cynet

THE DEFINITIVE SME CYBERSECURITY PLANNING CHECKLIST

A comprehensive cybersecurity plan for a small to medium-sized enterprise (SME) should include a range of technologies and actions that help address the important aspects of security.

This document provides an easy-to-use checklist for the key services, technologies, and initiatives that most SMEs should consider as part of their cybersecurity program. Each of the 36 items suggested are broken down into the key elements that should be considered for that item. When evaluating your organization's readiness, you should assess the importance of each element as well as the current level of effectiveness. This will provide a status assessment as well as input to your roadmap for improving your organization's cybersecurity posture.

The checklist is generalized and includes the elements that we believe are – or at least should be – common to most organizations. The specific mix of cybersecurity services, technologies, and actions you implement depend on your organization's needs, budget, support staff, and the nature of your operations. There is no one size fits all in security and each security pro should assess which elements best fit the specific conditions of his or her environment. No two organizations are the same and it makes sense to assume there would be a wide variance of needs and responses depending on your industry, team size, organizational culture, and other variables.

A cybersecurity program should also emphasize a defense-in-depth approach, ensuring that multiple layers of security are in place to protect against a wide range of threats. It is also crucial to regularly update and patch technologies to stay protected against evolving threats.

How to use this document:

- Assess the importance of each element to your organization (1 through 5)
- Assess the current effectiveness of each element within your organization
- Prioritize development based on the scoring, budget, and organizational readiness to implement and support needed protections

Summary

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Security Policies and Governance Platforms							
Cybersecurity Training							
Vulnerability Management							
Cybersecurity Incident Response Plan							
Cybersecurity Insurance							
Patch Management Tools							
Threat Intelligence Feeds							
Endpoint Protection (EPP)							
Endpoint Detection And Response (EDR)							
Device Control							
Firewalls							
Virtual Private Networks (VPNs)							
Network Access Controls (NAC)							
Network Detection and Response (NDR)							
Mobile Security							
Email security							
Security information and event management (SIEM)							
Security Orchestration, Automation, and Response (SOAR)							
Intrusion Detection and Prevention Systems (IDPS)							
DNS Filtering							
Web Application Firewall (WAF)							
DDOS Protection							
24*7 Security Analysts / Security Operation Center (SOC) / Managed Detection and response (MDR)							
Incident Response Service							
Darknet Monitoring Services							
User and Entity Behavior Analytics (UEBA)							
Identity and Access Management (IAM)							
Password Management Solutions							
Multi-Factor Authentication (MFA)							
Deception							
Data Backup and Recovery							
Data Loss Prevention (DLP)							
Encryption							
SaaS Security Posture Management (SSPM)							
Cloud Access Security Broker (CASB)							
Container and Microservices Security							

Security Policies and Governance Platforms

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Policy Management and Enforcement: Centralized management of security policies that define how security controls and measures should be implemented. Enforcing policies consistently across the organization ensures a standardized security posture.							
Compliance and Regulatory Alignment: Ensuring that security policies and practices align with industry-specific regulations and compliance requirements (e.g., GDPR, HIPAA, ISO 27001). Conducting regular assessments to confirm adherence to these standards.							
Risk Management and Assessment: Identifying, evaluating, and mitigating security risks that could impact the organization. Developing a risk management framework and conducting regular risk assessments.							
Incident Response and Reporting: Defining procedures for responding to security incidents, breaches, and vulnerabilities. Establishing a clear incident response plan that outlines roles and responsibilities, communication strategies, and containment measures.							
Security Awareness and Training: Implementing ongoing security awareness and training programs for employees and stakeholders. Promoting a culture of security awareness and educating users about best practices and potential threats.satellite communications to steal victims' data.							

Cybersecurity Training

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Phishing and Social Engineering Awareness: Phishing attacks and social engineering techniques are among the most common cybersecurity threats. Training should educate participants on how to recognize and respond to phishing emails, fake websites, and manipulative tactics used by cybercriminals.							
Secure Password Practices: Passwords are a primary line of defense against unauthorized access. Training should cover creating strong, unique passwords, managing credentials securely, and the importance of multi-factor authentication (MFA) for enhanced security.							
Data Protection and Privacy: Understanding how to classify, handle, and protect sensitive data is crucial. Training should cover data privacy regulations (e.g., GDPR, HIPAA) and emphasize the importance of encryption and secure data storage and transmission.							
Safe Browsing and Internet Practices: Teaching individuals to recognize and avoid malicious websites, downloads, and links is essential. This includes topics such as secure web browsing, using reputable sources for software downloads, and avoiding potentially harmful content.							
Incident Response and Reporting: In the event of a cybersecurity incident, individuals should know how to respond and report it effectively. Training should cover the steps to take when an incident occurs, including whom to contact and how to preserve evidence.							

Vulnerability Management

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Vulnerability Scanning and Assessment: Conducting regular vulnerability scans using automated tools to identify weaknesses in the network, systems, and software. These scans provide an initial list of vulnerabilities that need to be addressed.							
Prioritization and Risk Assessment: Assessing the severity and potential impact of identified vulnerabilities is essential. This involves assigning risk scores to vulnerabilities based on factors such as CVSS (Common Vulnerability Scoring System) scores and the potential impact on the organization.							
Patch Management: Developing and implementing a patch management strategy to ensure that identified vulnerabilities are patched in a timely manner. This includes testing patches before deployment to avoid disruptions.							
Compliance and Reporting: Maintaining compliance with industry standards and regulations is often a requirement. Generating reports on the status of vulnerabilities and actions taken is crucial for demonstrating compliance and tracking progress.							
Continuous Monitoring and Remediation: Vulnerability management is an ongoing process. Continuously monitoring the environment for new vulnerabilities, reassessing risks, and promptly remediating vulnerabilities are important for staying secure in a dynamic threat landscape.							

Cybersecurity Incident Response Plan

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Incident Categorization and Severity Classification: Developing a system for categorizing and classifying incidents based on their severity and impact. This helps prioritize responses and allocate resources effectively.							
Incident Detection and Reporting: Defining procedures for detecting and reporting security incidents, including who to contact, what information to gather, and how to initiate the incident response process.							
Incident Response Team Roles and Responsibilities: Assigning roles and responsibilities to members of the incident response team. This includes specifying the functions of incident handlers, incident coordinators, legal experts, and public relations personnel.							
Incident Containment and Eradication: Outlining the steps to take to contain the incident, minimize the damage, and eradicate the threat. This may involve isolating affected systems, removing malware, and restoring services.							
Communication and Reporting: Establishing clear communication procedures for both internal and external stakeholders. This includes how and when to notify senior management, legal authorities, customers, and the public, and the creation of incident reports.							

Cybersecurity Insurance

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Policy Coverage and Limits: Understanding the extent of coverage provided by the cybersecurity insurance policy, including what types of incidents or losses are covered and the policy limits. This may include coverage for data breaches, business interruption, legal costs, and more.							
Risk Assessment and Underwriting: Conducting a thorough risk assessment and providing accurate information to insurers during the underwriting process is essential. Accurate risk assessment helps in tailoring the policy to the organization's specific needs.							
Policy Exclusions: Being aware of policy exclusions is crucial. Insurance policies often have specific exclusions for certain types of incidents or circumstances, so it's important to understand what is not covered.							
Incident Response Planning: Developing an effective incident response plan is not only important for cybersecurity preparedness but also for ensuring that an organization complies with insurance policy requirements in the event of a cyber incident.							
Policy Renewal and Updates: Regularly reviewing and updating the cybersecurity insurance policy to align it with evolving cyber threats and organizational changes is important. This ensures that the policy remains effective and provides adequate coverage.							

Patch Management Tools

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Vulnerability Scanning and Assessment: Efficiently scan and assess systems and software to identify vulnerabilities. Prioritize vulnerabilities based on severity, potential impact, and relevance to your organization.							
Automated Patch Deployment: Automate the process of downloading and deploying patches to affected systems. Schedule and stage patch installations during maintenance windows to minimize disruption.							
Patch Testing and Staging: Provide a mechanism for testing patches in a controlled, isolated environment to ensure they won't disrupt production systems. Enable organizations to validate patches for compatibility and functionality before deployment.							
Reporting and Compliance: Offer robust reporting and monitoring capabilities to track the status of patch deployments. Ensure compliance with industry regulations, internal policies, and security best practices.							
Third-Party Patching: Support patching for not only the operating system and core applications but also third-party software, including web browsers, plugins, and productivity tools. Address vulnerabilities in commonly exploited third-party applications.							

Threat Intelligence Feeds

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Timely and Accurate Threat Data: Access to timely and accurate information on the latest threats, vulnerabilities, and attack techniques. Ensure that the threat intelligence data is relevant and up-to-date.							
Contextual Information: Threat feeds should provide contextual information, including details about the tactics, techniques, and procedures (TTPs) used by threat actors. Context enables security teams to understand the threat's significance and adapt their defenses accordingly.							
Indicators of Compromise (IoC): Deliver IoCs such as IP addresses, URLs, file hashes, and malware signatures associated with specific threats. IoCs help security teams detect and respond to active threats in their environment.							
Actionable Insights: Threat intelligence feeds should provide actionable insights that enable organizations to make informed decisions about their security posture. Recommendations for mitigating specific threats or vulnerabilities are valuable.							
Integration with Security Solutions: Ensure that the threat intelligence feed can be integrated with existing security solutions, such as SIEM platforms, IDS/IPS systems, and firewalls. Integration allows for real-time threat detection and automated responses.							

Endpoint Protection (EPP)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Antivirus and Antimalware: Traditional antivirus and antimalware solutions are foundational in protecting endpoints. These tools scan for and remove known viruses, malware, and other malicious software to prevent infections.							
Endpoint Detection and Response (EDR): EDR solutions offer advanced threat detection and response capabilities. They monitor endpoints for suspicious activities and provide incident response tools to identify and mitigate threats in real-time.							
Patch Management: Keeping operating systems and software up to date with the latest security patches is crucial. Vulnerabilities in unpatched software can be exploited by attackers. Effective patch management is a fundamental aspect of endpoint protection.							
Data Loss Prevention (DLP): DLP tools help prevent sensitive data from being leaked or accessed by unauthorized users. This is especially important for protecting sensitive information on endpoints.							
User Awareness and Training: One of the weakest links in endpoint security is often the end-user. Educating users about security best practices, safe browsing, and recognizing social engineering tactics like phishing can significantly enhance endpoint protection.							

Endpoint Detection And Response (EDR)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Threat Detection and Analysis: This is the core function of EDR. It involves real-time monitoring and analysis of endpoint data to identify suspicious activities and potential security threats. EDR solutions employ various detection methods, such as signature-based, behavioral analysis, and machine learning, to identify threats.							
Incident Response and Investigation: EDR solutions assist in responding to security incidents. They provide tools and capabilities for security teams to investigate the scope of an incident, determine its severity, and take appropriate actions to mitigate and remediate the threat.							
Behavioral Analytics: EDR systems often use behavioral analytics to establish a baseline of normal activity on endpoints and identify anomalies or deviations. This helps in detecting sophisticated, non-signature-based threats and insider threats.							
Forensics and Data Collection: EDR solutions collect extensive data from endpoints, including system logs, file activity, network traffic, and more. This data can be crucial for forensics and post-incident analysis to understand the full extent of a security breach.							
Integration with SIEM and Threat Intelligence: Effective EDR solutions integrate with Security Information and Event Management (SIEM) systems and leverage threat intelligence feeds. This integration enables better correlation of endpoint data with other security information and helps in identifying and responding to threats more effectively.							

Device Control

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Device Inventory and Visibility: Maintaining an up-to-date inventory of all devices connected to the network is fundamental. This includes computers, mobile devices, IoT devices, and more. Visibility into what's connected helps in managing and securing devices effectively.							
Access Control and Authentication: Implementing access control measures ensures that only authorized devices and users can access network resources. This includes strong authentication methods like multi-factor authentication (MFA) and device-level authentication.							
Endpoint Security: Endpoint security solutions, such as antivirus software and endpoint detection and response (EDR) systems, are crucial for protecting individual devices from malware, vulnerabilities, and other threats.							
Policy Enforcement: Defining and enforcing device usage policies is essential. This can include policies regarding which devices are allowed on the network, what they can access, and what security configurations they must adhere to.							
Remote Device Management: As more devices are used remotely or in a bring-your-own-device (BYOD) environment, remote device management is crucial. Tools and policies for managing and securing devices outside the corporate network are essential for maintaining security.							

Firewalls

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Access Control Rules: Define and maintain access control rules that permit or deny traffic based on source and destination IP addresses, ports, protocols, and application-level information. Fine-tune these rules to follow the principle of least privilege, granting only necessary access.							
Application Layer Filtering: Implement deep packet inspection and application layer filtering to identify and block traffic based on specific applications and services, not just ports and protocols. This enables more precise control and protection against application-layer attacks.							
Intrusion Detection and Prevention: Integrate intrusion detection and prevention capabilities to identify and block potentially malicious traffic. Regularly update intrusion signatures and rules to keep the firewall up-to-date with evolving threats.							
Logging and Monitoring: Enable logging and monitoring features to record and analyze network traffic and security events. Use these logs for threat detection, incident response, and compliance reporting.							
High Availability and Redundancy: Implement high availability and failover mechanisms to ensure the firewall's continuous operation. Use redundant hardware, configurations, and network paths to minimize downtime.							

Virtual Private Networks (VPNs)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Security and Encryption: Implement strong encryption protocols and algorithms to protect data in transit. Utilize robust security practices to ensure that only authorized users can access the VPN.							
Authentication and Access Control: Enforce multi-factor authentication (MFA) to verify the identity of users. Implement strict access control measures, allowing users access to only the resources they need.							
Logging and Auditing: Maintain detailed logs of VPN activity to monitor for potential security threats. Regularly review logs and audit VPN usage for security and compliance purposes.							
Privacy and Data Protection: Ensure that the VPN provider has a strict no-logs policy to protect user privacy. Choose a VPN service that is located in a jurisdiction with strong data protection laws.							
Redundancy and High Availability: Implement redundant VPN servers and failover mechanisms to ensure service availability. Plan for business continuity, even in the event of a server or data center failure.							

Network Access Controls (NAC)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Access Control Policies: Define and enforce access control policies that determine which devices and users can access the network. Specify the level of access and permissions based on user roles and device types.							
Device Identification and Authentication: Identify and authenticate devices and users seeking access to the network. Use various authentication methods, including username/password, certificates, and multi-factor authentication (MFA).							
Endpoint Security Posture Assessment: Conduct security posture assessments on devices attempting to connect to the network to ensure they meet security requirements. Assess factors like up-to-date antivirus, patch levels, and compliance with security policies.							
Guest Network Access: Provide controlled and isolated guest network access for visitors or non-employee users. Enforce policies to separate guest traffic from the main network and limit their access.							
Integration with Security Tools: Integrate NAC solutions with other security tools and systems, such as intrusion detection systems, firewalls, and SIEM platforms, to enhance threat detection and response. Leverage threat intelligence feeds and anomaly detection to identify and respond to network security threats.							

Network Detection and Response (NDR)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Traffic Analysis and Monitoring: Comprehensive monitoring and analysis of network traffic is at the core of NDR. This includes real-time analysis of packet-level data, flow data, and logs to identify anomalies and threats.							
Behavioral Analytics: NDR solutions use behavioral analytics to establish a baseline of normal network activity and identify deviations that may indicate suspicious or malicious behavior. Understanding and recognizing these anomalies is key to early threat detection.							
Threat Detection and Alerting: NDR tools should be able to detect various threats, such as malware, data exfiltration, lateral movement, and unauthorized access. Effective alerting and reporting mechanisms help security teams respond promptly.							
Network Segmentation and Micro-Segmentation: Proper network segmentation can limit lateral movement of attackers and reduce the potential impact of a breach. Understanding and implementing segmentation strategies is essential in NDR.							
Integration with Other Security Tools: Effective NDR systems should integrate with other security technologies, such as SIEM (Security Information and Event Management) solutions, endpoint detection and response (EDR) tools, and threat intelligence feeds. Integration allows for a more holistic approach to network security.							

Mobile Security

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Operating System Updates: Keeping the mobile operating system (e.g., Android, iOS) up to date is vital. Operating system updates often include patches for security vulnerabilities, so ensuring that devices are running the latest version is a fundamental security practice.							
App Security: The security of mobile applications is crucial. Topics within this category include app permissions, source verification, and regular updates. Users should review the permissions they grant to apps and be cautious about installing apps from unverified sources.							
Device Encryption: Enabling device-level encryption helps protect the data stored on the device. Full-disk encryption ensures that even if the device is lost or stolen, the data remains inaccessible without the proper credentials.							
Network Security: This encompasses various aspects, including secure Wi-Fi usage, VPN (Virtual Private Network) usage for public networks, and the avoidance of connecting to untrusted or rogue Wi-Fi hotspots, which can be used for eavesdropping and other malicious activities.							
Mobile Malware Protection: Mobile devices are not immune to malware. Utilizing mobile security software or antivirus apps can help detect and prevent malware infections. Users should also be cautious about sideloading apps from unofficial sources.							

Email security

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Phishing Protection: Phishing attacks involve tricking users into revealing sensitive information or clicking on malicious links. Email security measures, such as anti-phishing filters and user training, are crucial to detect and prevent phishing attempts.							
Authentication and Authorization: Implementing robust authentication protocols like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) helps verify the legitimacy of email senders and reduce the risk of email spoofing and impersonation.							
End-to-End Encryption: Encrypting email messages from sender to recipient ensures that the content remains private and secure. Technologies like S/MIME (Secure/Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy) can be used for end-to-end encryption.							
Security Awareness and Training: One of the weakest links in email security is often the human element. Regular training and awareness programs can help educate users about email security best practices and how to recognize suspicious emails.							
Zero-Day Threat Protection: Zero-day vulnerabilities are exploits that are unknown to the vendor and, therefore, unpatched. Email security solutions should include features that protect against these types of threats, such as advanced threat detection and sandboxing.							

Security information and event management (SIEM)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Log and Event Collection: Properly collecting logs and security events from various sources, such as network devices, servers, applications, and endpoints, is the foundation of SIEM. Understanding log formats, sources, and protocols is essential.							
Event Correlation and Analysis: SIEM systems use event correlation and analysis to detect patterns and anomalies in security data. This involves creating rules and using threat intelligence to identify potentially malicious activity.							
Alerting and Incident Response: Setting up alerting mechanisms to notify security teams when specific events or patterns of events are detected. Additionally, having incident response workflows integrated with SIEM for prompt action upon alerts.							
Log Storage and Retention: Storing logs and event data for an appropriate duration is important for compliance, forensic investigations, and analysis. Understanding log retention policies and archiving mechanisms is crucial.							
Compliance and Reporting: SIEM is often used to demonstrate compliance with various regulations and standards. Generating compliance reports and providing audit trails for security events are important aspects of SIEM.							

Security Orchestration, Automation, and Response (SOAR)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Security Orchestration, Automation, and Response (SOAR): SOAR platforms are designed to streamline security operations by automating tasks like incident response, threat hunting, and alert triage. They integrate with various security tools and enable security teams to respond to threats more efficiently.							
Threat Intelligence Automation: Automating the ingestion, analysis, and dissemination of threat intelligence feeds helps organizations stay updated on emerging threats and vulnerabilities, allowing them to proactively adapt their security measures.							
Vulnerability Management Automation: Automation can assist in the discovery, prioritization, and remediation of vulnerabilities in a network. This includes automating vulnerability scans, patch management, and compliance checks.							
User and Entity Behavior Analytics (UEBA): Automation in UEBA helps identify abnormal user and entity behavior patterns. Automated alerts and response actions can quickly flag and mitigate potential insider threats or compromised accounts.							
Automated Incident Response Playbooks: Defining and automating incident response playbooks can reduce response times and improve consistency in addressing security incidents. Playbooks may include steps for containing and eradicating threats, as well as communication protocols.							

Intrusion Detection and Prevention Systems (IDPS)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Signature-Based Detection: Signature-based detection involves comparing network traffic and system activities to known attack patterns or signatures. It's important for identifying well-known threats and attacks that have been previously documented.							
Anomaly-Based Detection: Anomaly-based detection focuses on identifying deviations from established baseline behavior. It is valuable for detecting novel or zero-day attacks that lack known signatures.							
Real-Time Alerting and Response: IDPS should provide real-time alerts and, in some cases, automated responses to detected threats. Timely response is critical for mitigating potential damage caused by intrusions.							
Network and Host-Based IDPS: Network-based IDPS monitors network traffic and detects threats at the network level. Host-based IDPS focuses on individual host systems and their logs for signs of intrusion. A combination of both provides a more comprehensive security posture.							
Tuning and False Positive Management: Effective IDPS requires ongoing tuning and management to reduce false positives (non-malicious events mistakenly identified as threats) and improve detection accuracy. Fine-tuning the system helps it focus on genuine threats and avoid alert fatigue.							

DNS Filtering

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Malware and Phishing Protection: DNS filtering is often used to block access to malicious websites and prevent users from inadvertently visiting sites hosting malware, phishing attacks, or other malicious content.							
Content Filtering: Organizations use DNS filtering to control the types of websites and content that users can access. This helps enforce acceptable use policies, improve productivity, and maintain a safe online environment.							
Threat Intelligence Integration: Effective DNS filtering services integrate with threat intelligence feeds to stay up-to-date on emerging threats and malicious domains. Real-time threat feeds and blacklists help block access to known malicious sites.							
Data Loss Prevention (DLP): DNS filtering can be used to prevent data exfiltration by blocking access to cloud storage and file-sharing services or sensitive data leakage points. This is especially important for organizations that need to protect confidential information.							
Customization and Reporting: DNS filtering solutions should offer customization options to tailor filtering policies to an organization's specific needs. Robust reporting and analytics tools help administrators monitor web traffic, identify trends, and fine-tune filtering rules.							

Web Application Firewall (WAF)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Threat Detection and Mitigation: Understanding and mitigating common web application threats, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other OWASP Top Ten vulnerabilities, is paramount. Effective threat detection and real-time mitigation are core functions of WAFs.							
Security Policy Configuration: Properly configuring security policies is essential. This involves defining rules and policies that specify what is allowed or blocked, as well as customizing WAF settings to meet the specific needs of the web application.							
Logging and Monitoring: Comprehensive logging and monitoring capabilities are vital for tracking and responding to security events. This includes monitoring web traffic, generating alerts for suspicious activities, and providing detailed logs for forensic analysis.							
Attack Signature and Pattern Updates: Staying up to date with the latest attack signatures and patterns is critical. Regular updates are essential to ensure that the WAF can effectively identify and block new and evolving threats.							
Incident Response Integration: Integrating the WAF with an organization's incident response processes is important. Security teams should know how to respond to WAF alerts and incidents, including the steps for investigation, containment, and eradication.							

DDOS Protection

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Traffic Scrubbing and Mitigation: Implementing traffic scrubbing and mitigation solutions to filter out malicious traffic is crucial. This includes employing DDoS protection services that can differentiate legitimate traffic from attack traffic and block or redirect the latter.							
Anomaly Detection and Traffic Analysis: Using advanced traffic analysis and anomaly detection techniques to identify abnormal traffic patterns, which may indicate the presence of a DDoS attack. This includes monitoring for sudden spikes in traffic or unusual behavior.							
Load Balancing and Redundancy: Implementing load balancing and redundancy across multiple servers and data centers can help distribute traffic and absorb the impact of DDoS attacks, ensuring that services remain available even during an attack.							
Content Delivery Network (CDN) Integration: Leveraging CDNs to distribute content and cache data can help absorb DDoS traffic and maintain service availability. CDNs often have built-in DDoS protection capabilities.							
Incident Response Planning: Developing an incident response plan that outlines the steps to take during a DDoS attack is vital. This includes communication procedures, roles and responsibilities, and strategies for mitigating the impact of the attack.							

24*7 Security Analysts / Security Operation Center (SOC) / Managed Detection and response (MDR)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Continuous Monitoring and Alert Triage: Security analysts need to continuously monitor security alerts and events, prioritize them based on severity and relevance, and investigate potential security incidents promptly.							
Incident Detection and Response: The ability to rapidly detect and respond to security incidents is a core function. This includes defining and implementing incident response processes, containing threats, eradicating malicious activity, and recovering systems.							
Threat Hunting: Proactive threat hunting involves actively searching for signs of compromise or vulnerabilities within the network. This requires a deep understanding of attacker techniques, as well as the use of threat intelligence and analytics to identify potential threats before they cause damage.							
Security Tool Expertise: Security analysts in SOCs and MDR services should be proficient with various security tools, including SIEM platforms, EDR solutions, and threat detection technologies. They should be able to use these tools effectively for monitoring and responding to threats.							
Threat Intelligence Integration: Incorporating threat intelligence into security operations is crucial. Analysts should be familiar with various threat feeds, understand their relevance to the organization's industry, and use this intelligence to improve detection and response capabilities.							

Incident Response Service

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Incident Classification and Prioritization: Properly classifying and prioritizing security incidents is crucial. Security teams should have a clear understanding of the types of incidents that can occur, their impact, and how to prioritize them for an effective response.							
Incident Detection and Alerting: Implementing robust monitoring solutions, such as Security Information and Event Management (SIEM) systems, intrusion detection systems (IDS/IPS), and endpoint detection and response (EDR) tools, is essential for early incident detection. Security teams must be well-versed in analyzing alerts and recognizing signs of compromise.							
Incident Response Playbooks: Developing and maintaining incident response playbooks helps guide the response process. These playbooks outline specific steps to take when different types of incidents occur, facilitating a faster and more effective response.							
Forensics and Investigation: Conducting thorough investigations to determine the scope and impact of security incidents is a critical topic. This involves collecting and analyzing digital evidence, identifying the root cause, and understanding how the incident occurred.							
Communication and Coordination: Effective communication within the incident response team and with external stakeholders is vital. This includes coordinating actions, sharing information, and ensuring that the incident response process aligns with business continuity and legal requirements.							

Darknet Monitoring Services

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Threat Intelligence Gathering: Collecting and analyzing data from the darknet to identify emerging threats, vulnerabilities, and malicious activities. Monitoring underground forums, marketplaces, and chat rooms to stay informed about potential security risks.							
Data Leak and Breach Detection: Identifying stolen or leaked data, including sensitive company information or customer credentials, on the darknet. Promptly notifying the organization when its data appears on the darknet, enabling quick response and mitigation.							
Criminal Marketplace Monitoring: Keeping an eye on criminal marketplaces for the sale of illegal goods, such as stolen data, malware, and hacking tools. Monitoring discussions related to cyberattacks, fraud, and other illicit activities.							
Deep and Dark Web Takedowns: Collaborating with law enforcement agencies to initiate takedowns of illicit websites or forums. Reporting illegal activities to appropriate authorities to prevent further harm and protect potential victims.							
Security Awareness and Preparedness: Providing organizations with actionable insights to strengthen their cybersecurity defenses based on the observed threats and vulnerabilities on the darknet. Educating security teams and employees about emerging risks and best practices for avoiding exposure.							

User and Entity Behavior Analytics (UEBA)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Behavioral Analysis: UEBA solutions employ behavioral analysis to establish baselines of normal behavior for users and entities. Understanding what "normal" looks like is crucial for identifying deviations and anomalies that may indicate security incidents.							
User Activity Monitoring: Continuously monitoring user activities, such as logins, file access, application usage, and network traffic, is a key component of UEBA. This helps in identifying unusual or suspicious user behavior.							
Entity Behavior Analysis: In addition to users, UEBA also focuses on entities, which can include devices, servers, applications, and other network elements. Monitoring entity behavior helps detect unusual activities that could be indicative of threats like malware infections.							
Machine Learning and Advanced Analytics: UEBA relies on machine learning and advanced analytics to analyze vast amounts of data and identify patterns, anomalies, and potential threats that may be difficult to detect using traditional methods.							
Alerting and Incident Response: UEBA solutions generate alerts when unusual behavior or anomalies are detected. Security teams must be trained to respond to these alerts promptly, investigate potential incidents, and take appropriate actions to mitigate threats.							

Identity and Access Management (IAM)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Identity Lifecycle Management: Managing the entire lifecycle of user identities, which includes onboarding, maintaining, and offboarding users. Ensuring that access rights align with users' roles and responsibilities throughout their tenure within the organization.							
Access Control and Authorization: Defining and enforcing access control policies to determine who can access what resources. Implementing role-based access control (RBAC) or attribute-based access control (ABAC) to assign appropriate levels of access to users.							
Authentication and Password Management: Establishing secure authentication processes, often involving username and password, but also incorporating stronger authentication methods, such as multi-factor authentication (MFA). Enforcing password policies for complexity, expiration, and resetting.							
Audit and Monitoring: Maintaining detailed logs of user activities and access permissions to enable oversight, compliance, and security monitoring. Continuously monitoring user behavior and access patterns to detect and respond to unauthorized or suspicious activities.							
Compliance and Governance: Ensuring that IAM practices comply with relevant regulations, industry standards, and organizational policies. Conducting regular security assessments, audits, and reviews to confirm compliance and identify areas for improvement.							

Password Management Solutions

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Password Complexity and Policies: Implement and enforce robust password policies that dictate complexity requirements, including length, character types, and expiration periods. Customize password policies to meet security standards and organizational needs.							
Password Storage and Encryption: Securely store user passwords using hashing and salting techniques to protect them from unauthorized access. Use strong encryption algorithms to safeguard stored credentials.							
Self-Service Password Reset (SSPR): Enable users to reset their own passwords securely through self-service portals or authentication mechanisms like email or SMS. Reduce the burden on IT support for password-related issues.							
Multi-Factor Authentication (MFA): Integrate MFA options, such as one-time passwords (OTP), biometrics, or hardware tokens, to enhance user authentication. Require users to provide multiple forms of identification to access accounts and systems.							
Audit and Reporting: Maintain detailed logs of password-related activities, including password changes, reset attempts, and failed logins. Use auditing and reporting features to monitor and investigate security incidents and maintain compliance with industry regulations.							

Multi-Factor Authentication (MFA)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Authentication Methods: Understanding the various authentication methods available for MFA, including something you know (passwords), something you have (tokens, smart cards), and something you are (biometrics), and selecting the most appropriate methods for your organization.							
Enrollment and Onboarding: Educating users on the MFA setup process, which may include enrollment and registration for MFA methods. Providing clear instructions and support during this phase is crucial.							
Management and Access Policies: Defining access policies and management processes for MFA, including how and when MFA should be used, user access controls, and exceptions (if any). This helps establish the security boundaries for MFA.							
Integration with Applications: Integrating MFA into the various applications and systems used by an organization. Understanding the integration options and ensuring that MFA is effectively applied to all relevant resources.							
User Training and Awareness: Educating users on the importance of MFA, how to use it, and best practices for protecting MFA tokens or devices. User awareness is essential for the successful implementation of MFA.							

Deception

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Deception Techniques: Understanding various deception techniques, such as honeypots, honey tokens, and honey files, and their application in creating attractive targets for attackers.							
Deception Infrastructure: Establishing and managing a deception infrastructure, which includes deploying decoy systems, networks, and services designed to attract and trap attackers.							
Attack Surface Reduction: Using deception to reduce an organization's attack surface by diverting attackers away from legitimate assets and towards decoys, thus minimizing the risk to critical systems.							
Alerting and Incident Response: Developing efficient alerting mechanisms for the detection of attacks on deceptive assets and establishing clear incident response procedures for handling and investigating incidents involving the deceptive infrastructure.							
Integration with Security Operations: Integrating cybersecurity deception into broader security operations, including SIEM (Security Information and Event Management), incident response, and threat intelligence, to provide a comprehensive defense strategy.							

Data Backup and Recovery

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Data Backup Strategies: Understanding and implementing different backup strategies, including full backups, incremental backups, and differential backups. Organizations should determine which strategy is suitable for their data and recovery needs.							
Backup Frequency and Retention: Deciding how often data should be backed up and for how long backup copies should be retained. Balancing the need for data recovery with storage capacity and compliance requirements is essential.							
Data Recovery Procedures: Developing clear and tested data recovery procedures for various types of data loss scenarios, including accidental deletion, hardware failures, and disaster recovery. This includes both file-level and system-level recovery plans.							
Off-Site and Cloud Backup: Implementing off-site or cloud backup solutions to protect data from physical disasters like fires, floods, or theft. Choosing secure and reliable off-site or cloud storage providers is crucial.							
Testing and Monitoring: Regularly testing the backup and recovery processes to ensure that backups are successful and recovery can be achieved within an acceptable timeframe. Continuous monitoring of the backup system's health and performance is also important.							

Data Loss Prevention (DLP)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Data Discovery and Classification: Identify and classify sensitive data across your organization, including personally identifiable information (PII), financial data, intellectual property, and other critical information. Tag and label data with appropriate sensitivity levels.							
Policy Definition and Enforcement: Define and enforce policies that dictate how sensitive data should be handled, stored, and shared. Create rules that trigger alerts or block data transmission based on policy violations.							
Endpoint and Network Monitoring: Monitor data movement across both endpoints (computers, mobile devices) and the network to detect potential data breaches. Implement both content inspection and contextual analysis to understand the context of data usage.							
Incident Response and Reporting: Establish an incident response plan for addressing data breaches or policy violations. Implement alerting and reporting mechanisms to notify security teams and management of incidents in real-time.							
User Education and Awareness: Educate employees about the importance of data protection and the organization's DLP policies. Promote a culture of security awareness to reduce accidental data leaks.							

Encryption

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Strong Encryption Algorithms: Implement robust encryption algorithms, such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography), to protect data from unauthorized access. Regularly update encryption algorithms and key lengths to stay resistant to evolving threats.							
Key Management: Develop and implement a sound key management strategy to securely generate, store, and distribute encryption keys. Rotate encryption keys regularly to reduce the risk of key compromise.							
End-to-End Encryption: Ensure end-to-end encryption for data transmission to protect data from interception or eavesdropping. Use secure communication protocols like TLS/SSL to establish encrypted connections for web traffic and email.							
Data-at-Rest Encryption: Encrypt data when it is stored, whether on local devices, servers, or in the cloud. Implement full-disk encryption or file-level encryption to safeguard sensitive data from unauthorized access, even if physical access is gained to the storage medium.							
Compliance and Regulations: Adhere to industry-specific regulations, data protection laws, and compliance standards relevant to your organization. Ensure that encryption practices align with regulatory requirements, such as GDPR or HIPAA, for handling sensitive data.							

SaaS Security Posture Management (SSPM)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Cloud Application Discovery and Inventory: Understanding what SaaS applications are in use across the organization is essential. It helps in gaining visibility into potential shadow IT and assessing the security risks associated with each application.							
User Access and Permissions: Managing user access and permissions for SaaS applications is crucial. It involves ensuring that users have the appropriate level of access to data and functionality, implementing role-based access control, and regularly reviewing and revoking access for employees who no longer need it.							
Data Protection and Encryption: Protecting sensitive data within SaaS applications is paramount. Topics include encrypting data at rest and in transit, data loss prevention (DLP), and monitoring data usage to detect and prevent unauthorized sharing.							
Security Configuration Assessment: Regularly assessing and aligning the security configurations of SaaS applications with best practices and compliance standards is vital. This includes settings related to identity and access management, authentication, and other security features.							
Compliance and Risk Management: Ensuring that SaaS applications comply with relevant industry standards and regulations is a key aspect. SaaS Security Posture Management should help identify and mitigate risks associated with non-compliance.							

Cloud Access Security Broker (CASB)

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Visibility and Control: Visibility into all cloud services and applications used within the organization.Control over data and access policies, including monitoring and enforcement of security policies for cloud services.							
Data Protection and Encryption: Data loss prevention (DLP) capabilities to prevent unauthorized sharing or leakage of sensitive data. Encryption of data at rest and in transit to protect it from potential breaches.							
Compliance and Governance: Ensuring compliance with industry-specific regulations (e.g., GDPR, HIPAA) and internal governance policies. Monitoring and auditing cloud activities to maintain regulatory compliance.							
Threat Detection and Response: Real-time threat detection and response for cloud applications, including identifying and mitigating suspicious activities and potential security breaches. Integration with Security Information and Event Management (SIEM) systems for a comprehensive security posture.							
Identity and Access Management: Implementing strong authentication and access controls, including single sign-on (SSO) for cloud applications. Managing user identities, roles, and permissions to prevent unauthorized access.							

Container and Microservices Security

	Level of Importance	Current Effectiveness					
	(1 to 5)	Great	Good	Okay	Bad	Very Bad	None
Image Security: Ensure the security of container images by scanning for vulnerabilities in the underlying software and dependencies. Regularly update and patch base images and libraries to mitigate known vulnerabilities.							
Runtime Security: Implement runtime security controls to monitor and protect containers and microservices during execution. Utilize security tools and practices, such as network segmentation, access control, and runtime monitoring, to detect and respond to threats.							
Orchestration Security: Secure container orchestration platforms, such as Kubernetes, by following best practices and applying proper access controls. Regularly audit configurations and manage secrets and sensitive data securely.							
Identity and Access Management: Enforce strong authentication and authorization mechanisms to control access to microservices and containers. Implement role-based access control (RBAC) to limit permissions based on user roles and responsibilities.							
Logging and Monitoring: Establish robust logging and monitoring for containerized applications and microservices. Use centralized logging and monitoring solutions to detect and respond to security incidents, including unusual behavior or unauthorized access.							

Need Any Help?

If you have any questions or would like some expert help in completing/prioritizing the checklist, feel free to contact us. Cynet specializes in helping SMEs stay safe from cyberthreats – without breaking the bank and without the need for a large, skilled security team.

Cynet was built with lean security teams in mind, as a natively automated, end-to-end security platform, backed by a 24/7 MDR service. With Cynet, comprehensive cybersecurity is stressless and transparent.

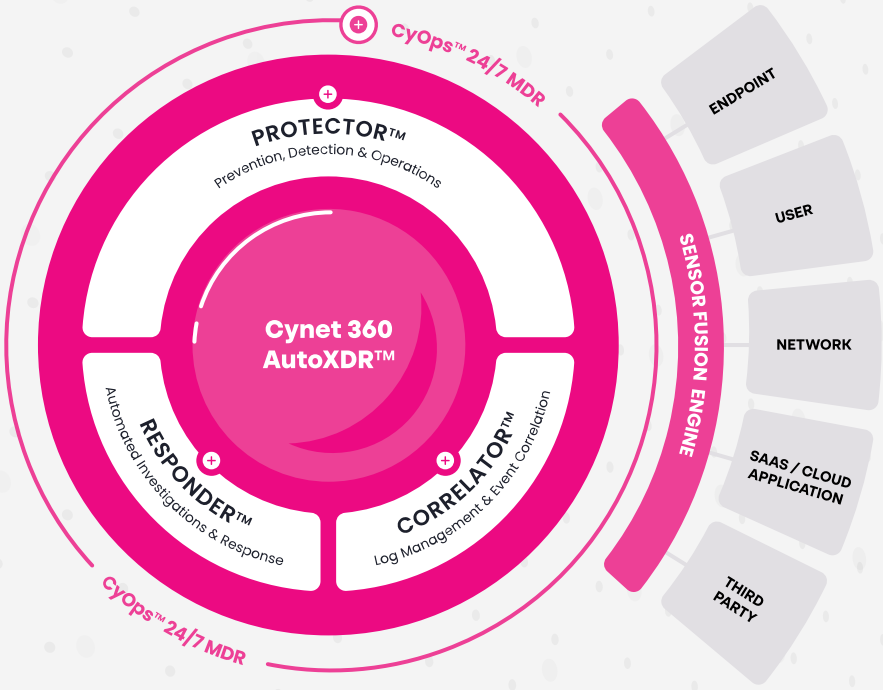
About Cynet

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.

Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.



Learn more