

Email Server:

Dec 14 08:00:00	Incoming Connection	18.8.10.10	224.189.69.101	220 Ready
Dec 14 08:00:05	EHLO Command	mail.mercifulredeemerchurch.com	EmailServer.SmartmeterCo.com	250 OK
Dec 14 08:00:10	MAIL FROM	micr0soft@microsoft.support.accounts.mercifulredeemerchurch.com		250 Accepted
Dec 14 08:00:15	RCPT TO	John@SmartMeterCo.com;		250 Accepted
Dec 14 08:00:15	Subject	{EXTERNAL} Office 365		250 Accepted
Dec 14 08:00:15	RCPT TO	Jack@SmartMeterCo.com;		250 Accepted
Dec 14 08:00:15	Subject	{EXTERNAL} Office 365		250 Accepted
Dec 14 08:00:15	RCPT TO	Vinod@SmartMeterCo.com;		250 Accepted
Dec 14 08:00:15	Subject	{EXTERNAL} Office 365		250 Accepted
Dec 14 08:00:15	RCPT TO	Mary@SmartMeterCo.com;		250 Accepted
Dec 14 08:00:15	Subject	{EXTERNAL} Office 365		250 Accepted
Dec 14 08:00:15	RCPT TO	Chillantra@SmartMeterCo.com;		250 Accepted
Dec 14 08:00:15	Subject	{EXTERNAL} Office 365		250 Accepted
Dec 14 08:00:20	DATA Command			354 Start mail input
Dec 14 08:00:25	Message Accepted			250 Message received
Dec 14 08:00:30	QUIT Command			221 Closing transmission

File Server:

Timestamp	User	Action	File Accessed/Modified	Result
Dec 14 10:30:25	John	Read	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 14 10:30:25	John	Update	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 14 10:30:25	Vinod	Copy	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 14 10:30:25	Vinod	Update	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 16 10:35:25	Chillantra	Read	/CriticalFileServer/HumanResources/EmployeeXMasBonuses.docx	Success
Dec 16 10:36:25	Chillantra	Update	/CriticalFileServer/HumanResources/EmployeeXMasBonuses.docx	Success
Dec 16 00:35:25	Chillantra	Read	/CriticalFileServerTopSecret/	Success
Dec 16 00:36:25	Chillantra	Copy	/CriticalFileServerTopSecret/	Success
Dec 16 00:39:30	Vinod	Copy	/CriticalFileServer/HumanResources/EmployeeInformation	Success
Dec 19 10:30:25	John	Read	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 19 10:30:25	John	Update	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 19 11:30:25	Vinod	Copy	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 19 11:30:25	Vinod	Update	/CriticalFileServer/TopSecret/IIoTProductSourceCode.txt	Success
Dec 24 00:42:15	Jack	Read	/CriticalFileServer/CompanyInfo/TopSecret/IIoTProduct/	Success
Dec 24 00:42:15	Jack	Copy	/CriticalFileServer/CompanyInfo/TopSecret/IIoTProduct/	Success
Dec 24 00:42:15	Jack	Update	/CriticalFileServer/CompanyInfo/TopSecret/IIoTProduct/	Success
Dec 24 01:42:15	Jack	Delete	/CriticalFileServer/CompanyInfo	Failure
Dec 24 01:43:15	Jack	Delete	/CriticalFileServer/TopSecretret	Failure
Dec 24 01:45:15	Jack	Delete	/CriticalFileServer/HumanResources	Failure

SQL Server:

Timestamp	User	Action	Query
Dec 14 11:00:25	app_user	SELECT	SELECT * FROM SmartMeterCoDB.Readings WHERE MeterID = '12345';
Dec 14 11:05:10	admin	UPDATE	UPDATE SmartMeterCoDB.Readings SET Value = '100' WHERE MeterID = '54321';
Dec 14 11:10:45	db_admin	DROP TABLE	DROP TABLE SmartMeterCoDB.Readings;
Dec 15 11:00:25	app_user	SELECT	SELECT * FROM SmartMeterCoDB.Readings WHERE MeterID = '12345';
Dec 15 11:05:10	admin	UPDATE	UPDATE SmartMeterCoDB.Readings SET Value = '101' WHERE MeterID = '54321';
Dec 15 11:10:45	db_admin	DROP TABLE	DROP TABLE SmartMeterCoDB.Readings;
Dec 19 11:00:25	app_user	SELECT	SELECT * FROM SmartMeterCoDB.Readings WHERE MeterID = '12345';
Dec 19 11:05:10	admin	UPDATE	UPDATE SmartMeterCoDB.Readings SET Value = '102' WHERE MeterID = '54321';
Dec 19 11:10:45	db_admin	DROP TABLE	DROP TABLE SmartMeterCoDB.Readings;
Dec 20 11:00:25	app_user	SELECT	SELECT * FROM SmartMeterCoDB.Readings WHERE MeterID = '12345';
Dec 20 11:05:10	admin	UPDATE	UPDATE SmartMeterCoDB.Readings SET Value = '102' WHERE MeterID = '54321';
Dec 20 11:10:45	db_admin	DROP TABLE	DROP TABLE SmartMeterCoDB.Readings;
Dec 21 11:00:25	app_user	SELECT	SELECT * FROM SmartMeterCoDB.Readings WHERE MeterID = '12345';
Dec 21 11:05:10	admin	UPDATE	UPDATE SmartMeterCoDB.Readings SET Value = '103' WHERE MeterID = '54321';
Dec 21 11:10:45	db_admin	DROP TABLE	DROP TABLE SmartMeterCoDB.Readings;
Dec 21 00:10:45	Jack	SELECT	SELECT * FROM SmartMeterCoDB.Readings:
Dec 21 00:10:45	Jack	SELECT	COPY * FROM SmartMeterCoDB.Readings DELIMITER ',' CSV HEADER;
Dec 22 11:00:25	app_user	SELECT	SELECT * FROM SmartMeterCoDB.Readings WHERE MeterID = '12345';
Dec 22 11:05:10	admin	UPDATE	UPDATE SmartMeterCoDB.Readings SET Value = '102' WHERE MeterID = '54321';
Dec 22 11:10:45	db_admin	DROP TABLE	DROP TABLE SmartMeterCoDB.Readings;