SOPRANOS CORP.

Security Incident Response Tabletop Exercise

Document ID	**SEC-TB-01**
Department	Corporate
Process Owner	Information Security Manager
Approved Date	22 August 2022
Pages	**1 of 3**
Record ID	**YYYYMM-[Dept]-[Usage]-xxxx**

Security Incident Response Tabletop Exercise

Exercise Name	Backdoors and Breaches, an Incident Response Card Game		
Exercise ID	2022.08-001		
Business area	Information Security & Privacy		
Plan owner	Paulie.G	**Position**	Cybersecurity Architect & Policy Officer (CAPO)
Plan coordinator	Paulie.G	**Position**	Cybersecurity Architect & Policy Officer (CAPO)

Describe Exercise:

Core team members work together to respond to a cybersecurity event. The team must work through the company's outlined processes and procedures to discover how the cybersecurity event occurred. The goal is to help prepare the team members for a cybersecurity event and identify procedural or technical gaps.

Backdoors and Breaches is a card game that crafts cyber-breach scenarios. An IT Team will then need to conduct an incident response to the breach scenario. The answers given by team members in the game should be specific to the company and its incident response capabilities.

URL: https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

Areas For Improvement

- Train Bobby.B, and Junior.S how to access Sentinelone(S1) and review logs.
- Desktop build process needs a Security software SOP.

Lessons learned

- More team members must learn and practice using the Sentinelone web-admin tool.
- There is no verification process to ensure Desktop systems have AV installed and active.
-

SOPRANOS CORP.

Security Incident Response Tabletop Exercise

Document ID	**SEC-TB-01**
Department	Corporate
Process Owner	Information Security Manager
Approved Date	22 August 2022
Pages	**2 of 3**
Record ID	**YYYYMM-[Dept]-[Usage]-xxxx**

Turn	Roll	Notes
1	9	Call a Consultant – Failed roll No one wants to associate with Sopranos Corp. New risk identified.
2	14	Firewall Log Review – Successful Roll We discovered the initial compromise!
3	19	SIEM Log Review – Successful Roll Found the attacker's Backdoor!
4	2	Network Threat Hunting – Failed roll
5	5	Firewall Log Review – Failed Roll Firewall logs were not large enough for the timeline of the breach.
6	17	Endpoint Security Protection Analysis – Successful Roll Did not turn up any new information. Bobby.B, and Junior.S don't know how to use S1
7	16	Server Analysis – Successful Roll Discovered Pivot and Escalate method!
8	11	Endpoint Analysis – Successful Roll Did not turn up any new information. The Desktop systems did not have AV installed and active.
9	14	Network Threat Hunting – Successful Roll Discovered Data Exfiltration method!
10	NA	NA

SOPRANOS CORP.

Security Incident Response Tabletop Exercise

Document ID	**SEC-TB-01**
Department	Corporate
Process Owner	Information Security Manager
Approved Date	22 August 2022
Pages	**3 of 3**
Record ID	**YYYYMM-[Dept]-[Usage]-xxxx**

Participant Name	Participant Signature	Date
Tony.S	*Tony Soprano*	1/10/99
Paulie.G	*Paulie Gualtieri*	1/10/99
Christopher.M	*Christopher Moltisanti*	1/10/99
Junior.S	*Corrado Soprano*	1/10/99
Silvio.D	*Silvio Dante*	1/10/99
Bobby.B	*Bobby Baccalieri*	1/10/99