VCCCD Security Resources

Security Applications	Adoption Status
Trend Micro XDR	LIVE
Trend Micro Cloud App Security	LIVE
Trend Micro Apex One	LIVE
Spirion Data Protection	LIVE/DECOMMISSIONED
O365 Defender DLP	LIVE/IN-PROGRESS
O365 Defender ATP	LIVE/IN-PROGRESS
O365 Defender Endpoint	NOT ACCEPTED
Palo Alto NGFW	LIVE
Thycotic Secret Server	LIVE
Thycotic Unix & Service Acct Mgt	IN-PROGRESS
Milton MDR	LIVE
CIS MCAP	LIVE
LogRhythm	LIVE
Anomali Threatstream	LIVE
Deloitte Cyber Detect and Respond	LIVE
IP Quality Score	LIVE
REN-ISAC	LIVE
Trustwave	LIVE
Splunk	IN PROGRESS
Veeam	LIVE
LAPS	LIVE/IN-PROGRESS
MS-ISAC	LIVE/IN-PROGRESS
MDBR	SIGNED UP

CONFIDENTIALITY NOTICE: This document is the property of the VCCCD. It may contain information which is confidential, sensitive, privileged, proprietary or otherwise protected by law. The information is solely intended for the named recipients, other authorized individuals, or a person responsible for delivering it to the authorized recipients. If you are not an authorized recipient of this message, you are not permitted to read, print, retain, copy or disseminate this message or any part of it. If you have received this e-mail in error, please notify the sender immediately by return e-mail and delete it from your e-mail inbox, including your deleted items folder.

Glossary

Adoption Status	Description
NOT ACCEPTED	The college did not accept the System-Wide integration
SIGNED UP	The college has agreed and signed up for the System-Wide integration
IN PROGRESS	Install is in progress at the college
NOT LIVE	The System is not available in Production environment for the users
LIVE	The System is now available in a Production environment and is actively used by the users
DECOMMISSIONED	The college decided to remove the System integration

Application Name	Description
Trend Micro XDR	eXtend Detection & Response - Endpoint telemetry, vulnerability reporting, email threat detection, correlation, endpoint and mail response, risk insights, "Vision One" console
TM Cloud App Security	API-driven email security(O365 & Gmail), cloud & host DLP, cloud storage security (SharePoint, OneDrive, Teams, Google Drive)
Trend Micro Apex One	Endpoint threat detection & prevention, web filtering, external device management, integrated with XDR/Vision One for response and containment
Spirion Data Protection	Data ID/lifecycle management; scanning, redaction and remediation capabilities. In-use on Servers via remote scanning. Endpoint agent decomm due to impact one Office applications
O365 DLP	Data loss prevention active for OneDrive, SharePoint, Teams, Planned for Exchange. Rules enabled for HIPAA, Financial data, PII, and Employee ID #s
O365 Defender ATP	Advanced Threat Protection for Exchange & Azure; Security posture and email security reporting. Spam prevention and alerting on high risk users enabled.
Palo Alto NGFWs	Next-Gen Firewalls; Network perimeter security, threat detection, exploit delivery prevention
Thycotic Secret Server	Thycotic (now "Delinea") - District IT secure password storage and management
Thycotic Unix & Service Acct Mgt	Unix account management and connection proxy, service account management discovery & mgt
Milton MDR	Managed Detection & Response. External partner providing 24/7 detection and response. Alerting and escalation, adversary hunting, issue tracking, incident response.
CIS MCAP	Malicious code analysis platform (provided by MS-ISAC). Web-based sandbox for detonation of suspicious files and links.
LogRhythm	Security Information and Event Management. Alerts based on 3rd party and internally created rules. Log aggregation and long-term storage.
Anomali Threatstream	Threat intelligence feed provided by MS-ISAC; standalone data for threat and adversary research, STIX/TAXI feed integrated with LogRhythm
Deloitte Cyber Detect & Respond	Repository of third-party feeds, Deloitte processed data, cyber threat analysis, threat actor profiles, and vulnerability notifications. Strategic and tactical threat reports. (MS-ISAC provided)

Application Name	Description
IP Quality Score	IP & Email fraud scoring, Proxy, VPN, and Tor detection. Integrated with student registration.
REN-ISAC	Daily watch report, Peer assessment services, SANS resources, Ops & Discuss email channels
Trustwave	PCI compliance tracking, validation, and completion wizard; Migrated to securetrust.com
Splunk	Data platform for log ingestion, alerting and visualization - AWS logging
Veeam	System & Data Backups, Disaster recovery
MS-ISAC	Multi State Information Sharing & Analysis Center - provides several free tools, monthly threat briefings, peer review, mentoring, CIS hardened images & workbench.
MDBR	Malicious Domain Blocking & Reporting; Akamai DNS service which allows to block and track access to malicious domains. Not currently adopted due to concerns of impacting DNS

CONFIDENTIALITY NOTICE: This document is the property of the VCCCD. It may contain information which is confidential, sensitive, privileged, proprietary or otherwise protected by law. The information is solely intended for the named recipients, other authorized individuals, or a person responsible for delivering it to the authorized recipients. If you are not an authorized recipient of this message, you are not permitted to read, print, retain, copy or disseminate this message or any part of it. If you have received this e-mail in error, please notify the sender immediately by return e-mail and delete it from your e-mail inbox, including your deleted items folder.