally, the eDiscovery (Premium) can help you with all six stages. You might ask yourself why does Microsoft have three tools when they have one that can do it all? If your guess is licensing, you are correct. The more features, the more licensing is required.

Demo: Content Search

Now that we have seen the theory, let's head over to the lab and check out content search in action. I am now in the lab environment. Let me open up the browser here where I'm back in the compliance portal, and under Solutions, let's take a look at Content search. What I will do for this demo, let me go and create a new search, and for this demo, we will search for project CT-123, and let's take a look, we'll call it CT-123 Leaks here. We can enter a description. Let's click on Next. And then we need to tell content search where to search. For this demo, I will say look in the exchange mailboxes, in the SharePoint sites, and public folders, and I can also choose which ones. Maybe I'd want to search everything else, except the site in the team where those conversations should be. So we can decide what services to search in, as well as what specific sites, teams, and mailboxes we want to filter for this search. Now let me click on Next here. Now I have my conditions. What do I want to search? For this demo, I'll just search for the keyword CT-123. I can also add more conditions, such as the Sender, Subject, File type, things like that. We will keep it simple. Let's click on Next. We have a summary of everything we have configured, and now let's click on Submit. After we click on Submit, my search will be created. It shows up over here, and as you can see on the status, this search is starting. So what I will do now is I will pause the recording for the 2-5 minutes I will take for this search to finish. It might take longer depending on how much content you have, but in this demo tenant, I do not have a lot of content, so it should be quite fast. Great! So, it just finished. So let me take a look and let's take a look at the items that it found. So it will take a few seconds to load again, shouldn't be too long. But if everything goes fine, we should have some teams' messages in here that content search has found. There we go, it finished loading, and here's an example that we see from a team's message. I have Hello Vanessa, don't tell anyone, but our new product called CT-123 will launch end of September. So I was able to find this message in a team's chat, and as you can see, the keyword is highlighted in here. So this is an example of an eDiscovery tool, the most basic one in Microsoft's eDiscovery solutions, but this gives you an idea of how you're able to find all of the content that relates to a topic that you might need for a legal case. This is it for this demo. Now let's head back to the slides and talk about Microsoft Purview audit.

Microsoft Purview Audit

Last, but not least in our compliance tool belt is Microsoft Purview Audit. The way that I always joke about it is that every step you make, every breath you take will be saved in the Microsoft Unified Audit Log. The unified audit log is a centralized audit log that contains activities from almost all the Microsoft 365 products in a single location. The information is kept in there for a maximum of either 90 days or 10 years, depending on the user license. Microsoft also has APIs that allow you to export audit logs into your own systems if you need to and want to keep it for longer than that. If you have smaller needs for a specific part of the audit log, you can also simply export it to a CSV file. If we take a look at an audit log example, you can see different fields, such as date, which is in UTC format, the IP address of the device that was used when the activity was logged, the user or service account that did the action, in this case, it was vlad@globomantics.org, and I can also see the activity, so in this case, I performed a search query. One of the nice features of the unified audit log is that you can also configure alerts based on activities in the audit log. This allows you to be more proactive when certain actions happen in the organization. I mentioned licensing a bit earlier, so let's talk a bit about that. Microsoft also offers Microsoft Purview Audit (Premium), which requires extra licensing, but it gives us three main features, long-term retention of audit logs for up to 10 years, as well as access to more events in the audit log, such as when a mail message is read, or even when somebody searches for something in a mailbox. Audit Premium also gives us more high-bandwidth access to the Office 365 Management Activity API, allowing us to export unified audit logs or analyze them through the API without being throttled.

Demo: Microsoft Purview Audit

Now that we have seen the theory, let's head over to the lab and check out the unified audit log. We are now back in the lab environment. Let me open up the browser here where we are in the compliance portal. Under solutions on the left, I will click on Audit, and then it will take a few seconds, but I will be able to add all my different filters. For example, what is the date and time range that I want to search? Are there any activities in particular that I'm looking for? For example, accessed a file, deleted a file marked as a record, discarded a file checkout, or deleted a file. You can really search, for example, if I search for a message, I will be able to see all the activities that have to do with a message in Exchange, Teams, and so on. So really, you have a ton of different filters in order to find the content that you want because if not, you will have a lot of noise in there. The ones that I use the most often are usually the file, folder, or site. So if you're looking for something in SharePoint, you can, for example, put the site URL in there to only see the information on that site, or specifying a user name. So if you add the user's name, you'll see everything that they did. Now, I already created a search a bit earlier in the interest of time, as it takes a few minutes for it to be done, where I just put from September 6 to September 7 everything that happened, no filters. We see that a lot of them are vlad@globomantics.org logging in. We can even see, for example, the MFA user log in that we did a bit earlier today, and you can also have, for example, the no more passwords. Remember in the identity module demo, we logged in using password-less with the NoMorePasswords@globomantics.org login name, and the operation failed. It got saved here inside the audit log. I can also see that, for example, Vlad viewed a list here, and I have the item ID. I really can see everything that I viewed, I changed, and the same thing for everybody in my tenant. This is it for this quick demo of the unified audit log. Here is where you go to find what happened in the past, whether it's a login, accessing a page, or a document, or deleting some content, everything is saved in here. And depending on the license that you have, you'll be able to access it for between 90 days and 10 years. This is it for this demo. Now let's head back to the slides and finish off this module.

Module Conclusion

To finish off this module, let's review what we have learned. We have first started this module by doing an introduction to regulatory compliance as an industry term to really understand what it means. We have then learned about the six Microsoft privacy principles, which are control, transparency, security, strong legal protections, no-content based advertising, and finally, benefits to you. Next, we learned about the Microsoft Service Trust Portal and how it can help us. With the basics out of the way, we start diving deep into Microsoft Purview, Microsoft's suite of cloud-compliance solutions. And we have learned about the Compliance Manager, which also includes the compliance score, information protection, Data Loss Prevention, Insider Risk Management, eDiscovery, as well as auditing in Microsoft 365. This is it for this module, which is almost the last module of this course. But before we're done, we have a small course conclusion module where we will recap everything that we have learned in this course and share more resources to learn about security, compliance, and identity in the Microsoft cloud.

Safeguard and Respect Privacy with Microsoft Priva

Module Introduction

Welcome to the next module of this course in which we will learn how Microsoft Priva can help us safeguard and respect privacy in our organization. This module will be all about introducing Microsoft Priva and its two different solutions, which are Priva Privacy Risk Management and Priva Subject Rights Requests. And we will learn how each one of them can help. By the end of this module, you understand how Microsoft Priva can help your compliance team be more efficient when it comes to privacy and personal information.

Introduction to Microsoft Priva

Let's start by doing an introduction to Microsoft Priva, and let's start with a nice definition by Microsoft. Microsoft Priva helps companies safeguard personal data and build a privacy-resilient workplace by proactively identifying and protecting against privacy risks such as data hoarding, data transfers, and data over sharing, empowering information workers to make smart data handling decisions and automated and managing subject requests at scale. We know that Priva wants us to build a privacy-by-default organization. But if we dive down into how it helps us, first of all, proactively identify and protect against privacy risks such as data hoarding, problematic data transfers, and data over sharing. It will help us gain visibility into the storage and movement of personal data and something that I really like a lot is empower employees to make smart data handling decisions and truly empowering the business users to do more without having the compliance and privacy team take 100% of the task. Finally, Priva helps us manage subject rights requests at scale instead of manually doing each one of them. Microsoft Priva has two main solutions that help us achieve all of that. They are Priva Privacy Risk Management and Priva Subject Rights Requests. From a licensing point of view, Microsoft Priva is only available as an add on, so it's not included into any other Microsoft 365 licenses. And each one of the two solutions I shared earlier are licensed separately and they each have their own licensing model. As always, make sure to check with your licensing professional as licensing can often change.

Priva Privacy Risk Management

Now that we know about the suite, let's dive deeper into each solution, starting with Priva Privacy Risk Management, which gives you the capability to set up policies that identify privacy risks inside your Microsoft 365 environment and enable easy remediation. Privacy risk management has three key areas, first to limit data overexposure, second to find and mitigate data transfers, and third, to minimize stored data. Let's dive deeper. First of all, we have the Privacy Risk Management dashboard, which provides us an overall view into your organization's data in Microsoft 365. Privacy administrators can monitor trends and activities, identify and investigate potential risks involving personal data, as well as build policies. Talking about policies, let's talk about our first feature, limiting data overexposure. Microsoft Priva allows you to create policies that detect if personal data is accessible by too many people. For example, if it's in a site that it's too open and you can either only alert admins or the part that I love is that you can directly engage content owners and let them take the action themselves as we can see in the screenshot on the right where Sam Davies received an email about a document that contains credit card numbers that is too broadly accessible. And then Sam can either make it private or keep it the way it is and provide a justification why. You can also provide training directly in that notification, which is, of course, something that I love. Next up, let's talk a about finding and mitigating data transfers. Truth is that transferring personal data can create a big privacy risk for an organization. Microsoft Priva allows you to create policies to monitor the transfer of personal data between departments or different world regions of your organization or between internal and external users. Those policies allow you to find and even limit personal data transfers, and you can, for example, automatically block messages in Teams that go against your policy. Finally, it helps organizations minimize stored data. From a legal point of view, keeping personal data of our customers that is no longer needed, for example, can create a privacy risk. Privacy Risk Management allows you to create policies that detect personal data that has been stored for a certain amount of time or that hasn't been modified in a certain amount of time. And it can either create an alert for privacy admins or engage the content owner directly so that he can check if it's still needed or not. Priva Privacy Risk Management works across Microsoft 365 and it can help detect data in Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.

Priva Subject Rights Requests

Next up, let's learn about Priva Subject Rights Request. The Microsoft Priva Subject Rights Request solution is designed to help alleviate the complexity and length of time involved in responding to data subject inquiries. Let's first of all learn about the problem that it's built to solve. Several privacy regulations around the world grant individuals or data subjects the right to make requests to review or manage the personal data that companies have collected about them. Those subject rights requests are also referred to as data subject requests or data subject access request or consumer rights requests. For companies that store large amounts of information, finding the relevant data can be a formidable task. Fulfilling the request for most organizations is a highly manual and time-consuming process. Microsoft Priva enables you to create a subject right request by simply providing the information of the data subjects such as name, residency, email, what is the relationship, so is it a customer or is it a current or former employee? And Microsoft provides multiple built-in templates based on the most popular requests such as data access, data export, or data deletion. The way that it works after is that Microsoft Priva will immediately kick off a data evaluation to help you collect all the data that might contain your data subject. And it will also help in prioritizing the content review by showing the most important content first with files that might include confidential data or files that might contain more than one person's data. Once you start the subject rights request, Priva will create a Team channel dedicated to collaborating on this request so you can easily collaborate with all the stakeholders in a single location. Finally, Microsoft Priva can help you automatically generate reports after you have identified the data needed, and it can include the data package that you will send to the data subject, audit logs, and more.

Module Conclusion

To finish off this module, let's review what we have learned. In this module, we learned about Microsoft Priva, a suite of two independent solutions that empower privacy teams to reduce risk and automate subject requests. We then deep dived into each one of them and learned how Priva Privacy Risk Management can help us limit data overexposure, find and mitigate data transfers, and minimize stored personal data, as well as how Priva Subject Rights Requests can help your privacy teams automate data subject rights requests to be able to do them at scale.

Course Conclusion

Course Conclusion

Hello, and welcome to the final module of this Microsoft 365 Security, Compliance, and Identity Concepts course. In this course conclusion module, we will do a quick review of everything that we have learned and share other courses which might be interesting for you to learn more about Microsoft 365. We started this course by learning one of the most important concepts, the shared responsibility model, because security in the cloud is a partnership, and there are always things that you are responsible for. The amount of things you are responsible for depends on the type of computing service that you have. In Infrastructure as a Service, you have more things to secure than in Software as a Service. But again, very important, there are always things that the customer is responsible for securing. We have learned about Zero Trust, a cybersecurity model with a very simple premise, eliminate the concept of trust from your network. And Zero Trust has three main guiding principles, verify explicitly, least privileged access, and assume breach. After we covered Zero Trust, we went into identity and learned first of all about the basics, which are authentication and authorization and what is the role of each one of those processes. We have then learned about the concept of modern authentication and the role of the identity provider in the Microsoft ecosystem. And we have also learned about both Microsoft Active Directory and Azure Active Directory, probably the most popular directory service in the world, and how they can help you with authentication and authorization, whether your on-premises, in the cloud, or have a hybrid setup. As this is a cloud course, we have then focused on Azure Active Directory and looked at the different authentication methods from standard username and password to multi-factor authentication and even passwordless. We have also learned about Azure AD Conditional Access, a feature that sits between the authentication and authorization stages and allows us to verify every attempt and depending on a set of signals, accept authentication attempt, require something, or deny it. We have then switched over to threat protection solutions and first of all, learned about the industry terms, SIEM, SOAR, and XDR, which are categories of threat management tools to make our security teams more productive. We have then learned about what Microsoft tool goes into what category, and we have learned about the different products part of the Microsoft 365 Defender Suite, as well as Microsoft Sentinel, a SIEM and SOAR solution that can help us collect data with over 100 built-in connectors, discover incidents, and automatically respond with playbooks. After talking about threat management, we moved on to compliance, which similar to security in the cloud, it's a partnership between the cloud provider and you, as some compliance configurations will still always depend on you. Our first topic was Microsoft's six key privacy principles, which are control, transparency, security, strong legal protections, no content-based targeting, and benefits to you, which outline Microsoft's guiding principles for managing your data. And we have also learned about the Service Trust Portal, a single location where you can find audit reports, Pen Tests, Security Assessments, and more information on how Microsoft manages security, privacy, and compliance. Afterwards, we have covered multiple compliance solutions, part of the the Microsoft Perview suite of compliance products that help us achieve our compliance goals. And we have talked about the Compliance Manager, the compliance score, Information Protection, Data Loss Prevention, Insider Risk Management, eDiscovery, and Audit. So we have covered the most important products that apply to compliance in Microsoft 365. With the overview done, what's next? If Microsoft 365 is your passion, you can work towards a Microsoft 365 certification, and the first one I would recommend is the Microsoft 365 Certified: Fundamentals certification. It's a fundamental level certification where you can prove that you understand the options available in Microsoft 365 and the benefits of adopting cloud services, the Software as a Service model, and implementing Microsoft 365 cloud services. The exam number is MS-900, and you can find more information about the exam on Microsoft Learn at the link in the slides. And there's also a certification path on Pluralsight dedicated to this certification. What I love most about this certification is that since it's a fundamentals level certification, you don't need to be an IT pro or a developer. It's really aimed at everybody. Whether you're a presales, a business analyst, or just getting started in IT, it shows your passion and upscaling in understanding the value of Microsoft 365 and knowing the solutions inside, so I highly recommend that you take a look at it. If your passion is more focused on security compliance and identity solutions, Microsoft has a full certification portfolio focused on just that with four different certifications inside. If you haven't done it yet, I highly recommend starting with the SC-900 certification exam, the Security, Compliance, and Identity Fundamentals certification, which is targeted to those looking to familiarize themselves with the fundamentals of security, compliance, and identity for both Microsoft 365 and Azure. There is a certification path on Pluralsight dedicated to the SC-900 exam as well. This is it for this course. Before we're done, I'd also like to introduce you to a really nice feature on Pluralsight. You can now follow authors on Pluralsight, so if you have enjoyed this course and want to get notifications when I create new content, please go to my profile and click on Follow. On the last note, I just want to say a huge thank you for listening to my course. I really hope you have enjoyed listening to it as much as I enjoyed creating it. You have my Twitter, LinkedIn, blog, and YouTube channel out there. I do my best to create interesting content. And if you ever see me speak at one of the conferences you're attending, don't be a stranger, and come say hi. Thank you very much again for listening to this course.