SCM

Due diligence is a legal principle that says the subject has used best practice or reasonable care when setting up, configuring, and maintaining a system. When you're trying to hire a vendor, you need to ensure that they have done due diligence on their supply chain and you need to do your due diligence on them.

This includes things like ensuring that their cybersecurity program is properly resourced. You also want to make sure that they have security assurance and risk management processes and programs in place. And by doing this, this will help make sure that they have a valid organization and a way of doing due diligence within themselves. Another thing you want to look at is the product support lifecycle. If you're going to buy a product, you need to make sure that they're going to be able to support it for the long term.

If you're giving them access to your data because they're doing something like Software-as-a-Service, you want to make sure they have the proper security controls in place to ensure your data remains confidential. Another thing you have to think about is when things go wrong, will they be there to help you? If you have to conduct an incident response or do forensic investigations, will that company be able to support you and provide you assistance?

Trusted Foundry

Now, one of the organizations that has a very low tolerance or low risk appetite for hardware is the Department of Defense, and so they create something known as the trusted foundry. Now, the trusted foundry is a microprocessor manufacturing utility that's part of a validated supply chain, one where the hardware and software does not deviate from its documented function. And again, this was created and operated by the Department of Defense, which is the US military because if they're going to put up a microprocessor to run a jet or a bomb or something like that, they want to make sure it does exactly what it's supposed to do each and every time.

Root of Trust

In this lesson, we're going to talk about the concept of a hardware Root of Trust or ROT.
Now, this is a cryptographic module embedded within a computer system that can endorse trusted execution and attest to boot settings and metrics.

If you think about your TPM module inside your BIOS, that is a root of trust.

TPM

You really need to remember that TPM, the trusted platform module, is this part of your system that allows you to have the ability to ensure that when you're booting up, it is done securely and we can take those reports and digitally sign them using the TPM.

Now, when you're dealing with TPM, your TPM can be managed inside of Windows using TPM.MSC, which is a console or you could do it through group policy.

HSM

This is an appliance for generating and storing cryptographic keys that is less susceptible to tampering and insider threats than using storage-based solutions.

Anti-Tamper

These are methods that make it difficult for an attacker to alter the authorized execution of software. Now, if you think about anti-tamper and you think about the physical world, you buy a thing like aspirin and you open up the bottle. What do you see on top? That sealed layer that says this has been protected, this is sealed for your protection.
This is an anti-tamper device.

And there are two main ways of doing that. We have anti-tamper mechanisms that include things like an **FPGA**, which is a Field Programmable Gate Array or a physically unclonable function or **PUF**.
Both of these are anti-tamper mechanisms that could be used and designed inside your systems.

This means that if somebody tries to tamper with the system, what these things will do is actually zero out your cryptographic key, which then can automatically wipe out

the information on that system, making sure you know it's been tampered with and therefore, nobody can get the information.

Trusted Firmware

Now, as I talk about trusted firmware, we have to think about the idea of a firmware exploit because we're trying to prevent firmware exploits by using trusted firmware. A firmware exploit is going to give an attacker an opportunity to run any code at the highest level of CPU privilege. Because if you're at the firmware, for instance, in the BIOS or the UEFI, you can actually have essentially a rootkit that runs over the entire system, and that's loaded even before Windows is. So, your anti-malware is not going to find it.

Terms to cover:

1. UEFI
2. secure boot
3. measured boot
4. attestation
5. eFuse
6. trusted firmware updates
7. self-encrypting drives

UEFI

Unified Extensible Firmware Interface or UEFI. This is a type of system firmware providing support for 64-bit CPU operations at boot. It also gives you a full GUI and mouse operations at boot and better boot security.

To be able to run a lot of the other things we're going to talk about in this lesson, you have to have UEFI and not BIOS for your system.

Secure Boot

This is a feature of UEFI that prevents unwanted processes from executing during the boot operation. Essentially, as a computer is booting up, it's going to check things and make sure that there's digital signatures installed from those operating system vendors. If Microsoft Windows isn't signed by Microsoft, we're not going to boot it.

Measured Boot

Now, a measure boot is a UEFI feature that gathers secure metrics to validate the boot process in an attestation report. So, as you're booting up, it's going to be taking different measurements, how much time does it take for you to do this? How much process should it take to do that, and based on that, it's going to collect that data, it's going to create a report, and then it's going to attest to it. Which brings us to the idea of attestation.

Attestation

Now, an attestation is a claim that the data presented in a report is valid, and it does this by digitally signing it using the TPM's private key. So, the UEFI, it's going to take that report, it's going to sign it with that digital key, and then send it on to the operating system into the processor. This way we know we can trust it.

eFUSE

Now, eFuse is a means for software or firmware to permanently alter the state of a transistor on a computer chip. Now, this comes from the idea of a fuse. If you've ever worked with electricity before, and you've worked in a breaker panel, you may have seen things like these, these are fuses.

Trusted Firmware Update

So, when we have a trusted firmware update, this is a firmware update that is digitally signed by the vendor and trusted by the system before it's installed. Anytime you're going to go and do a firmware update, you need to make sure that it is trusted because if it's trying to do something that's not trusted, you have the potential to blow one of these eFuses that we just talked about.

Self Encrypted Drive

The idea with these self-encrypting drives is that they have firmware on them that is used to do the encryption when data is being written to the drive. It also decrypts that information when data is being read from the drive. All of this is done at the hardware level, so it takes the processing load off of your own computer and off of your operating system, because it's all done here in the firmware.

Secure Processing

Now, when we talk about secure processing, this is a mechanism for ensuring the confidentiality, integrity, and availability of software code and data as it's executed in volatile memory. Because after all, we're going to take data off of our hard drive or off of our network and we're going to put it into RAM and then from RAM into our processor. And all of that time going from RAM to the processor or while it's stored in RAM, has the potential for it to be modified or for it to be stolen or for it to be not available.

Processor Security Extensions.

Now, these are low-level CPU changes and instructions that enable secure processing. And these are built into your microprocessor. Now, they're called different things depending on if you're using an AMD or an Intel processor. If you're using an AMD processor, this is known as Secure Memory Encryption (SME) or Secure Encrypted Virtualization (SEV). On the other hand, if you're using Intel processors, you're going to be using Trusted Execution Technology or TXT or Software Guard Extensions (SGX).

Trusted Execution

The CPU's security extensions invoke TPM and a secure boot attestation to ensure a trusted operating system is running. So, any time we want to boot up the system, we want to make sure that we are using that trusted firmware using UEFI and using TPM and secure boot to tell us that this operating system that's being booted is something we trust.

Secure Enclave

Now, a secure enclave is an extension that allows a trusted process to create an encrypted container for sensitive data.
This will help us prevent things like buffer overflow attacks, and typical application usage here, we'll be able to store encryption keys and other sensitive data inside of the secure enclave.

Atomic Execution

Now, there are certain operations that should only be performed once or not at all. For example, initializing a memory location. This should only happen one time, right? And so, once you've initialized it, that should be it. Well, the idea of atomic execution is there are these extensions in place to make sure somebody can't reuse or hijack an atomic execution operation like doing a memory initialization. This can help you prevent buffer overflows and race conditions by being able to control these processes and again, this is something that's built into those processors these days.

Bus Encryption

Now, bus encryption is data that is encrypted by an application prior to being placed on the data bus. This will ensure that the data being sent over the network or over a bus is going to be protected because it's going to end up as encryption. Now, for this to work, we have to ensure the device at the other end of the bus is trusted to decrypt that data.