Survey of Cybersecurity Solutions 2022

A Look Into the Security Tools Used by Industry Experts

By Aaron R. Warner, CEO & Lindy Trout, Creative Technical Writer
ProCircular, Inc.

ProCircular's role is to help organizations understand and manage their cyber risk. Organizations can defend themselves best by sharing information with one another, and this whitepaper is another way for ProCircular to share knowledge. Each year, we survey our existing clients to determine how they choose to address their current regulatory and cybersecurity needs. This year, we received feedback from 29 separate organizations from various industries (see graph) to answer the survey. We hope that these results will reveal options you may not have considered, contextualize your currently implemented solutions, and develop confidence in your security approach.

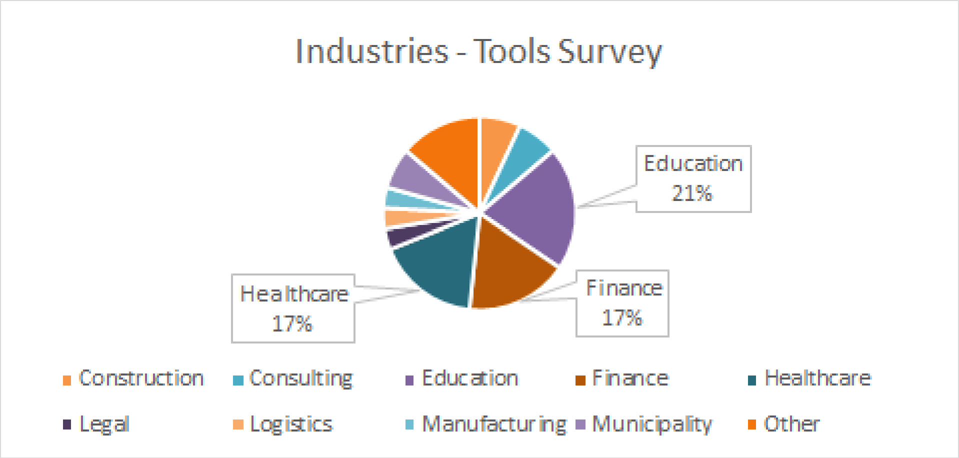
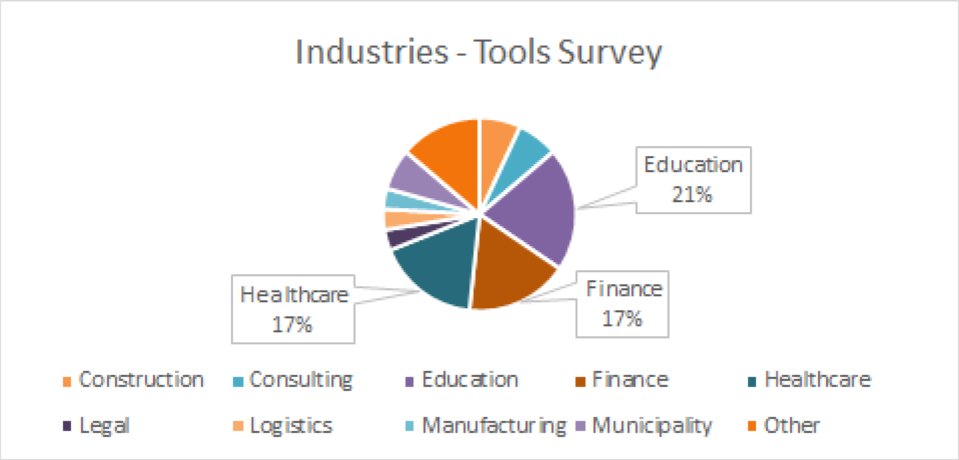


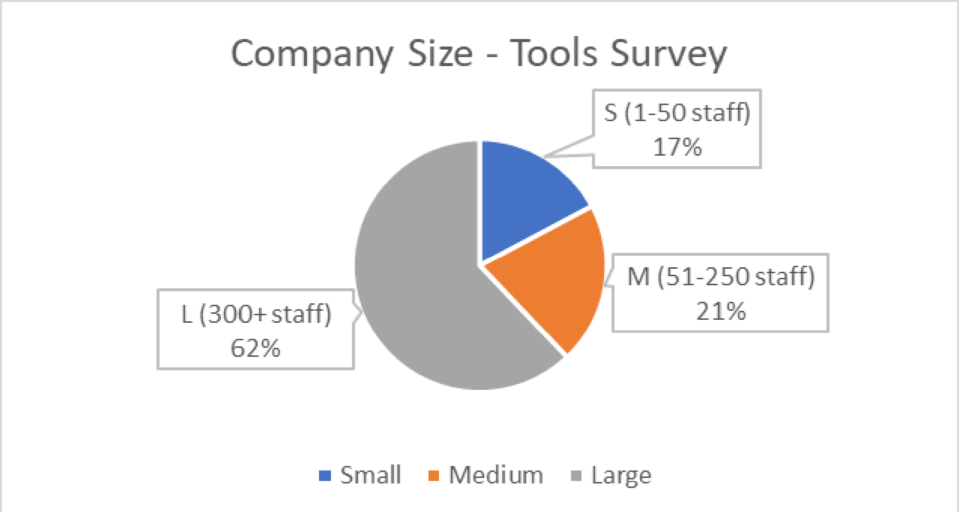
Table of Contents:

Client Information

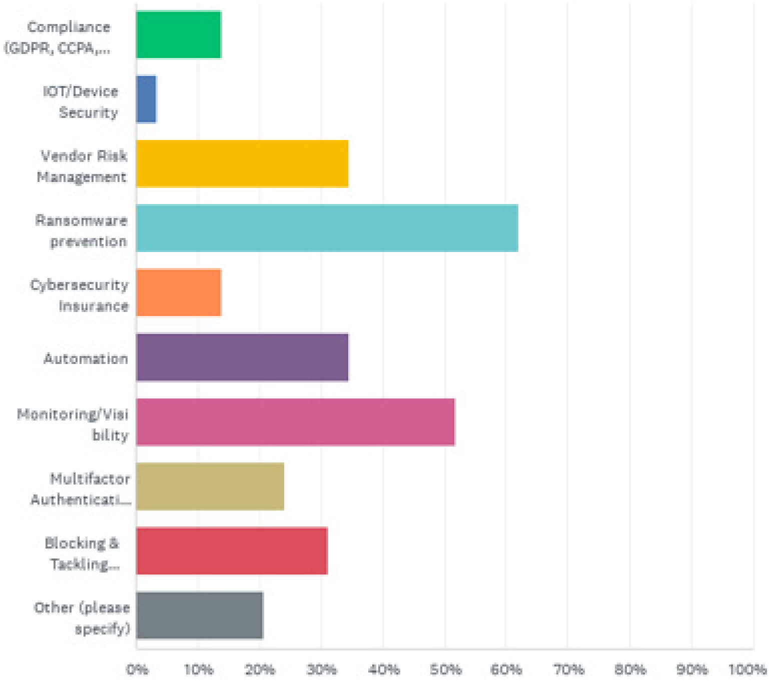
ProCircular surveyed 29 organizations across an array of industries, primarily education, healthcare, and finance.



Client Sizes

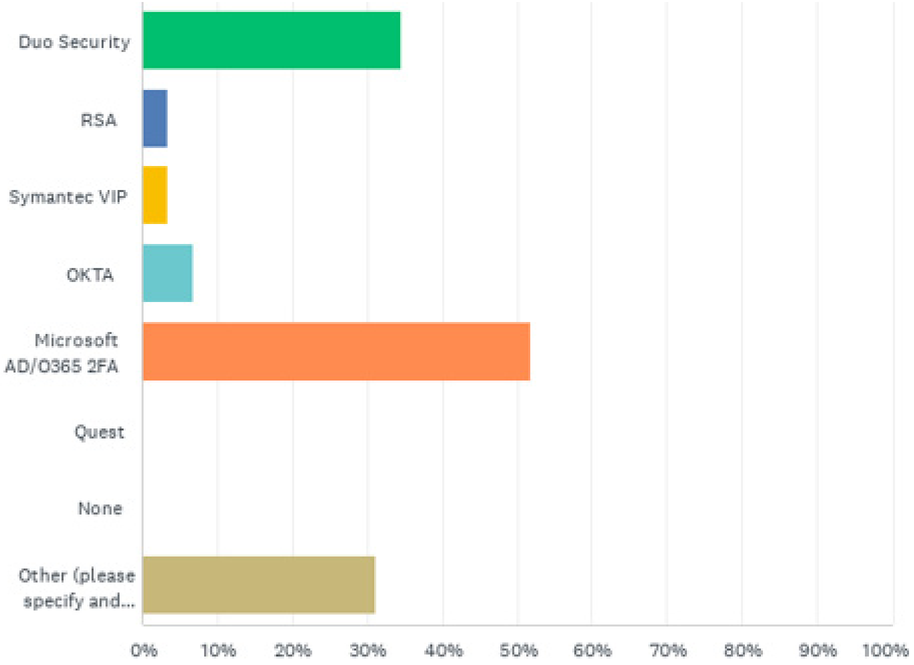


Question 1 - What topics or issues are top of mind for you in 2022?



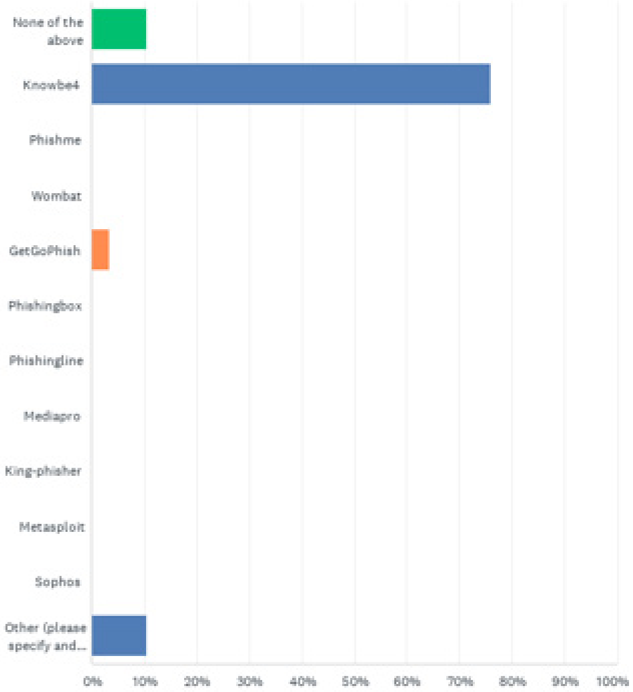
Other – DR, MDR, data loss prevention, secdevops, IAM & PAM

Question 2 – Which Multi-Factor Platform is in use at your organization?



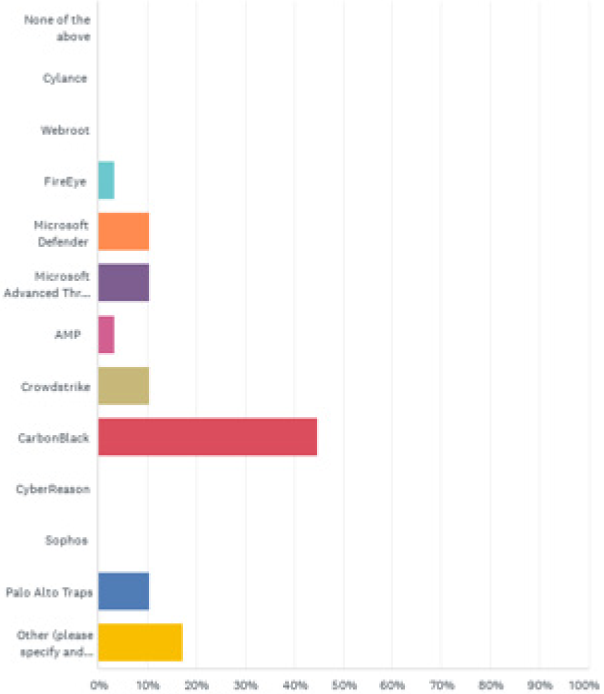
Other - PortalGuard, Passly, PingID, Yubikey, FortiAuthenticator (4), Google G Suite

Question 3 - What Phishing Platform is in use at your organization?



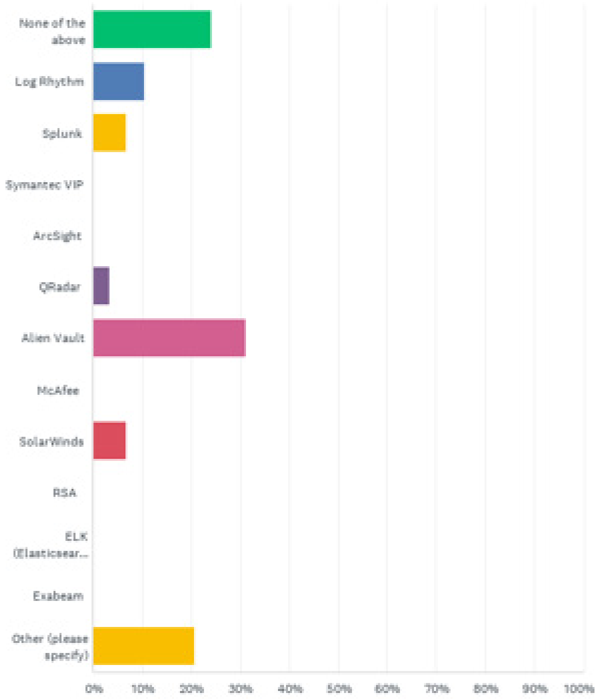
Other - Cofense PhishMe, Securence, Bullphish

Question 4 - What Endpoint Protection is in use at your organization?



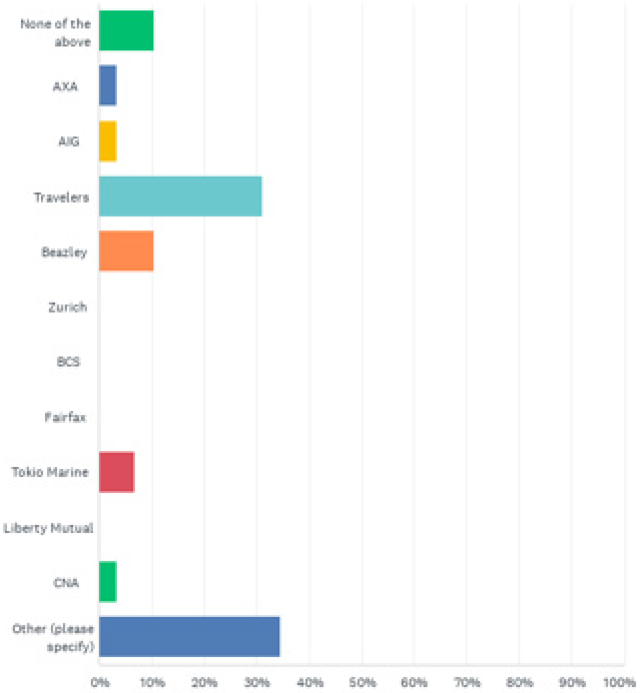
Other- Symantec Endpoint Protection, ESET, Huntress, Bitdefender, FortiClient, Palo Alto Cortex XDR Pro employee computers. Defender for non-employee computers. Also Attivo EDN on employee computers

Question 5 - What SIEM (Security Incident Event Monitoring) Platform is in use at your organization?



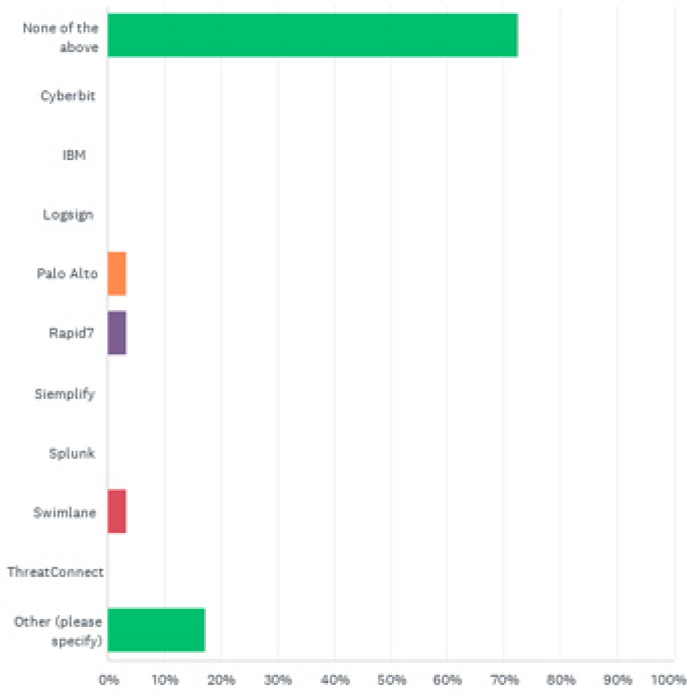
Other - Arctic Wolf, Adlumin, Quadrant Sagan, RocketCyber, Pseudo SIEM - Palo Alto Cortex XDR Pro Per TB

Question 6 - Which Cybersecurity Insurance Carrier are you using?



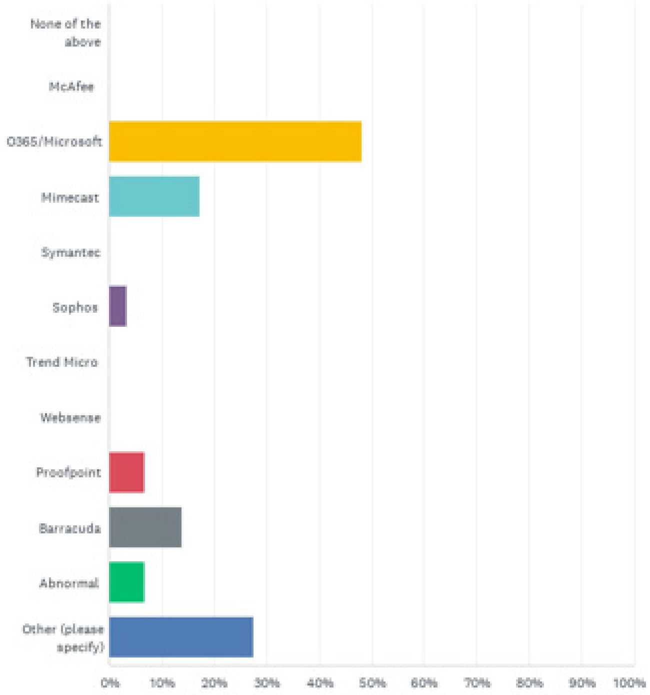
Other- ACE/Tokio Marine, CUNA Mutual provided, Bouslog and Iowa Communities Assurance Pool, Holmes Murphy, In-house/self insured, Federated, Lockton, EMC, Allied Solutions

Question 7 - What SOAR (Security Orchestration, Automation, and Response) is in use at your organization?



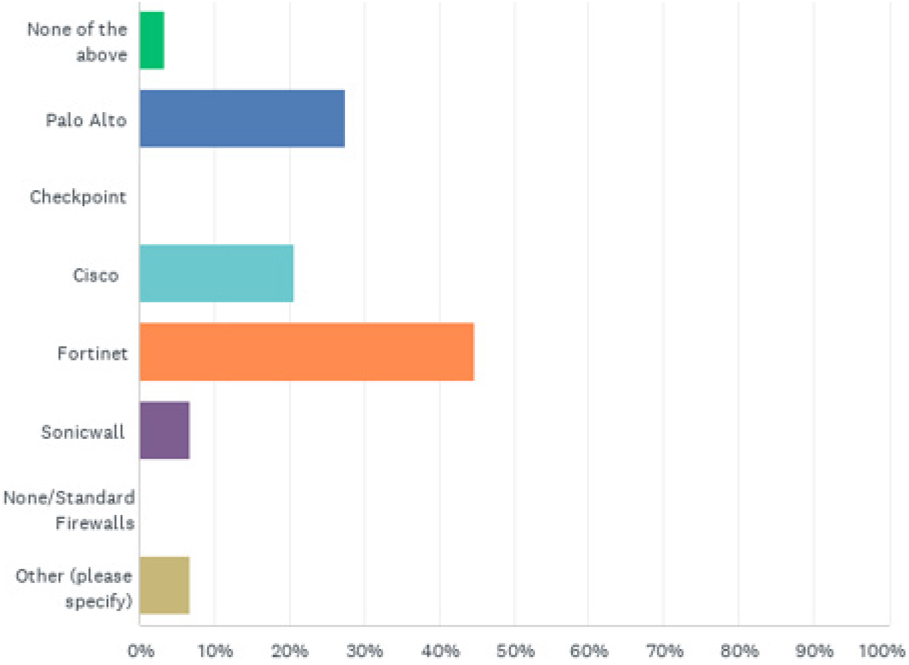
Other - Cisco SecureX, Greymatter, Internally-built, SIEM functionality (2)

Question 8 - What Email Security Platform is in use at your organization?



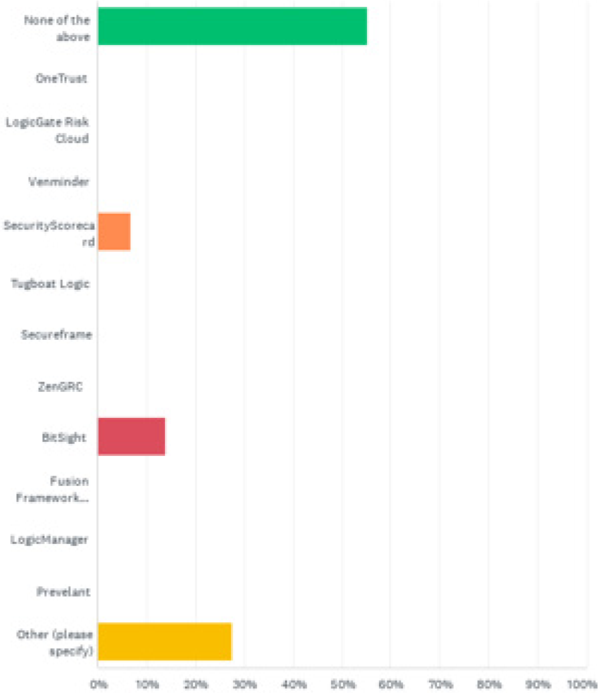
Other- Darktrace Antigena Email, FireEye ETP and Vipre Enterprise, Securence, Microsoft Advanced Threat Protection, With AD Pro, Iron Port, FortiMail, Google G Suite

Question 9 - What Next Gen Firewall is in use at your organization?



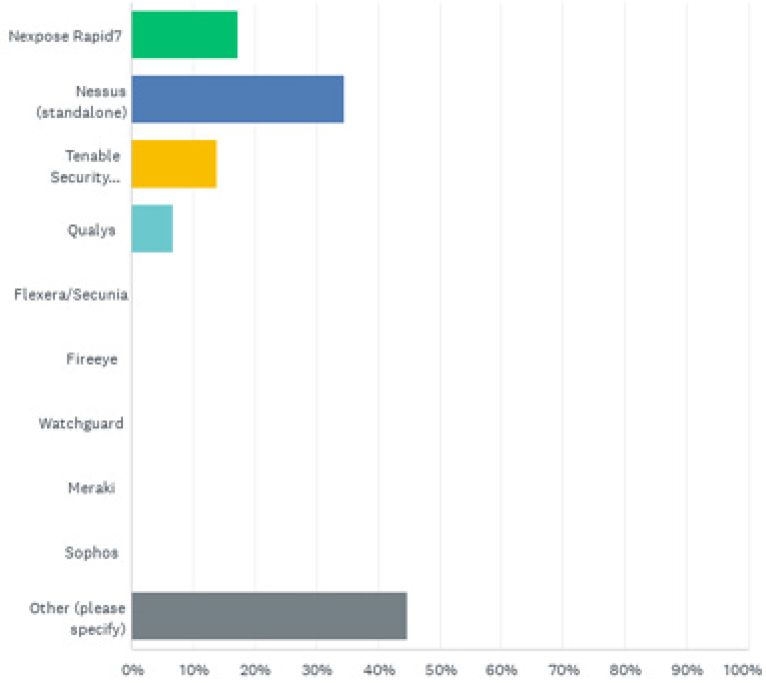
Other - Old Cisco ASA 5500, WatchGuard

Question 10 - What Vendor Risk Management platform are you using?



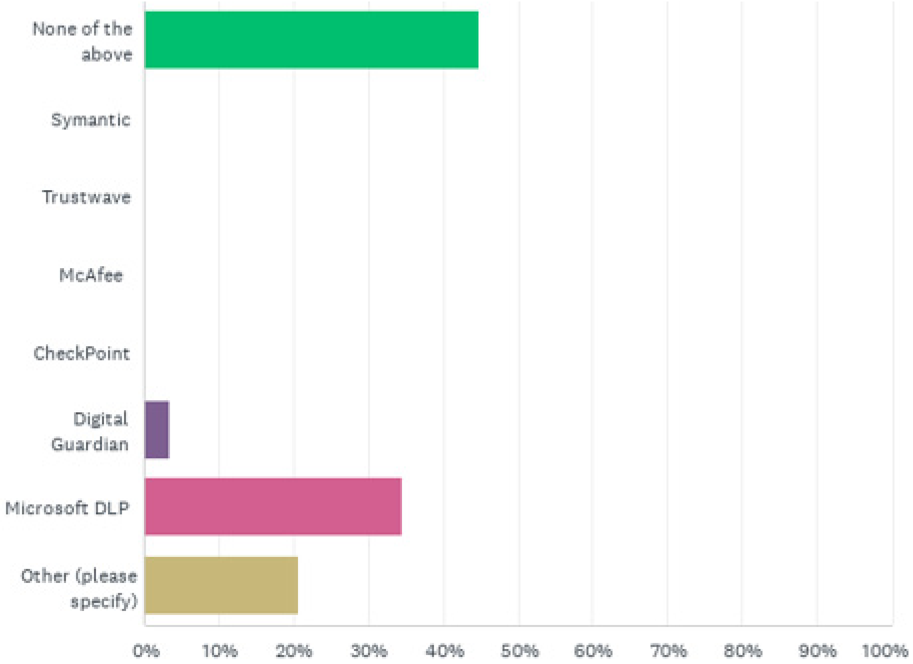
Other- Hecvat, Shodan, SBS TRAC, Excel/Sharepoint, NContracts, AuditBoard, NContracts

Question 11 - What Vulnerability Scanning Platforms are in use at your organization?



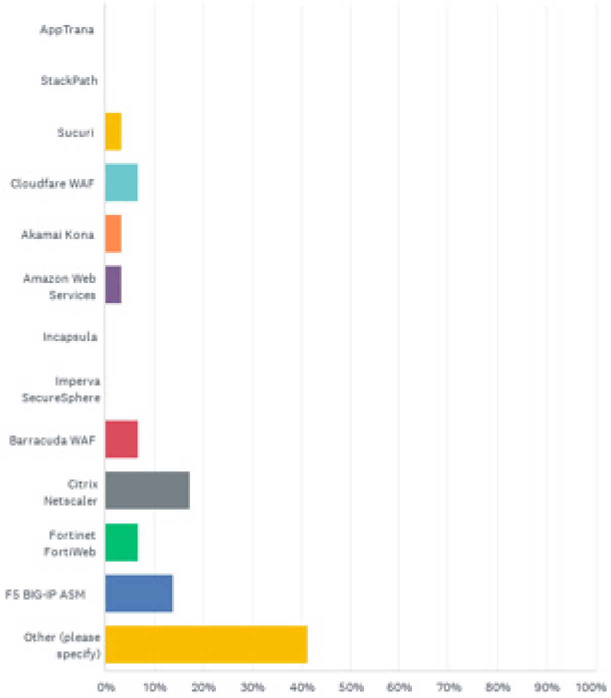
Other - ORDR, ProCirc CyberBlock, Alienvault, Tracesecurity, RocketCyber, CISA, Tripwire, Infosight, Defender ATP

Question 12 - What Data Loss Prevention (DLP) Platform is in use at your organization?



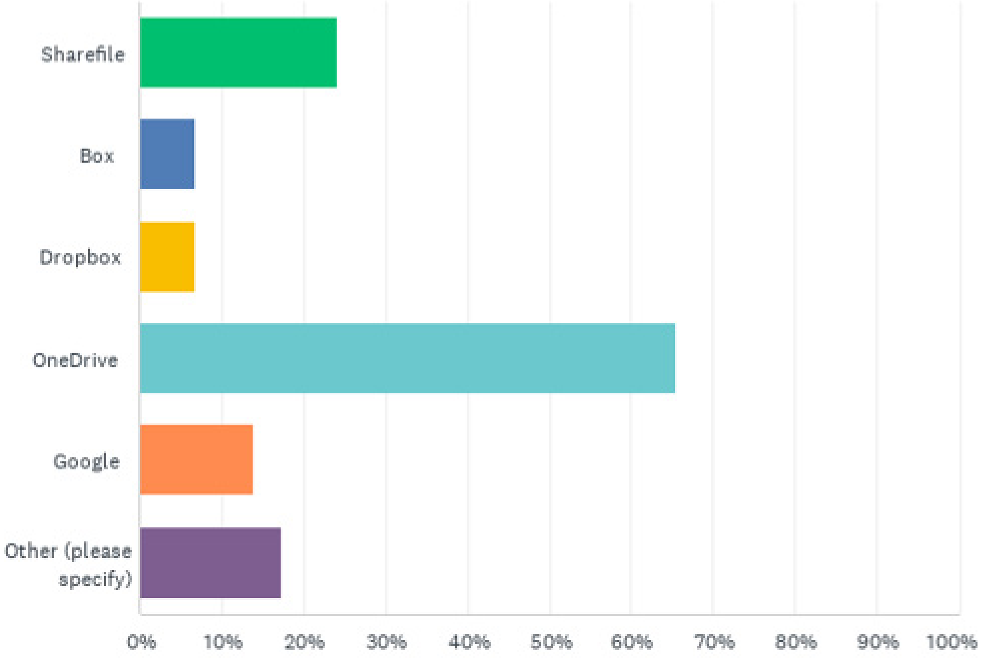
Other- SureBackup, Fortinet/LogRhythm policies and alerts, Microsoft but in passive mode, Palo Alto, Google. Dell Avamar

Question 13 - What Web Application Firewall (WAF) Platform is in use at your organization?



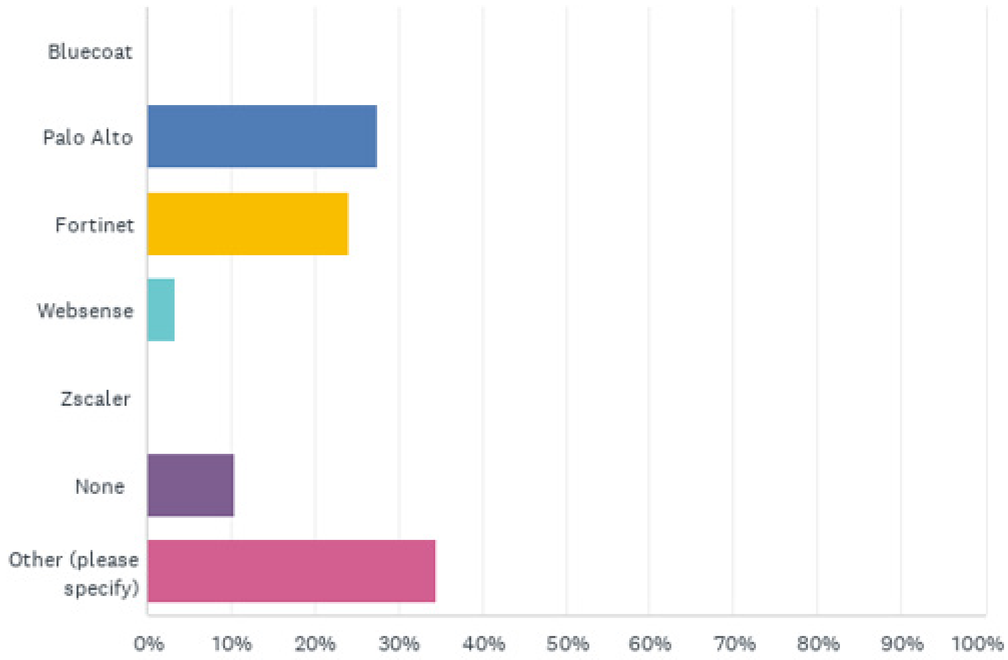
Other – None (7), Kemp (2), CISCO Umbrella, Sonicwall, Fortigate

Question 14 - What Secure Cloud Storage Solution is in use at your organization?



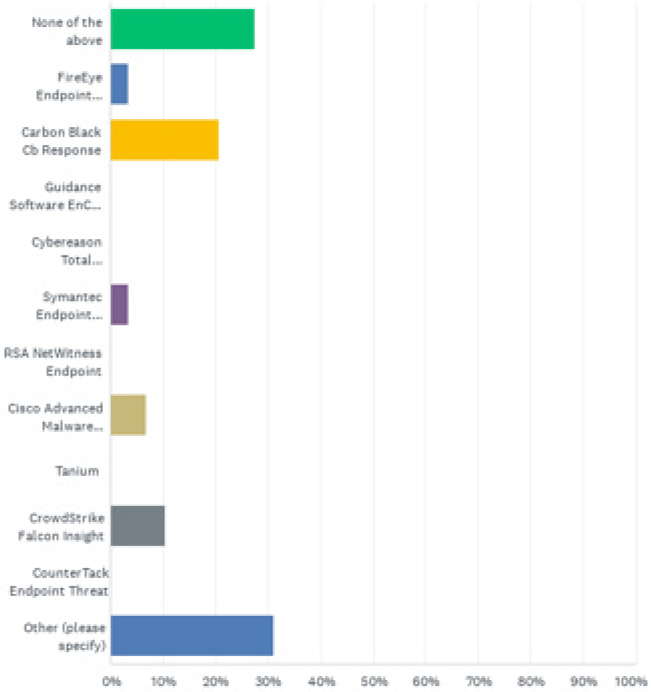
Other – CISCO Umbrella (6), Sonicwall, Watchguard, Defender ATP, WatchGuard, Forcepoint

Question 15 - What Web Filtering Platform is in use at your organization?



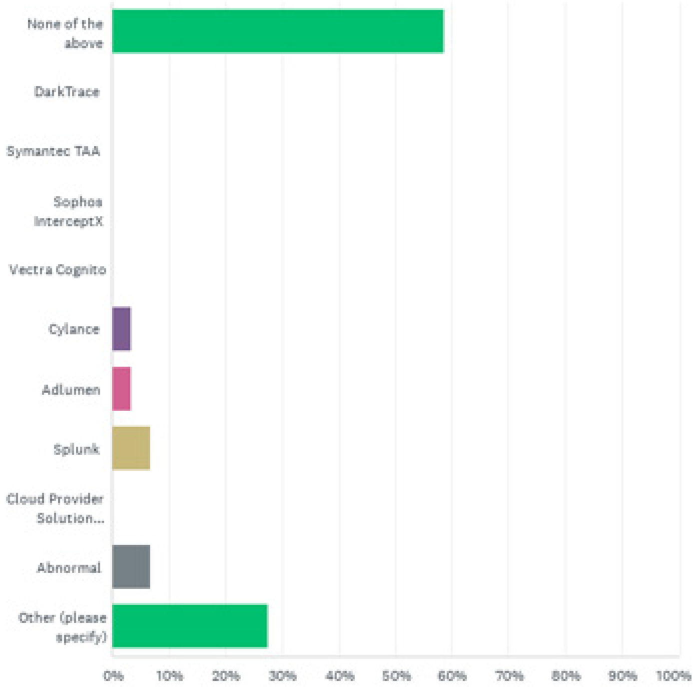
Other – SFTP Server, None (2), provided, OneDrive is shadow IT

Question 16 - What Endpoint Detection & Response Solution are deployed in your organization?



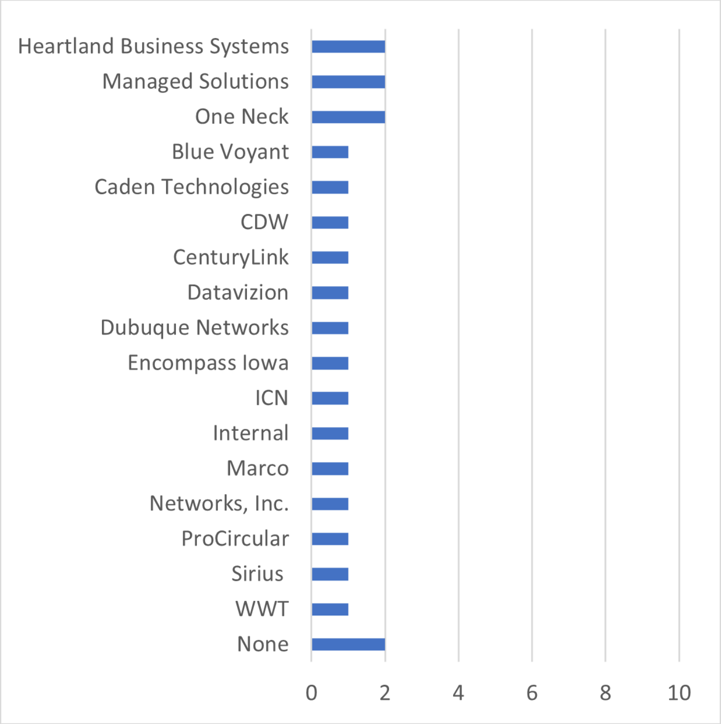
Other – Meraki, Huntress, Palo Alto Cortex XDR, Palo Alto XDR and Attivo EDN, Sonicwall IDS, Microsoft Defender, Red Canary, Defender ATP, Palo Alto Cortex XDR

Question 17 - What AI/ML Pattern or Anomaly Detection tools have been deployed in your organization?

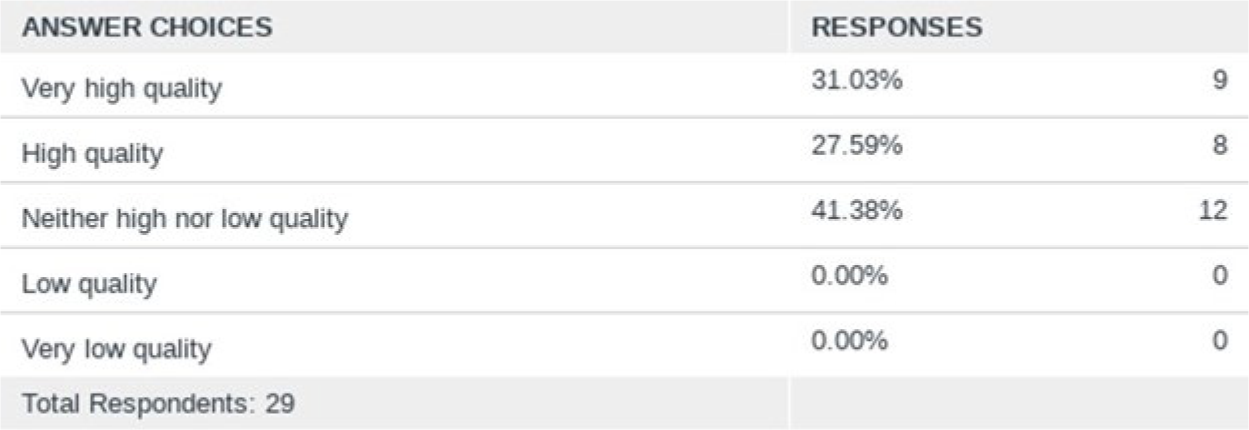


Other - Falcon Complete, Microsoft Advanced Threat Analytics, Attivo ADAssesso & Cortex EDN, None FireEye Network Security, Dell Secureworks iSensor, LogRhythm UEBA, CloudAI, Crowdstrike Falcon, Solar Winds SEM, Lansweeper

Question 18 -Who is your Primary I.T Service Provider?

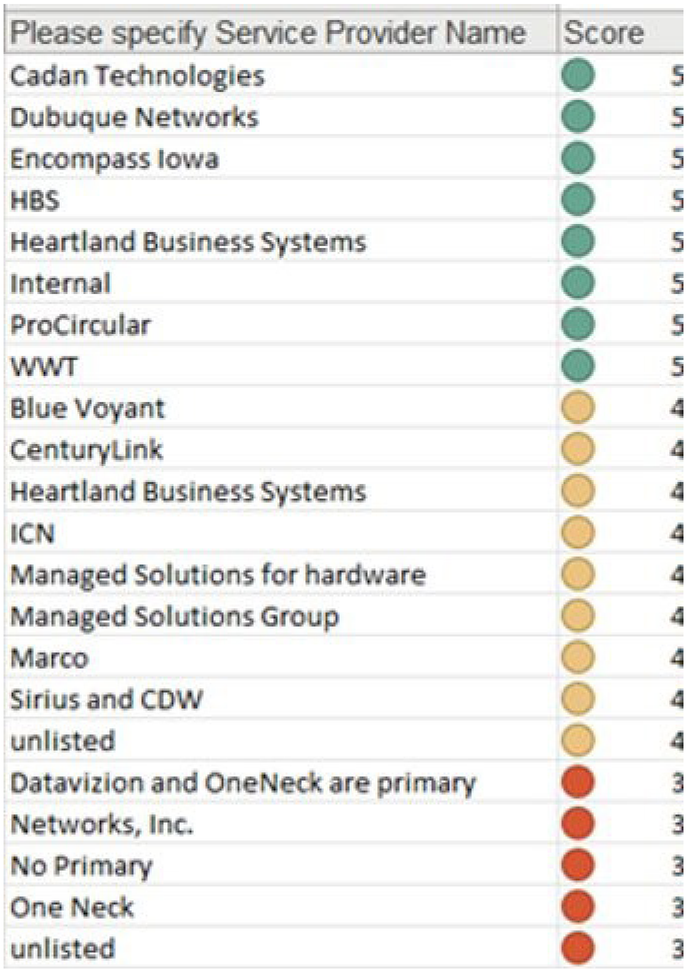


Question 19 – Please rate your I.T. Service Provider



ANSWER CHOICES	RESPONSES	
Very high quality	31.03%	9
High quality	27.59%	8
Neither high nor low quality	41.38%	12
Low quality	0.00%	0
Very low quality	0.00%	0
Total Respondents: 29		

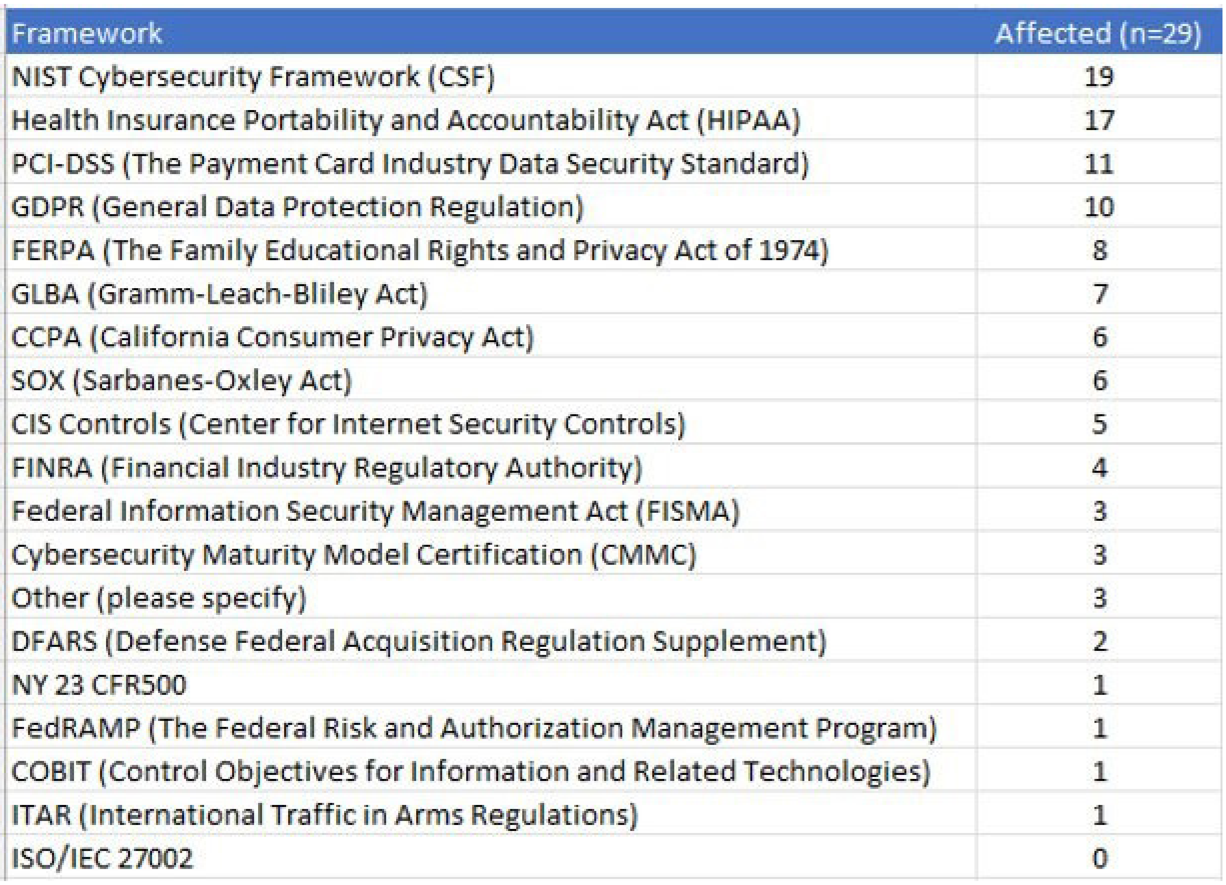
Figure 1 - Generalized I.T. Service Provider Rating



Please specify Service Provider Name	Score	
Cadan Technologies	🟢	5
Dubuque Networks	🟢	5
Encompass Iowa	🟢	5
HBS	🟢	5
Heartland Business Systems	🟢	5
Internal	🟢	5
ProCircular	🟢	5
WWT	🟢	5
Blue Voyant	🟠	4
CenturyLink	🟠	4
Heartland Business Systems	🟠	4
ICN	🟠	4
Managed Solutions for hardware	🟠	4
Managed Solutions Group	🟠	4
Marco	🟠	4
Sirius and CDW	🟠	4
unlisted	🟠	4
Datavizion and OneNeck are primary	🔴	3
Networks, Inc.	🔴	3
No Primary	🔴	3
One Neck	🔴	3
unlisted	🔴	3

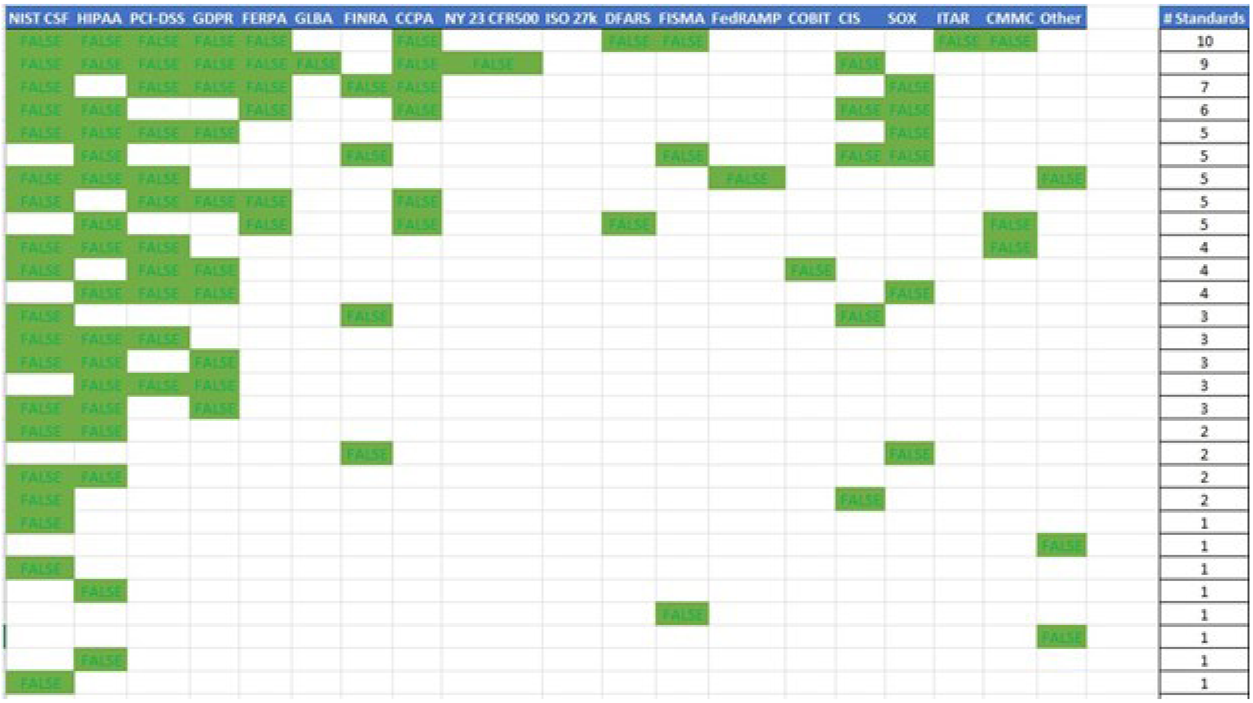
Figure 2 - I.T. Service Provider Ratings

Question 20 – Please check all the compliance standards that likely apply to your organization, or that you've chosen to use internally for your security program.



Framework	Affected (n=29)
NIST Cybersecurity Framework (CSF)	19
Health Insurance Portability and Accountability Act (HIPAA)	17
PCI-DSS (The Payment Card Industry Data Security Standard)	11
GDPR (General Data Protection Regulation)	10
FERPA (The Family Educational Rights and Privacy Act of 1974)	8
GLBA (Gramm-Leach-Bliley Act)	7
CCPA (California Consumer Privacy Act)	6
SOX (Sarbanes-Oxley Act)	6
CIS Controls (Center for Internet Security Controls)	5
FINRA (Financial Industry Regulatory Authority)	4
Federal Information Security Management Act (FISMA)	3
Cybersecurity Maturity Model Certification (CMMC)	3
Other (please specify)	3
DFARS (Defense Federal Acquisition Regulation Supplement)	2
NY 23 CFR500	1
FedRAMP (The Federal Risk and Authorization Management Program)	1
COBIT (Control Objectives for Information and Related Technologies)	1
ITAR (International Traffic in Arms Regulations)	1
ISO/IEC 27002	0

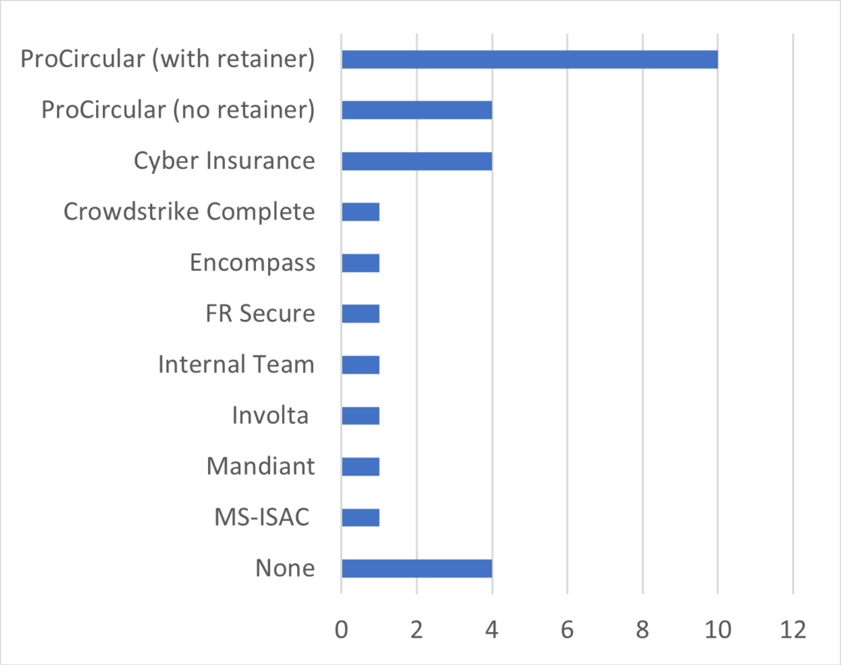
Figure 3 - Companies affected by Compliance



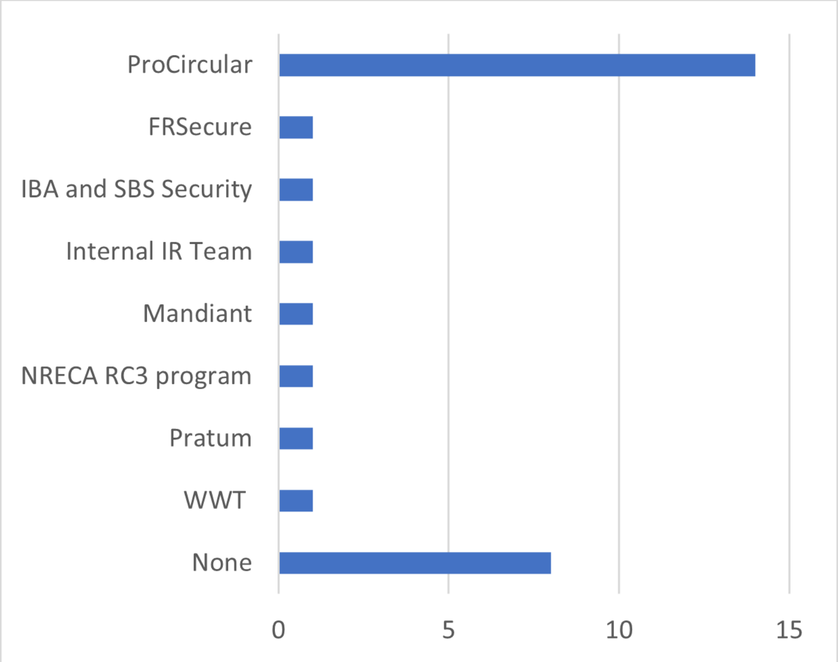
NIST CSF	HIPAA	PCI-DSS	GDPR	FERPA	GLBA	FINRA	CCPA	NY 23 CFR500	ISO 27k	DFARS	FISMA	FedRAMP	COBIT	CIS	SOX	ITAR	CMMC	Other	# Standards
FALSE	FALSE	FALSE	FALSE	FALSE			FALSE			FALSE	FALSE					FALSE	FALSE		10
FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE						FALSE					9
FALSE		FALSE	FALSE	FALSE		FALSE	FALSE								FALSE				7
FALSE	FALSE			FALSE			FALSE							FALSE	FALSE				6
FALSE	FALSE	FALSE	FALSE												FALSE				5
	FALSE					FALSE					FALSE			FALSE	FALSE				5
FALSE	FALSE	FALSE										FALSE						FALSE	5
FALSE		FALSE	FALSE	FALSE			FALSE												5
	FALSE			FALSE			FALSE			FALSE							FALSE		5
FALSE	FALSE	FALSE															FALSE		4
FALSE		FALSE	FALSE										FALSE						4
	FALSE	FALSE	FALSE												FALSE				4
FALSE						FALSE								FALSE					3
FALSE	FALSE	FALSE																	3
FALSE	FALSE		FALSE																3
	FALSE	FALSE	FALSE																3
FALSE	FALSE		FALSE																3
FALSE	FALSE																		2
						FALSE									FALSE				2
FALSE	FALSE																		2
FALSE														FALSE					2
FALSE																			1
																		FALSE	1
FALSE																			1
	FALSE																		1
											FALSE								1
																		FALSE	1
	FALSE																		1
FALSE																			1

Figure 4 - Compliance Heat Map

Question 21 - Who do you use for Incident Response partners? (list as many as apply)

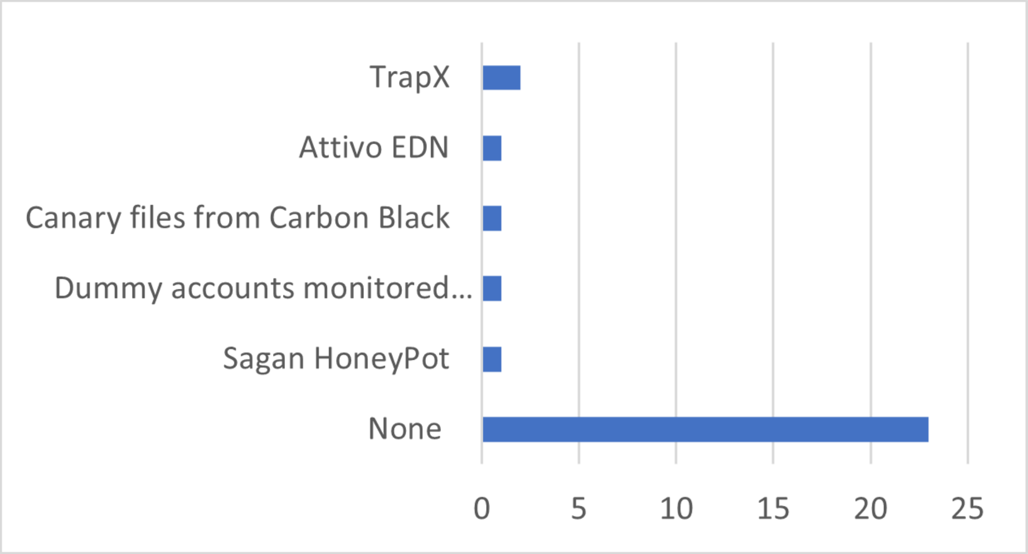


Question 22 - Who do you use for Incident Response Tabletop exercises? (list as many as apply)

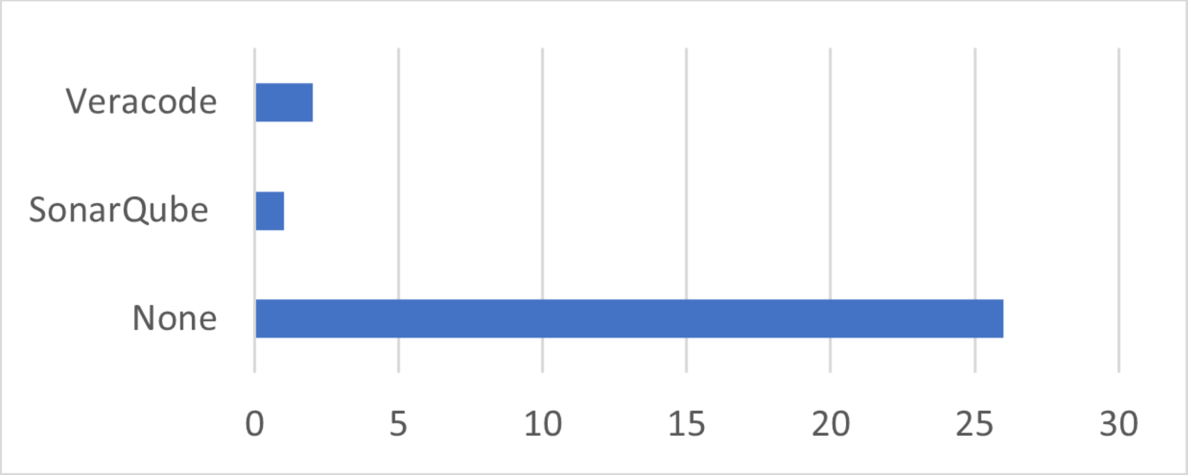


Comments- Loved the escape room, We should conduct tabletops more often, Considering options from ProCircular, Involta, and internal IR teams, Engagements with ProCircular are performed on an annual, bi-annual, and one-off basis.

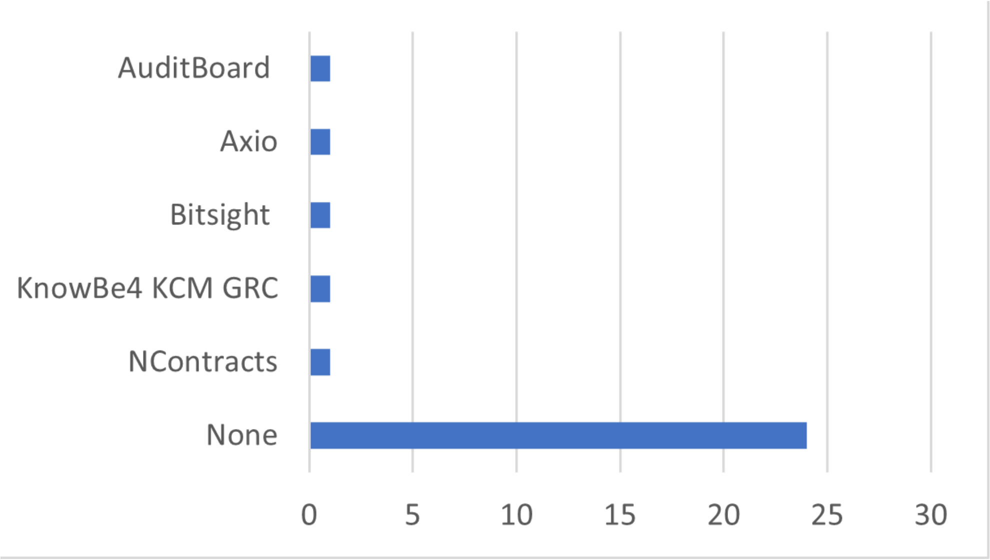
Question 23 - What deceptive technologies do you use? (list as many as apply)



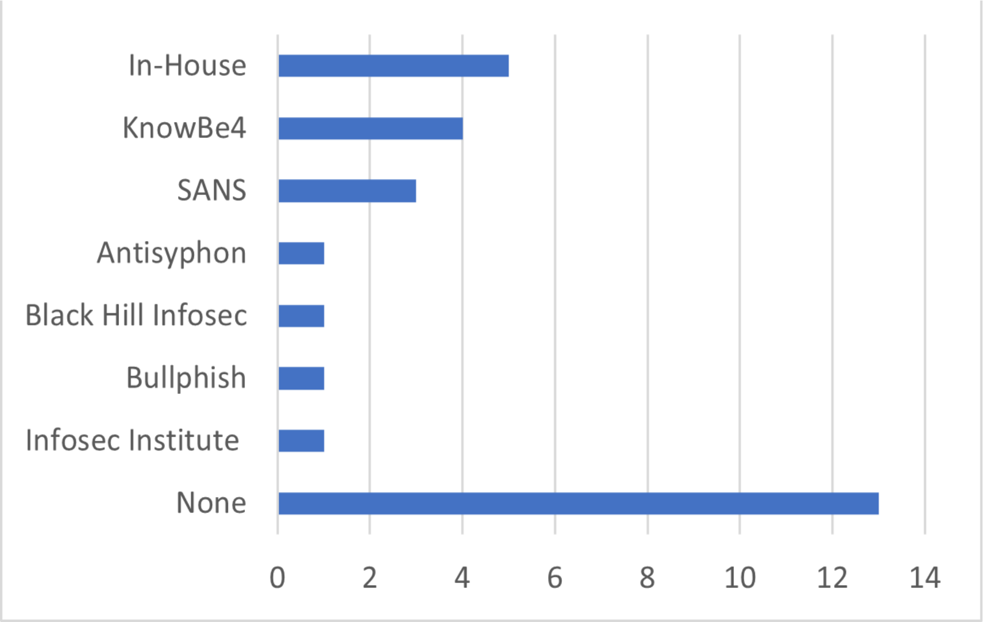
Question 24 - What Code Analysis tools are you using?



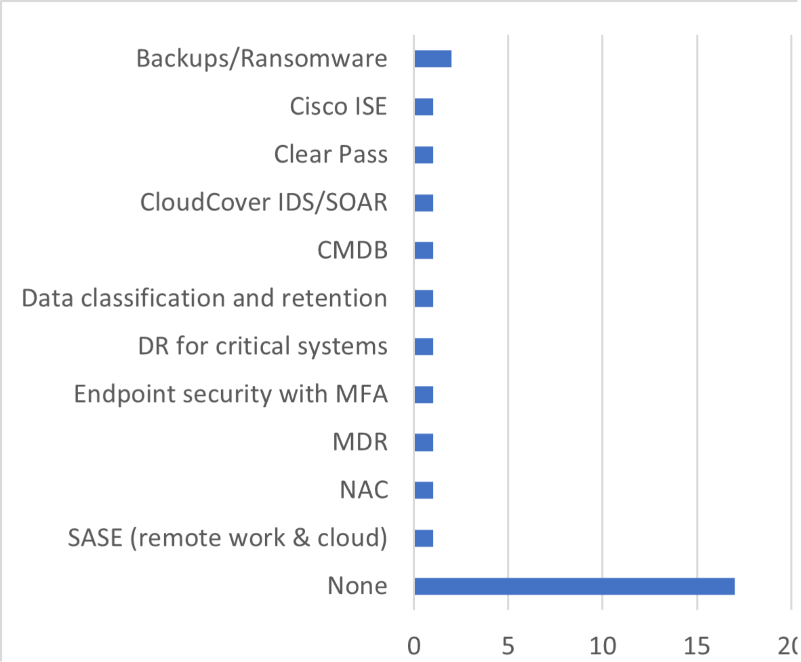
Question 25 - What Risk Management Platforms (GRC) are in use at your organization?



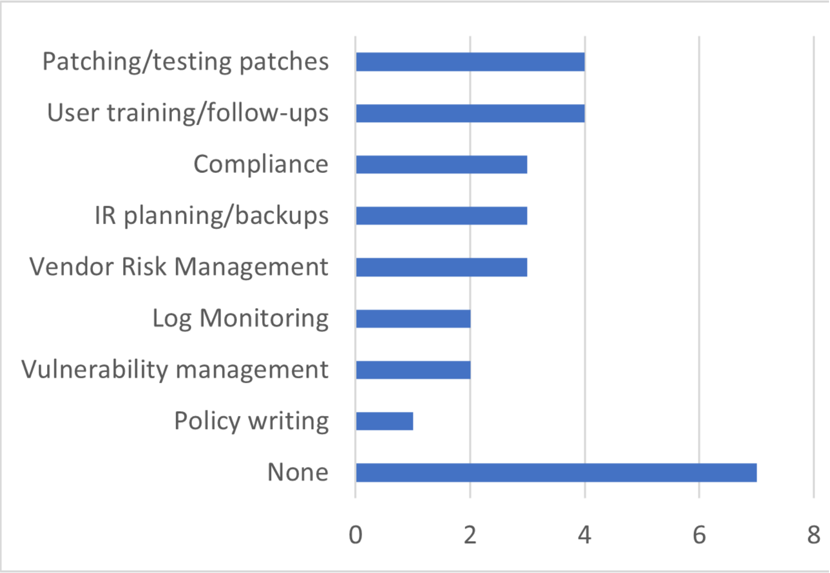
Question 26 - What in-person training are you using for cybersecurity?



Question 27 - What major services or tools have you budgeted for 2022 that are not here? (list as many as apply)



Question 28 - What security task would you get rid of if you could?


Patching/testing patches
User training/follow-ups
Compliance
IR planning/backups
Vendor Risk Management
Log Monitoring
Vulnerability management
Policy writing
None