Juliana's story: Asset protection

Meet Juliana Soto, who recently completed an online cybersecurity certificate program and was hired as a cybersecurity analyst for Right-On-Time Payment Solutions, a fictional payment processing company allowing individuals to transfer money to friends and family. Right-On-Time also allows companies to accept payments from customers or organizations.

In this reading, you will begin a three-part journey that follows Juliana as she takes on new roles and responsibilities within the cybersecurity team of her new company.

Juliana decides that one of her first objectives is to gain a better understanding of the most important assets to the company by reviewing various company reading materials that will help her learn what is most valuable to them. On her first day, she is given reading materials to help her familiarize herself with the company. She learns that customers must create unique usernames and passwords and provide their full name or company name to sign up for the service as an individual. Business customers can also sign up for the service if they provide their employee identification number (EIN). Finally, customers must enter their bank account information or debit card number for payments to be accepted.

Juliana discovers that this company handles a lot of personally identifiable information (PII) from its customers. This kind of information is considered sensitive data. Unauthorized access to it can lead to significant damage to the organization’s finances, its customers, and its reputation. Juliana realizes that the most important asset to this company is customer data.

After finishing the required onboarding materials, she decides to put together an information lifecycle strategy. She learned about this when completing her online cybersecurity certificate program.

Information lifecycle strategy

Juliana recalls the following steps of the information lifecycle:

- The first step in the information lifecycle is to identify the important assets to the company, including sensitive customer information such as PII, financial information, social security numbers, and EINs.
- The second step is to assess the security measures in place to protect the identified assets and review the company’s information security policies. There are different components to this step, ranging from vulnerability scanning to reviewing processes and procedures that are already in place. Juliana is new to the company and might not be ready to conduct vulnerability scans.

- The third step of the information lifecycle is to protect the identified assets of the organization. Once again, this is only Juliana’s first day on the job. She asks her supervisor if she can observe a more senior security analyst for a day. This will give her the opportunity to learn how the security team monitors the company’s systems and network.
- The last step of the security lifecycle is to monitor the security processes that have been implemented to protect the organization’s assets. She contacts her supervisor and gives them a detailed report of what she has learned on her first day. She requests to finish her day by monitoring a few of the systems that are in place. Her supervisor is impressed with her initiative and prepares Juliana to monitor the security systems. What a great first day for Juliana!

Key takeaways

Identifying the important assets of a company is a key security analyst responsibility. Once you identify the assets, it can be helpful to follow the information lifecycle strategy to help ensure those assets are being protected effectively. Reviewing a company’s security policies will also help an analyst understand what is important to the company and how the analyst should be protecting that data.

Revision #1
Created 2024-01-07 11:35:32 UTC by naruzkurai
Updated 2024-01-07 11:35:42 UTC by naruzkurai