INNOVATIVE PROTECTION: CISCO BREACH SUITE WITH FORTISX MDR

How Cisco Breach Suite with FortisX Managed Detection and Response (MDR) Defend Against Ransomware, Extortionware, and BEC.

By Robert Keblusek, Sentinel Chief Innovation & Technology Officer

Overview

Sentinel and Fortis by Sentinel assist clients daily in safeguarding their on-premises and cloud environments against rising ransomware threats and data breaches. Attackers continuously target users through increasingly sophisticated threats, taking advantage of innovative technologies such as generative artificial intelligence (AI) to enhance phishing and social engineering methods. This enables them to create customized attacks that frequently include deepfakes, behavior analysis, and social media manipulation. Despite substantial cyber awareness training efforts, enterprises still fall prey to cyberattacks primarily due to human mistakes, which Verizon reports amount to 74% of all breaches (Verizon, 2023 Data Breach Investigations Report).

Often users who are deceived by these attacks become the unwitting victims of credential compromise. According to Microsoft, it takes an average of 1 hour and 12 minutes for an attacker to access private data after a person falls for a phishing email (Microsoft, New Windows 11 security features are designed for hybrid work, 2022). Attackers use a mix of technical exploitation, social engineering, and psychological manipulation to bypass or coerce users into bypassing multifactor authentication (MFA), making it inadequate to prevent ransomware events on its own.

The emergence of extortionware, where malicious actors steal and threaten to expose data without encrypting it, has made the risks higher than ever. Security and Risk Management (SRM) leaders need to strengthen their defenses and improve their response strategies to effectively deal with these threats. Additionally, business email compromise (BEC) is on the rise and highly

targeted attacks made possible by AI are continuing to increase the speed and complexity of these attacks.

No matter if an organization is dealing with ransomware, extortionware, or BEC, a strong and complete lifecycle plan for prevention, detection, response, and recovery is essential. The recovery portion in particular often goes ignored and/or fails to undergo regular testing, which can result in major failures when a real incident occurs. FortisX managed detection and response, when combined with Cisco's Breach Suite of solutions (XDR, Secure Cloud Analytics, Secure Network Analytics, Secure Endpoint Protection, Advanced Cloud Email Threat Defense all powered by AI), creates that critical protection lifecycle to identify and stop attacks quickly then aid in the recovery process.

Threat Protection

Generative AI and services such as WormGPT increase the risks of ransomware, extortionware, and BEC by using advanced language models to produce realistic phishing emails, generate harmful code, and create persuasive social engineering attacks. The SANS institute reported that ransomware cases rose by 73% in 2023, indicating that current measures are insufficient to stop these types of threats (SANS Institute, Ransomware Cases Increased by 73% in 2023 showing are actions have not been enough to thwart the threat, 2023). Organizations need to improve their cyber defense strategies and implement advanced and automated responses that work at machine speed. Human response alone is no longer sufficient.

Cisco's Breach Suite combines important building blocks for a strong foundation to protect against these cyber threats. Through Cisco's Breach Suite, organizations can deploy a set of protection services that work together to identify and respond to threats no matter where they occur, including corporate networks, cloud services, and work from anywhere environments. The suite also includes extended detection and response (XDR) that works not only with Cisco's own security tools, but also many tools from leading vendors such as Crowdstrike, Microsoft, Palo Alto, SentinelOne, Fortinet, and more. Cisco Breach Suite includes:

· Cisco XDR with Secure Cloud Analytics

· Cisco Network Virtual Module

· Advanced Threat Intelligence (powered by Cisco Talos)

· Cisco Secure Endpoint

· Cisco Identity Threat Detection and Response

· Cisco Cloud Email Threat Defense

· Cisco Secure Network Analytics

· Support for over 25 additional no cost and premium threat intelligence sources

The combination of these solutions provides an excellent foundation for organizations to begin their security transformation journey to modernize for today’s most advanced attacks.

Cisco XDR with Secure Cloud Analytics

According to Gartner researchers, it is essential for organizations to deploy “behavioral-anomaly-based detection technologies to identify ransomware attacks early” (Gartner, How to Prepare for Ransomware Attacks, 2024).

Cisco XDR offers a comprehensive and integrated threat detection and response platform specifically designed for SecOps teams and FortisX MDR. This platform addresses the critical need to counter evolving cyber threats with machine-speed efficiency. Cisco XDR utilizes an extensive data lake that processes over 400 billion signals daily, in conjunction with threat intelligence from Cisco Talos, the world's largest non-governmental threat intelligence organization. Powered by advanced AI and machine learning technologies, Cisco XDR enhances threat detection, provides sophisticated AI-driven reporting, and includes a new AI assistant to enable SecOps teams to respond more rapidly and accurately.

Cisco XDR integrates nicely with the entire range of Cisco products, and supports other top third-party security providers as well. With Cisco XDR, you are not limited to a single vendor's product in various areas such as endpoint, email, edge/firewall, cloud, and network. Cisco's neutral approach to threat detection and response is tightly connected via APIs to provide fast detection analytics & correlation that create a full attack chain based on MITRE ATT&CK attack technique and procedures (ATPs) with automated remediation and containment playbooks.

Cisco XDR uses Secure Cloud Analytics (SCA), previously Stealthwatch Cloud, to implement the behavior-based detection that Gartner recommends. This adds security by finding abnormal behaviors that might signal a threat. This is vital for catching complex threats that are capable of evading usual signature-based defenses. Cisco XDR with SCA achieves this through:

· Machine Learning and Behavioral Modeling – SCA learns what normal network/user behavior looks like and keeps track of traffic to spot deviations from the norm. These deviations reveal threats like data theft, unauthorized internal movement, remote control communications, and other anomalies.

· Network Virtual Module (NVM) – Deployed across the network and on the endpoints, NVM gives deep visibility into network traffic while also monitoring and analyzing flows within and between segments. This helps Cisco XDR detect and stop threats such as unusual data transfers, unauthorized access, or abnormal communication patterns among devices. NVM allows for fine-grained network segmentation, which helps in quickly containing threats. Cisco XDR can automatically respond based on NVM's data, with actions such as isolating affected devices or blocking malicious traffic to reduce the attack's scope and impact.

· Complete Visibility – XDR with SCA enables visibility across on-premises, cloud, and hybrid environments. It supports Network Virtual Module (NVM) on every endpoint along with Cisco Secure Endpoint and many other leading endpoint protection solutions to keep users safe no matter if they work at the office or remote.

· Using Updated Threat Intelligence – SCA connects with Cisco Talos threat intelligence and uses behavioral analysis and current threat intel to find known, new, and unknown threats based on their behavior.

· Automated Alerts and Response – Response teams are automatically alerted when threats are found. Alerts work with ITSM tools and collaboration tools like Cisco Webex, Microsoft Teams, and Slack. They provide details about the bad activity and can include AI-powered investigation reports that show the full attack chain across multiple signals in the environment.

· User and Entity Behavior Analytics (UEBA) – Cisco XDR identifies insider threats and compromised accounts by observing changes from normal user behavior. This is crucial to detect credential abuse and insider threats that might evade conventional security measures.

· Asset Visibility and Prioritization – Recognizing that not all assets have equal importance, Cisco XDR enables the determination of your most critical assets and the appropriate response for each. Leveraging asset context from sources such as NVM and third-party products like Microsoft Intune, XDR ensures comprehensive visibility of assets and tracks outdated software within your environment. Threat responses, whether manual or automated, can be tailored based on your asset classifications, featuring up to 10 levels of criticality.

When combined with the other components in the Breach Suite, Cisco XDR strengthens your defenses better than any comparable solution available today, so you stay well protected against ransomware, extortionware, and other attacks that threaten your data. When combined with FortisX managed detection and response, you can trust that the best technology and security operations teams are guarding you from the most sophisticated cyberattacks.

Cisco Secure Endpoint

Cisco Secure Endpoint is part of the Breach Suite, with two licenses per user. It operates on common user endpoints and mobile devices to offer protection and response with automation. It also connects with Cisco XDR for advanced analytics and threat detection with alerting that links to other security system findings that build the attack chain and report according to MITRE ATT&CK TTPs. Cisco Secure Endpoint easily co-exists and complements many other endpoint protection systems as well. NVM should also be installed on endpoints to enhance device visibility and control, enabling automated responses to prevent data breaches from spreading and potentially causing a ransomware/extortion event. This is available with Cisco Secure Endpoint and other leading third-party endpoint technologies supported by Cisco XDR.

Cisco Secure Endpoint meets Gartner's best practice recommendations through various advanced features including but not limited to:

· Unknown Threats Detection – Using machine learning and behavioral analysis to go beyond signature-based detection, Secure Endpoint detects and responds to ransomware attacks that are known or unknown.

· Memory randomization – Randomizing the location of key data structures and executable code in memory prevents attackers from predicting where to find and exploit vulnerabilities. This is a critical capability not available in many other EDR platforms. By utilizing polymorphism within code and within runtime or OS environments, a threat actor quickly loses their ability to predict stored memory variables and memory scanning techniques used for exploitation within memory structures (the heap or stack). This AMTD (Automated Moving Target Defense) technique is effective at thwarting the execution of common software vulnerabilities and exposures. (Gartner, Emerging Tech: Security — Emergence Cycle for Automated Moving Target Defense, 2023)

· Real-Time Response – Secure Endpoint can isolate compromised endpoints, block malicious activities, and remediate threats automatically with real-time detection and automated response, without manual intervention.

· Adaptive – Secure Endpoint uses machine learning algorithms to continuously acquire knowledge from new data and improve its ability to detect and respond to emerging threats, ensuring it stays effective against rapidly-changing ransomware techniques.

· Forensics and Threat Hunting – Secure Endpoint provides detailed forensic data and threat hunting capabilities, allowing security teams to investigate and analyze the behavior of ransomware and its effect on the device and environment. This is one of the main reasons why Fortis by Sentinel's ActiveRecovery™ incident response team chooses Secure Endpoint as their tool when they help customers recover from an incident.

· Proactive – Instead of waiting for an event to happen and then taking action, Secure Endpoint includes automated pre-execution analysis and sandboxing to help identify and block

ransomware before it can run.

· Enhanced Ransomware Defense integrated with NVM - Cisco Secure Endpoint and NVM collaborate to analyze endpoint network traffic and detect coordinated attack patterns, applying network segmentation to limit threats and prevent lateral movement while using automated policies to block malicious traffic and isolate compromised segments.

· Unified Threat Management Integrated with Cisco XDR - Combining Cisco Secure Endpoint and NVM with Cisco XDR offers comprehensive visibility and a coordinated response across endpoints, networks, and cloud environments, enabling real-time detection, automated threat response, and seamless investigation to significantly enhance security posture and expedite ransomware remediation.

Cisco Secure Endpoint meets the criteria suggested by Gartner best practices for ransomware prevention and Gartner's Automated Moving Target Threat Defense suggestions to help protect your organization from a ransomware and data theft event. Along with Cisco NVM and XDR, your organization can feel confident knowing you have the most advanced protection on endpoints and mobile devices to prevent an incident from known and unknown attacks.

FortisX Managed Detection and Response adds 24/7 security operations that respond to high priority events detected by Cisco XDR in your environment with automated and manual response, as well as escalation to Sentinel's expert network operations center (NOC). In higher impact attacks, Fortis by Sentinel's ActiveRecovery™ incident response experts extend your organization's defense capabilities with our large technical team that brings over 20,000 unique technical skills to generate a faster, higher quality and more effective response.

Identity Threat Detection and Response

It has become essential for organizations to evolve their identity strategies beyond just multi-factor authentication (MFA) towards a continuous adaptive trust model to outpace adversaries and enhance user experiences. Gartner forecasts that by next year, organizations adopting a continuous adaptive trust approach will reduce account takeover (ATO) and other identity risks by 30% and improve the authentication user experience by lowering prompts twentyfold. (Gartner, Shift Focus From MFA to Continuous Adaptive Trust, 2023)

Cisco's Identity Intelligence, from their acquisition of Oort, greatly improves its Extended Detection and Response (XDR) platform through the incorporation of sophisticated Identity Detection and Response (ITDR) functionalities. Identity Intelligence enables Cisco XDR, alongside Cisco Duo and Cisco Secure Access, to more effectively shield against identity-based threats by capitalizing on Oort's proficiency in identity security. The augmented ITDR capabilities will concentrate on advanced identity services like Microsoft Entra, Okta, and Duo,

offering comprehensive security solutions for organizations using these systems. Identity Intelligence is available today in Cisco Duo Advantage and higher; it works with Cisco XDR and Cisco Secure Access for a complete identity detection and response solution.

Furthermore, integrating Identity Intelligence enhances Cisco's newest zero trust access platform, Cisco Secure Access. By merging ITDR with zero trust concepts, Cisco aims to deliver thorough security solutions that tackle contemporary threats targeting identities and access controls. Industry specialists stress that ITDR is becoming essential for effective security protection, detection, and response strategies. Analyst firms, including Gartner and Forrester, have emphasized the need for strong identity security measures to combat advanced cyber threats, highlighting the significance of Cisco's increased focus on identity detection and response.

Cisco Cloud Email Threat Defense

Most organizations have switched to cloud-based email solutions, especially those using Microsoft 365 with services such as Teams, SharePoint, and OneDrive. These SaaS applications include basic built-in security tools that are often poorly set up to prevent data loss, encryption, and business email compromise (BEC). Threat actors use generative AI to quickly profile people on the internet and social media, then create very convincing targeted emails that increase phishing and successful attempts at business email compromise. At the same time, end user awareness training, which is a vital part of a comprehensive ransomware/extortionware defense, is not delivering the expected results of educating end users so that they do not accidentally give up their credentials and compromise multifactor authentication allowing threat actors to access your organizations IT systems.

According to The FBI's Internet Crime Complaint Center (IC3) report, in 2023 IC3 received a record number of complaints from the American public: 880,418 complaints were registered, with potential losses exceeding $12.5 billion. This is a nearly 10% increase in complaints received, and it represents a 22% increase in losses suffered, compared to 2022 (FBI IC3, 2024). The financial damage caused by these attacks shows their growing threat and demonstrates that traditional email defense systems or basic included cloud email protection systems are insufficient to protect your organization from cybercrime.

Gartner reports that today’s primary sources of infiltration are phishing, remote attacks on public-facing infrastructure, and unauthorized remote desktop connections (Gartner, How to Prepare for Ransomware Attacks, 2024). Cisco’s Cloud Email Threat Defense, which is part of Cisco’s Breach Suite or can be purchased separately, uses AI to provide an extra layer of defense against advanced email compromise attempts that could harm your organization's users and

data assets. By using Cisco's email security to protect your organization, you gain the following abilities to help avoid a ransomware/extortionware incident:

· AI-Based Recognition - Advanced machine learning algorithms examine email content, context, and metadata. This enables it to spot complex phishing and Business Email Compromise (BEC) attempts that are created using generative AI. The system constantly learns from new threats, adjusting its recognition capabilities to match evolving attack patterns.

· Multiple-Protection Mechanism - Powerful spam and phishing filters scan incoming emails for known malicious signatures and suspicious behaviors. By combining signature-based recognition with heuristic analysis, it can find and block AI-generated phishing emails that might evade traditional security measures.

· Behavior Analysis - The platform uses behavioral analysis to track user interactions and email communication patterns. This helps in finding anomalies that may suggest a breached email account or a spear-phishing attack. Behavioral-based recognition is a crucial component to Gartner's best practice recommendations.

· Domain-Based Message Authentication, Reporting and Conformance (DMARC) – Essential support for DMARC, along with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), checks the validity of email senders. This authentication process lowers the risk of email spoofing, a common technique in BEC attacks. Enabling these protection capabilities further conforms with Gartner's recommended best practices to protect against business email compromise (Gartner, How to Protect Organizations Against Business Email Compromise Phishing, 2023).

· Talos Powered Threat Intelligence – As one of the biggest threat intelligence groups, Talos gives real-time updates on new threats, making sure the security system is always up to date. Constant threat intelligence feeds let the platform quickly adjust to new AI-driven attacks.

· Automated Threat Response and Remediation – When a threat is detected, Cisco's solution can automatically isolate risky emails, stop bad URLs and attachments, and remove dangerous content from users' inboxes. This automated response limits opportunities for attackers, lowering the risk of successful breaches.

· Optional User Training and Awareness – Tools and resources can help organizations teach employees about security awareness on a regular basis. Training users on the latest phishing and BEC methods improves their ability to spot and report suspicious activities. User training is also available as a managed service offering by Fortis by Sentinel Cyber Advisory experts, improving the impact of your security awareness efforts.

· Reporting and Analytics – The platform has detailed reporting and analytics features, letting security teams get insights into the type and frequency of email threats. This visibility helps in improving security policies and overall defenses.

Cisco's Breach Suite, when fully integrated with Cisco XDR, strengthens its ability to deliver unified threat visibility and response. Cisco XDR offers comprehensive threat visibility and coordinates response across endpoints, networks, and cloud environments. This integration improves detection through advanced behavioral analysis and machine learning, enables real-time automated incident response, and enhances forensic investigations by combining detailed threat intelligence. Organizations can then benefit from a robust, adaptive security posture that efficiently utilizes resources to protect against sophisticated cyber threats, including AI-powered email compromise attacks. The continuous feedback loop of these security tools working together to enrich Cisco XDR's AI-powered constant threat hunting helps identify previously undetectable threat(s) within your organization. Fortis by Sentinel's FortisX MDR teams constantly monitor your XDR deployment for high priority risks, and our security analysts respond to XDR-identified threats with further investigation and remediation. This includes optional playbook automation for the system to respond at machine speed, stopping attackers in their tracks.

Cisco Secure Network Analytics

Cisco Secure Network Analytics (SNA), formerly known as Stealthwatch Enterprise, is the final major component included in the Cisco Breach Suite. It provides advanced network detection and automated response (through Cisco ISE) that enhances your ability to prevent and mitigate ransomware and extortionware attacks. According to the SANS Institute, "Investments in NDR, SIEM, EDR, and perimeter prevention alone are not enough to stop modern-day cyber-attacks. These tools lack network context, a fundamental requirement for achieving cybersecurity. NDR bolsters every phase of a SOC's maturity and an organization's maturity model" (SANS Institute, Advanced Network Detection and Response (NDR), 2022).

Many organizations lack adequate network and cloud visibility to spot and stop a cyberattack in progress. Often, attackers steal user credentials and evade perimeter and endpoint security measures, allowing them to profit from their attack. Here are critical ways Cisco Secure Network Analytics helps to prevent attacks:

· Comprehensive Network Visibility - Delivers deep visibility into all network traffic, giving a complete view that is essential for detecting suspicious activities related to ransomware, extortionware, and data exfiltration. This level of insight helps security teams catch threats that may slip past traditional endpoint security measures.

· Behavior Anomaly Detection - Advanced behavioral analytics and machine learning integrated with Cisco's NVM is used to spot anomalies in traffic patterns on the endpoint, network, and cloud platforms. This can detect the lateral movement of ransomware and unusual data exfiltration activities associated with extortionware, which are often overlooked by other security tools.

· Early Threat Detection - By constantly monitoring network traffic and incorporating threat intelligence, Cisco Secure Network Analytics can identify ransomware activities early, enabling organizations to act proactively before the ransomware can fully execute and inflict serious damage.

· Automated Response and Mitigation - The connection with Cisco's wider security ecosystem, including Cisco ISE and XDR, allows for automated responses. When a threat is detected, the system can quarantine affected devices, block malicious traffic, and apply network segmentation to stop the ransomware from spreading.

· Improved Incident Response - SNA provides forensic data that helps in assessing the full extent and impact of an attack. This data is essential for effective incident response and remediation, allowing security teams to quickly and correctly address threats.

· Integration with Existing Security Tools - The platform integrates with other Cisco security solutions and third-party tools, improving the overall security posture through coordinated threat detection and response across various layers of the security stack.

· Powered by Threat Intelligence - SNA uses threat intelligence from Cisco Talos, ensuring that it has the latest information on emerging threats. This continuous enrichment helps the platform keep up with evolving ransomware and extortionware tactics.

AI: Your Most Powerful Analyst

Information technology devices, cloud-based solutions, and Software as a Service (SaaS) platforms are generating an increasingly large amount of event data, driven by the need for comprehensive logging for management, informational, and security purposes. These logs are invaluable for providing insights into the activities happening within a system, including any potentially dangerous actions that might indicate an attempted or successful security compromise. In the current landscape, it is impractical for human analysts to handle such vast volumes of data without support from machine learning and artificial intelligence tools. Moreover, perpetrators are employing a mix of tactics and techniques creating complex attacks that evade detection and circumvent even the most cutting-edge security systems.

Unlike many other vendors on the market, Cisco includes advanced ML/AI detection and AI assistant capabilities within their platforms. AI models are trained on extensive datasets that include known attack patterns, behaviors, and anomalies, enabling Cisco XDR to detect both known and unknown threats, including zero-day attacks and advanced persistent threats (APTs). AI-based behavioral analytics detects deviations from normal user, device, and network behaviors. By creating baselines of normal activity, Cisco XDR quickly identifies unusual or suspicious actions, such as credential misuse or lateral movement within a network, which are common signs of a breach.

The AI capabilities of Cisco XDR enhance the investigation process by automatically correlating and enriching security alerts with contextual information. The platform leverages AI to consolidate related alerts into incidents, thereby reducing alert fatigue by filtering out redundant or low-priority alerts. AI-driven playbooks facilitate automated response actions, enabling quick containment and mitigation of threats. Additionally, Cisco's integrated AI assistant analyzes incident data and, with a single command, generates detailed root cause analyses, attack chain steps, and timelines that would otherwise take human analysts hours or even days to compile. This comprehensive information is invaluable for organizations to fully understand the incident's scope, even in persistent multi-week scenarios.

FortisX

FortisX Managed Detection and Response (MDR), powered by Cisco XDR, is the most advanced SOC service available on the market. It is the first Cisco certified and audited XDR managed detection and response service in the world and the only service available also certified as an MSP with Cisco's Splunk. FortisX with Cisco's Breach Suite follows recommendations for industry expert best practices to ensure your organization stays protected from ransomware and extortionware attacks.

Fortis is more than a service. It is a partnership based on four pillars: dependable technology, skilled and qualified people, proven methods, and utmost fidelity. With FortisX your cyber security maturity will improve over time, enabling your organization to constantly assess its security environment, skills, and capabilities to resist and react to the latest cyber threats:

· Xtreme Intelligence: AI-powered threat detection and mitigation using sophisticated analytics, automation, and orchestration across all environments—email, edge, endpoint, identity, cloud, IoT, and more.

· Xtreme Vigilance: 24x7x365 SOC service with a dedicated team of security experts utilizing automation tools to monitor, analyze, investigate, and resolve threats.

· Xtreme Speed: Rapid detection and response capabilities, informed by the latest research, to counteract attackers within minutes, safeguarding against the quickest and most damaging cyberattacks.

· Xtreme Compliance: Compliance-centric SOC services, meeting the highest U.S. standards (CJIS, DoD, etc.), and offering customized sovereign SOC services for unmatched organizational protection.

· Xtreme Skills: Access to over 450+ technical resources and 17,000+ individual skills, ensuring a ready bench of experts equipped to solve nearly any technical challenge or security issue.

· Xtreme Recovery: With Fortis by Sentinel's ActiveRecovery services, be assured of rapid incident response and recovery, complemented by optional proactive Incident Response (IR) service contracts for enhanced readiness.

· Comprehensive Cyber Security Solution: Enhanced optional services including managed services, NOC, consulting, CISO services, advanced technology assessment, compliance, incident response and recovery, proactive and reactive forensics, and continuous threat exposure management.

· Fortis Security Insights SIEM (powered by Splunk): Advanced log searching, alarming, and IT system integration capabilities for comprehensive compliance, long-term log storage, search, and executive reporting.

· Secure Hybrid Environments: Tailored protection for hybrid, multi-vendor, multi-vector environments using AI-powered detection and response to combat AI-powered threats.

· Partnership and Growth: A partnership approach based on dependable technology, skilled personnel, proven methods, and commitment, aimed at enhancing cyber security maturity, innovation, and business growth.

Conclusion

As ransomware, extortionware, and business email compromise (BEC) attacks continue to occur with greater speed and effectiveness along with the advancements of generative AI, it is more essential than ever to safeguard your organization with a robust lifecycle protection strategy with a focus on prevention, detection, response, and recovery.

The combination of Cisco’s Breach Suite with FortisX Managed Detection and Response (MDR) services, supported by the award-winning 24x7x365 Fortis Security Operations Center (SOC), will

ensure you have the proper tools and expertise to keep your environment and users safe from all types of evolving threats.

Contact Sentinel if you are interested in learning more about Cisco Breach Suite with FortisX MDR and how these innovative offerings can protect your organization no matter its size or industry.

Works Cited

FBI IC3. (2024, March 18). *Federal Bureau of Investigation Internet Crime Report 2023*. Retrieved from Federal Bureau of Investigation Internet Crime Report 2023: https://www.ic3.gov/Media/Y2024/PSA240318

Gartner. (2023). *Emerging Tech: Security — Emergence Cycle for Automated Moving Target Defense*. Gartner.

Gartner. (2023). *How to Protect Organizations Against Business Email Compromise Phishing*. Gartner.

Gartner. (2023). *Shift Focus From MFA to Continuous Adaptive Trust*. Gartner.

Gartner. (2024). *How to Prepare for Ransomware Attacks*. Gartner.

Microsoft. (2022, September). *New Windows 11 security features are designed for hybrid work*. Retrieved from https://www.microsoft.com/en-us/security/blog/2022/09/20/new-windows-11-security-features-are-designed-for-hybrid-work/

Microsoft. (2023, May 31). *ITDR with Microsoft: Identity threat-level detections and automatic attack response*. Retrieved from ITDR with Microsoft: Identity threat-level detections and automatic attack response.: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/itdr-with-microsoft-identity-threat-level-detections-and/ba-p/3834631

SANS Institute. (2022, May 26). *Advanced Network Detection and Response (NDR)*. Retrieved from Advanced Network Detection and Response (NDR): https://www.sans.org/webcasts/advanced-network-detection-and-response-ndr/

SANS Institute. (2023, January 15). *Ransomware Cases Increased by 73% in 2023 showing are actions have not been enough to thwart the threat*. Retrieved from

https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/

Verizon. (2023, June 6). *2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket*. Retrieved from 2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket: https://www.verizon.com/about/news/2023-data-breach-investigations-report