CASE STUDY

MASERGY | Cybersecurity

MASERGY SOLUTIONS

- Managed Security
- Managed Detection and Response
- Cloud Workload Protection

WannaCry, HIPAA violations, phishing: three stories of security success

For most enterprises, staying on top of cyber security is a task that requires the help of managed security services partners like Masergy. Backed by integrated technologies and machine-learning enabled analytics, our managed detection and response services provide teams of analysts who work 24/7 to monitor security reports, distill alerts into a prioritized list of action items, and quickly take action to help your team respond.

But what do these services defend against, and how do they deliver real business value? Craig D'Abreo, VP of Security, outlines three customer success stories demonstrating how IT teams leverage Masergy to protect their infrastructure.

Managed detection and response service alerts to WannaCry attack

Customer: Financial services organization

Detection: Patches for each operating system were available prior to the WannaCry outbreak, and most organizations were vulnerable without the patch. Behavioral analytics detected suspicious activity on unpatched machines across the network.

Response and further investigation: Analysts acted quickly to quarantine the infected host and utilized DNS logging and additional vulnerability scans to identify what other machines could be susceptible to this attack.

"Masergy didn't have a specific security signature looking for this activity. It came up as a result of Masergy's behavioral analytics. Masergy had deployed sensors, which revealed the anomalous behavior and allowed us to determine suspicious activity. This case study is a great example of how people, process, and technologies are working together to deliver effective detection and response programs for our customers."

Craig D'Abreo
VP of Security, Masergy

CASB system flags accidental HIPAA violations

Customer: Healthcare company

Detection: Cloud access security broker (CASB) data leakage prevention alerts flagged activity as a potential HIPAA violation. Using Microsoft OneDrive (a sanctioned application for file sharing) an employee accidentally shared files and personal health information with a third party.

Response and further investigation: Masergy immediately quarantined the files and built additional custom policies and data leakage prevention alerts to detect any future activity on unstructured data. Security training programs were also amended.

"CASB solutions provide very helpful data containerization capabilities that can be used to prevent situations like these. Job functions may require employees to view certain files with sensitive information, but when it comes to copying and pasting that information into other third-party systems, technology should stop the user. With data containerization, you can do just that."

Cloud workload protection defends against phishing

Customer: High-tech company

Detection: Cloud Workload Protection recognized a new workload engaged in command and control activity and flagged it as an unusual anomaly.

Response and further investigation: Masergy shut down the rogue instance and quarantined the user account. Additional forensics determined the workload was initiated by an unauthorized user account, created after a phishing attack gained customer credentials.

"There's really no way to organically monitor security activity within cloud infrastructures. This is why our customers deploy Cloud Workload Protection in every single one of those instances within their virtual private cloud environment. Not only can you run vulnerability scans against each of the instances, but you can also set up very specific configurations for security monitoring."

Learn more about Masergy Managed Security solutions

- Managed Detection and Response Services
- Cloud Workload Protection
- Managed Cloud Access Security Broker (CASB)
- Network Visibility Tool
- Security Monitoring for Office 365
- 24x7 Expert Monitoring
- Network Behavioral Analysis
- Integrated Threat Intelligence
- Intrusion Detection and Prevention
- SIEM+
- Vulnerability Scanning
- Managed Firewall