CU*ANSWERS Network Services

AdvantageCIO

Navigating Cybersecurity:
A Guide to CNS Services

Cybersecurity has become a focal point for all businesses, and more acutely for financial institutions. At this point everyone has been affected either directly or indirectly by a cybersecurity event. Examples of direct events include ransomware, phishing, credential harvesting, and exfiltration of sensitive data. Indirect events include those involving key partners or solutions such as the vulnerabilities to Microsoft Exchange, Oracle Java, Solar Winds and Kaseya. One truth that has emerged the last few years is that these threats are constant and they're not going away.

Understanding your institution's cybersecurity posture is vital. As many outsource key functions to third parties, knowing what they cover and what they don't is critical. We believe that a good approach to cybersecurity is divided into three areas: 1) your staff, 2) your IT team (such as CNS), and 3) the specialists (e.g. legal, forensic, insurance, security operations, etc.). Determining the best set of partners is both a business and risk management decision.

CU*Answers Network Services and AdvantageCIO provide many cybersecurity related services to credit unions. This document is a guide to what services we do and do not offer.

Workstation and Server Management

What we do

Systems Monitoring and Administration

- Automated log collection and monitoring of Windows servers and workstations
- Continuous alerting for common system telemetry values, critical processes, M-F 8 to 5 support/response
- All server log information is archived for 180 days in Kaseya VSA system hosted at CNS in a SSAE 16 SOC 2 environment
- Weekly scheduled reporting for key system metrics, such as environment health, patch status, login, and systems access activity
- Server and workstation asset management tracking and scheduled/on-demand reporting, covering both software and hardware assets

Patch Management

- Monthly server patch installation scheduled during off peak hours.
- Automated workstation patch installation as patches become available
- Weekly review of workstation patch status, ticket generation for systems out of compliance
- Patching scope includes workstations and server operating system patching (Microsoft) and 3rd party applications (Chrome, Adobe, etc.)
- Monthly patch status report

Managed Security

- Trend Micro Worry-Free Business software configured with automated alerting (client defined)
- Host-based intrusion prevention services (client defined)
- Data Loss Prevention controls for servers and workstations (client defined)
- Managed website content filtering, alerting and reporting with Cisco Umbrella
- Active Directory oversight, alerting and reporting with Netwrix Auditor

What we don't do

- Realtime response to all event types
- SEIM and MDR/XDR type 24x7 aggregation, real time monitoring, alerting and response
- Security Operations Center (SOC)
- Respond in real-time to events in Netwrix Auditor, Trend Micro WFB or Cisco Umbrella
- Guarantee real-time response to zero-day threats

Email Management

What we do

Hosted Email

- Microsoft Business 365 Premium, licensed per user
- Mailboxes up to 50GB per user
- Email backup to CNS with VEEAM 365
- Calendar, contacts, and public folders
- Mobile access for phones and tablets

Email Security

- Data loss prevention policies for member/confidential data
- Customized monitoring and alerting
- Anti-malware, attachment scanning and anti-phishing controls
- Conditional access and multifactor authentication
- Client directed and automated email encryption
- Email archival, e-discovery and litigation hold
- Mobile device management with Microsoft Intune

What we don't do

- Realtime response to all event types
- SEIM and MDR/XDR type 24x7 aggregation, real time monitoring, alerting and response
- Security Operations Center (SOC)
- Monitor email content or security in real time
- Guarantee you will not be targeted by phishing or other social engineering threats
- Guarantee that cloud providers won't have incidents that affect you

Managed Network Infrastructure

What we do

Network Monitoring and Alerting

- Continuous alerting for all managed network components M-F 8 to 5 support/response
- Performance reporting including interface specific uptime/downtime, throughput, packet loss, latency, and hardware performance
- Regular configuration backup at CU*Answers (outers)
- Technical Support including configuration changes (does not include network design/project work)

Firewall Management

- Continuous Firewall Syslog Collection by Fortinet's FortiAnalyzer software, 90-day retention
- Customized monitoring and alerting (client defined)
- Application layer security, including intrusion prevention and gateway anti-virus/malware
- Secure Remote and Mobile Access with multifactor authentication
- Change management and technical support (does not include network design/project work)
- Regular firmware updates, hardware and software warranty
- Weekly activity reporting

What we don't do

- Realtime response to all event types
- SEIM and MDR/XDR type 24x7 aggregation, real time monitoring, alerting and response
- Security Operations Center (SOC)
- Monitor and respond to firewall event information in real time
- Guarantee that the firewall will block all malicious traffic from entering your network

Backup and Business Continuity

What we do

Backup and Data Protection

- Incremental backups for target servers run on a scheduled basis
- Daily backup data replicated to Network Services data centers (500GB offsite storage included)
- On-appliance virtualization recovery capabilities
- Full reporting, both weekly and on-demand
- AES data encryption for backup data in transit and at rest
- Weekly integrity checking of backup jobs for both on and offsite files

Virtual Branch

- Virtual hot site business continuity/disaster recovery service
- CNS Private Cloud SSAE 18 SOC 2 datacenters
- VMware Horizon VDI images running core/client defined software
- Annual disaster recovery test for all systems
- Recovery test report and gap analysis

What we don't do

- Realtime response to all event types
- SEIM and MDR/XDR type 24x7 aggregation, real time monitoring, alerting and response
- Security Operations Center (SOC)
- Guarantee that your backups will not be affected by malicious activity from threat actors
- Guarantee that the firewall will block all malicious traffic from entering your network

CU*ANSWERS Network Services

Support

What we do

Helpdesk

- Includes unlimited remote support during business hours, 7:30 AM to 12 PM ET; does not include project labor, training or after hours/weekend support
- Variable onsite support resources through Presence Tech and Virtual Presence Tech services
- Project labor for custom projects, standard rate $100/hour; quote provided or Time and Materials
- Incident response support rate $120/hour
- Fulfillment of any IT equipment, from PCs to networking gear through our online store: https://store.cuanswers.com/store/network-services/
- Management/tracking of all subscription-based services and renewals

Operations

- Daily checks on site and system outages, endpoint system alerts, onsite and offsite backups, events and alarms on servers, virtualization/infrastructure and 365 backups
- Weekly checks on report delivery, systems have endpoint security installed, patch management status/functionality, systems have RMM agent installed, workstations are in proper OUs, and login failure reporting
- Monthly check on patching, assurance reports and agents that have not checked in

What we don't do

- Realtime response to all event types; resources are only available on a first come, first served basis
- SEIM and MDR/XDR type 24x7 aggregation, real time monitoring, alerting and response
- Security Operations Center (SOC)
- Guarantee that no cybersecurity related events or incidents will occur

AdvantageCIO

What we do

vCIO Bundle

- Compliance
  - Annual information security report for the board of directors
  - Annual information security risk assessment
  - Business continuity plan with business impact analysis
  - Security incident response plan
  - Comprehensive information security program and policies
  - Annual NCUA ACET completion/updates
  - Assistance with annual audit and examination preparation and response
- Planning
  - 3-year strategic technology plan
  - Annual technology budget
  - Lifecycle management report

Managed Vulnerability Services

- Quarterly internal vulnerability scan
- Quarterly external vulnerability scan
- Quarterly vulnerability report with remediation recommendations and tracking/trending analysis
- Utilizing Tenable Nessus on-demand vulnerability scanning platform

Cybersecurity Training and Testing

- Monthly education campaigns, targeted training
- Quarterly phishing testing
- Quarterly management reporting
- Annual USB/vishing testing

Continued on next page

AdvantageCIO

What we don't do

- Realtime response to all event types
- SEIM and MDR/XDR type 24x7 aggregation, real time monitoring, alerting and response
- Security Operations Center (SOC)
- Guarantee that no cybersecurity related events or incidents will occur
- Provide documents that should be viewed in perpetuity; all documents, findings and recommendations are a point in time only
- Guarantee that following recommendations will prevent you from having a cyber event at your institution

Some additional things we don't do

- Dark web monitoring
- Threat hunting
- Forensic or remediation services
- Provide or assess cybersecurity insurance
- Provide legal advice
- Provide communications guidance regarding incident response
- Guarantee you will not have a cyber event at your institution

Why don't we do these things?

There is no solution or set of solutions that can guarantee cybersecurity. Therefore, no matter how much you do we can't guarantee that you won't be affected. We encourage a layered approach, that you train/test your people, have an independent assessment, and find the right partners. In many cases you don't need to be the most secure institution in the world, just more secure than your peers.

These are all services where you want to use a firm that specializes and focuses on that area specifically. Just as you would not take medical guidance from someone who isn't a doctor, and if you had a fire, you would call the fire department, we encourage you to work with experts in these areas.

We still play a key role as your IT team, but if you were to have an incident, you'll want to bring in experts to work with the credit union and us. We are currently reviewing offerings from 24x7 monitor/alert/response providers and may have some recommendations for partners you can look at.

Glossary of Terms:

SIEM: *Stands for Security Information and Event Management. These systems aggregate event information from various sources, for example endpoint, event log, syslog, etc., and correlate in real time and alert if an incident or indicator of compromise is detected. Today SIEM is typically delivered "as a service" and monitored by a SOC. While CNS does some of these functions like log aggregation and basic alerting, the SIEM takes it a step further by leveraging more sources of event data and then correlating that across all their client base.*

XDR: *Extended Detection and Response solutions collect and correlate data over multiple sources, including email, endpoint, server, etc., and can quickly detect and alert on threats. This service is also typically delivered "as a service" including a SOC.*

MDR: *Managed Detection and Response. Same concept as XDR but with a predetermined response in the event a threat is detected. Actions are assigned to either the client or a SOC.*

SOC: *The Security Operations Center is a combination of people, processes and technology designed to provide 24x7x365 monitoring and alerting. They may also include response. Since the bad guys are working 24x7x365 you may wish to use a SOC and one of the previous defined solutions to enhance cybersecurity at your institution.*

Endpoint Protection: *Previously called anti-virus, this is modern security software that is installed on workstations, laptops, servers, etc. The protections commonly include real time anti-virus/anti-malware scanning, application white/blacklisting, data loss prevention controls and reporting/alerting. CNS uses Trend Micro WFB for all managed clients.*

CU*ANSWERS
Network Services

AdvantageCIO