CoreView support for FINRA and IT Security

Summary

CoreView Reports for Microsoft Office 365 provide required auditing and incident reporting forensics not available natively, and which are required by FINRA for financial services firms. Actionable reports can also trigger alerts to reduce cyber event impact. In support of FINRA's guidance, CoreView Reports for Office 365 support the following requirements:

- Technical controls for auditing Office 365 access and activity for a 12-month period (longer retention available in CoreView – Microsoft stores most events for just 90 days)
- Creation of an Incident Response Plan for the containment, mitigation, eradication, recovery, investigation and notification of compromising events.

These items are mapped to FINRA's Checklist for a Small Firm's Cybersecurity Program, below.

Requirements for FINRA Members

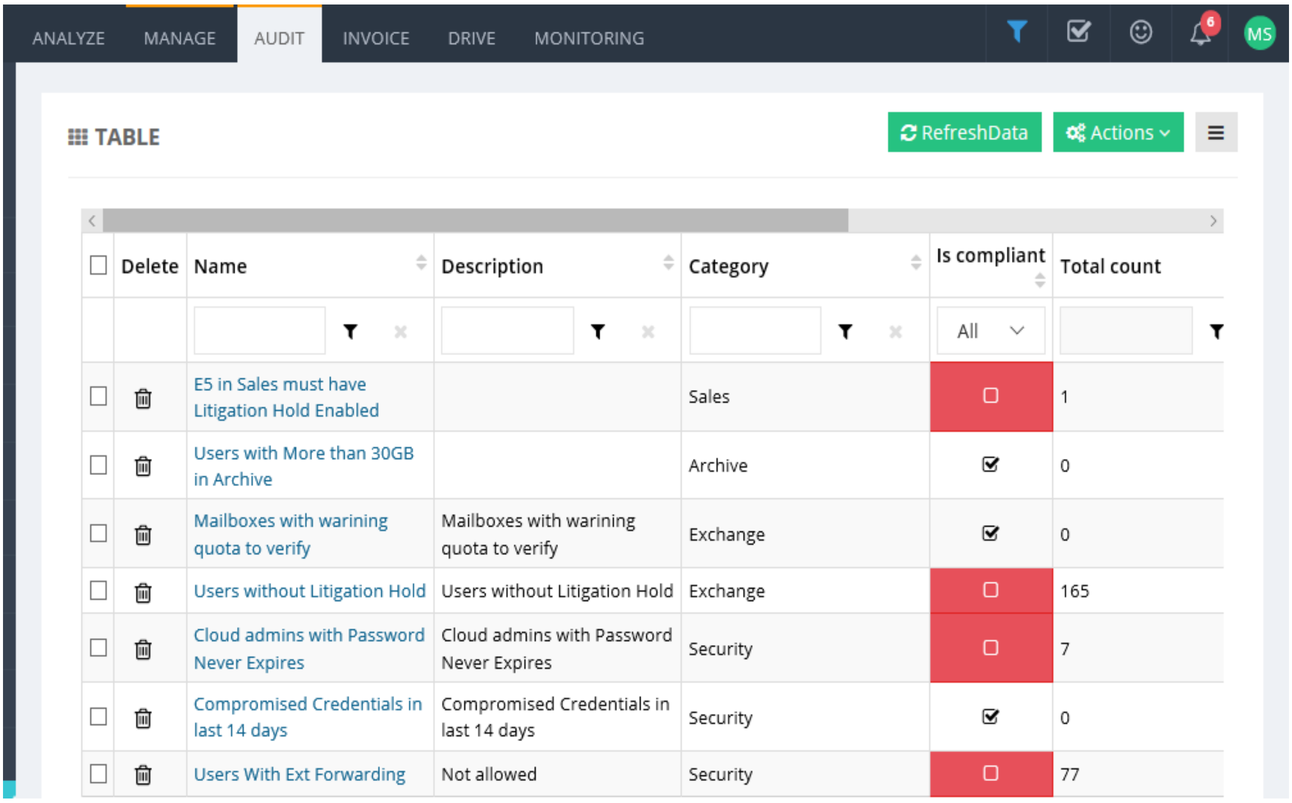
FINRA – the Financial Industry Regulatory Authority – has created a Checklist for a Small Firm's Cybersecurity Program to assist firms in establishing a cybersecurity program to:

- identify and assess cybersecurity threats, protect assets from cyber intrusions
- Detect when their systems and assets have been compromised
- Plan for the response when a compromise occurs

FINRA expects firms to consider the principles and effective practices in this report as they develop their cybersecurity programs. FINRA will assess the adequacy of firms' cybersecurity programs.

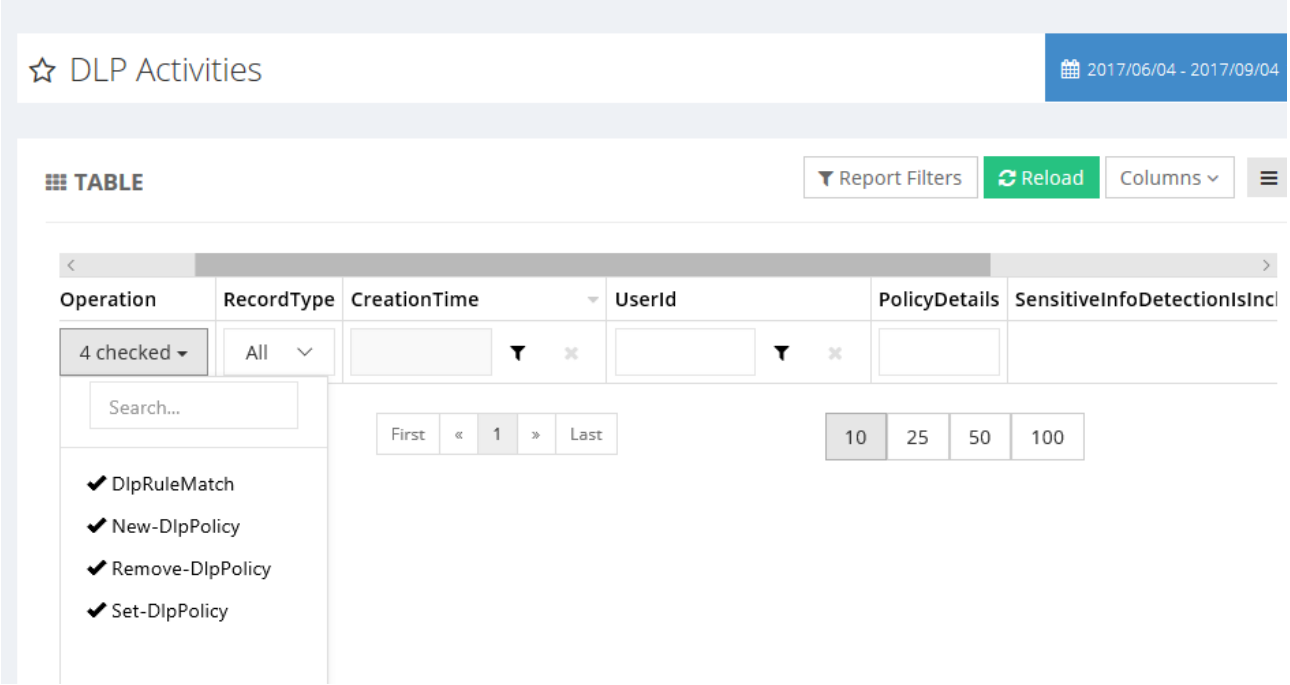
1. IDENTIFY AND ASSESS CYBERSECURITY THREATS

CoreView's Compliance Reports depict Desired Configuration Management (DCM) for user accounts and settings – like Litigation Hold, mobile device Policies, and compromised accounts.



☐	Delete	Name	Description	Category	Is compliant	Total count
☐	🗑	E5 in Sales must have Litigation Hold Enabled		Sales	□	1
☐	🗑	Users with More than 30GB in Archive		Archive	☑	0
☐	🗑	Mailboxes with warining quota to verify	Mailboxes with warining quota to verify	Exchange	☑	0
☐	🗑	Users without Litigation Hold	Users without Litigation Hold	Exchange	□	165
☐	🗑	Cloud admins with Password Never Expires	Cloud admins with Password Never Expires	Security	□	7
☐	🗑	Compromised Credentials in last 14 days	Compromised Credentials in last 14 days	Security	☑	0
☐	🗑	Users With Ext Forwarding	Not allowed	Security	□	77

Firms can utilize Microsoft Office 365's Data Loss Prevention (DLP) policies to identify documents and messages which have customer personally identifiable information (PII). CoreView's Audit for Exchange and SharePoint DLP activities log and track items that trigger PII policies for content:

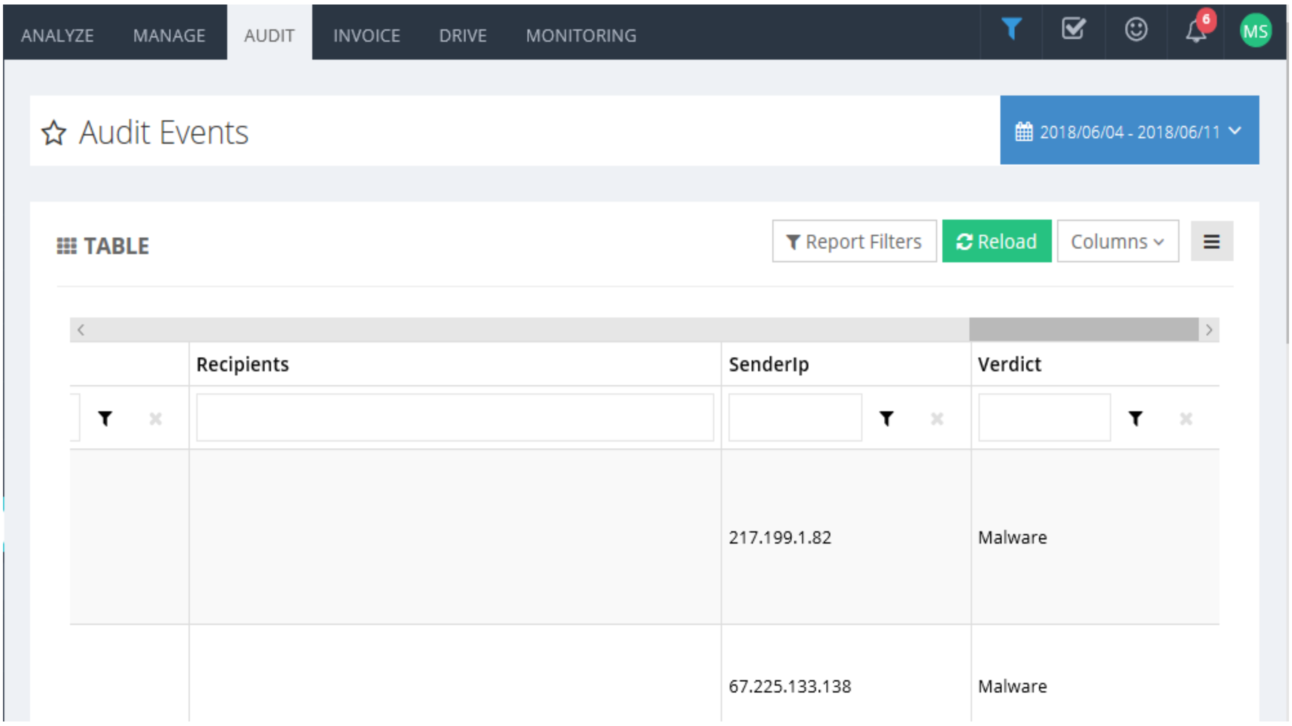


Operation	RecordType	CreationTime	UserId	PolicyDetails	SensitiveInfoDetectionIsIncl
4 checked	All				

✔ DlpRuleMatch
✔ New-DlpPolicy
✔ Remove-DlpPolicy
✔ Set-DlpPolicy

2. DETECT INTRUSION

Firms can leverage Microsoft Office 365 Advanced Threat protection and use CoreView's Threat Intelligence Reports to identify malware, suspicious login attempts, and brute force attacks.



Recipients	SenderIp	Verdict
	217.199.1.82	Malware
	67.225.133.138	Malware

3. CREATE A RESPONSE PLAN

Every response to a workstation virus, ransomware, compromised account, or malicious attack should include CoreView's Audit report of all account actions on the platform. HR should initiate a CoreView Office365 report for every separated employee. Data is stored for a minimum of one year and includes every account action – file access and downloads, dates, times, groups, files, settings changes – a complete record. Use audit reports after a ransomware attack to detail every file accessed within a date range. For compromised accounts, see all O365 user and administrative actions, including IP addresses and devices.

Conclusion

The CoreView Platform for Office 365 provides a cost-effective way to enhance and extend the capabilities of Microsoft Office 365 for security and eDiscovery. These unique capabilities assist firms satisfy their FINRA responsibilities by extended auditing retention, correlation of data across multiple Microsoft Office 365 applications, and enhanced intelligence supporting comprehensive incident response.