Identification and Investigation

LOG #	OBSERVATIONS	SECURITY IMPLICATION(s)
3	Successful Login @ 8:10:23 AM EST Using RDP (logon type 10), they logged in as user JohnDoe on DESKTOP-1234567 Login GUID 0 = no GUID for the login session => less traceability for the logon session Logon was initiated from IP address 192.168.1.2 port 50215 SYSTEM (using winlogon.exe process) processed user JohnDoe's RDP logon	
5	Successful policy change by User ADMINISTRATOR on computer DC-SERVER-01 @ 9:45:32 AM EST They created a new file or folder	
10	Failed Login @ 10:32:17 AM EST on DESKTOP-1234567 (IP address 192.168.1.100) Tried to login as user "admin" but failed due to bad username or password Logon was initiated from IP address 192.168.1.100 port 50789 Logon type 3 = network logon (logon from within same network usually)	port scanning
11	Failed Login @ 10:32:19 AM EST on DESKTOP-1234567 Tried to login as user "admin" again but failed due to bad username or password Logon type 3 = network logon (logon from within the same network usually) Logon was initiated again from IP address 192.168.1.100 port 50791	port scanning
12	Successful login @ 10:32:21 AM EST on DESKTOP-1234567 Logged in as user "admin" Logon type 3 = network logon Logon was initiated again from IP address 192.168.1.100 port 50793	port scanning + privilege escalation (normal user JohnDoe => admin)
13	Firewall warning @ 10:33:45 AM EST on DESKTOP-1234567 Event category 2 = logon Event id 2004 = successful Logon initiated from IP address 192.168.1.100 to IP address 192.168.1.1 using TCP protocol at port 445	Indicates use of SMB protocol - file sharing or reading/updating files on remote system possible prep for lateral movement
1	Application error @ 12:01:15 PM EST on DESKTOP-1234567 Attempted to access Windows Explorer Exception Code 0xc0000005 = access violation	access violation
6	Firewall warning @ 1:23:15 PM EST on DESKTOP-1234567 Event category 2 = logon Event id 2004 = successful SSH login from IP address 192.168.1.125 to IP address 192.168.1.1	
7	Error @ 2:10:12 PM EST on SERVER-12345 User DESKTOP-1234567/JohnDoe attempted to use UDP at port 53 (not allowed)	possible attempt at data exfiltration in the guise of DNS queries as port 53 is typically for DNS queries
2	Warning @ 3:23:52 PM EST for MS SQL SERVER on SQLSERVER-12345 Error: 823, Severity: 24, State: 2 => MS SQL SERVER is having trouble reading data from disk (I/O error) Trying to read from mydatabase.mdf (primary database file wich contains schema and data)	database corruption
8	Failed logon @ 3:34:56 PM EST on DESKTOP-1234567 Tried to logon as user "admin" but failed due to bad username or password logon type 3 = network logon logon was initiated from IP address 192.168.1.50 port 50837	
9	Microsoft Windows Security warning @ 4:45:32 PM EST on SERVER-12345 Event Category 1280 = Windows Firewall settings or configuration issues Event id 5156 = network connection allowed by firewall Connection from IP address 10.0.0.2 port 12345 to IP address 10.0.0.1 (SERVER-12345) port 80 (Application unknown.exe	insecure connection between the two IP addresses (possible setup for exfiltration)
4	Failed logon @ 5:34:56 PM on SERVER-12345 logon type 2 = interactive login (physically at the system) tried to login as user "Admin" but failed due to bad username or password	

QUESTIONS FOR MANAGEMENT			
Is there a network topology diagram available to reference?			
What network access controls does the company currently have?			
Is only host-based monitoring implemented or are there network-based monitoring and logging systems in place?			
What is the company's password policy?			
Have employees undergone security awareness training?			