Date: July 3, 2024	Entry #1
Description	1. **Detection & Analysis**: Using the Nessus vulnerability scanner tool, it found numerous critical features of the software containing vectors of attack for potential bad actors. The organization contacted its own response team to find a solution to the zero day threats. 2. **Containment, Eradication, Recovery:** The company had the blue team pull down the computer network and recover the operating system from an onsite backup they had just in case. There they found the problematic software and isolated it and got rid of the malware contained within.
Tools	Nessus Vulnerability Scanner, Virtual Machines, Firewalls
5 W’s	**Who:** A group of unethical hackers and insider employees **What:** A malware from depreciated software duplicated itself on the operating system. **Where:** A lawyer Firm **When:** July 3, 2024 at 10:00 AM **Why:** Some older software was downloaded and used from the archives of the internet. The program used was an older version of Mozilla Firefox which is open to the public to be used by anyone. Unethical hackers have sent tampered downloads of the software over the internet, which an employee used without permission. Alongside the software the virtual machine and Microsoft Office programs seemed to be infected and information seemed to have been taken about the company’s new products ready to be shipped.
Risk Analysis & Solutions	The employees of the company must be reminded and retrained in the proper behavior on how to use the assets of the company. This will result in less systems being hit by malware. They must also be trained in internet etiquette and not to click on suspicious links and notify the IT team beforehand. Establish a policy to upload finished documents to the cloud to always have a working backup copy in case we ever have this situation ever again. In the future the company will just pick up work from another computer from anywhere they like. The Blue team will have to run Antivirus scanners more often to have a better chance of detecting malware in the future and make room for more virtual machines so actual assets are not endangered going forward.

	The IT admin must update permissions of power users to never allow employees to download specific software in computer’s options

Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

Controls assessment checklist

Control:

Least Privilege (NO)
Disaster recovery plans (Yes)
Password policies (NO)
Separation of duties (YES)
Firewall (NO)
Intrusion detection system (IDS) (NO)
Backups (YES)
Antivirus software (NO)
Manual monitoring, maintenance, and intervention for legacy (YES)
Systems (YES)
Encryption (YES)
Password management system (YES)
Locks (offices, storefront, warehouse) (YES)
Closed-circuit television (CCTV) surveillance (NO)