CASE STUDY | CYBERSECURITY

Reducing cybersecurity risk through the expert use of QRadar for enterprise security information and event management (SIEM)

CLIENT INDUSTRY

Federal Government

PROBLEM

Due to the client's enormous IT infrastructure and workforce, they were experiencing cyber attacks. They wanted to reduce their cybersecurity risk.

The client has a geographically distributed workforce, and its primary operational site comprises ten interconnected buildings. It has one of the largest and most geographically diverse tele-workforce programs in the civilian portion of the federal government. Currently provides connectivity to over 20,000 permanent nodes including five sites. The client operates multiple domestic and international wide-area networks (WAN), VPNs, and other external connections.

SOLUTION

Evolver implements IBM QRadar for client's enterprise security information and event management (SIEM).

BENEFITS TO CLIENT

Fewer malicious attacks on users from foreign countries from QRadar's:

- advanced reporting practices
- monitoring system settings and rules
- data analysis

EVOLVER: EXPERTS IN QRADAR

Evolver's Operations Center Managers are experts at administration, monitoring, reporting, and analyzing QRadar events/offenses. Also, highly skilled in aggregating other system alerts into QRadar to alleviate multipoint incident handling issues.

Evolver Implements QRadar Solution

QRadar Reporting and Monitoring

1. Configure QRadar reports to run after hours to reduce impact on the network resources
2. Integrated QRadar alerts to function with monitoring system, this was an ongoing project for 3 months of tuning and identifying workflow procedures:
    - The team has successfully aggregated 98% of all security events to be managed via infrastructure monitoring system for applications and devices.
        - Previously only 68% of alerts came to the team via the monitoring system, the alerts came in many formats i.e. multiple email inboxes, request from customers, different support groups.

- Alerts are received via a single source, this improves security incident handling significantly and increases operation readiness efficiency. Email, phone, or multiple system request was an antiquated means to triage, track, and respond to security threat notifications.
- The team has aggregated 98% of all security events, this has incurred a 129% increase in security alerts. Even though there was an increase in security alerts, the Network Analyst staff shared 38% of the Cyber Analyst workload and along with our security best practices approach to handling security incidents, the staff was still able to meet the require SLA of 95%
- Monitoring system and QRadar are redundant to eliminate a single point of failure. This increased the CIO's confidence that any particular security threat was minimal to the customer infrastructure.

evolver®

www.evolverinc.com

Security Incident Analysis

- To assist our client, Evolver re-analyzed and categorized all security incidents originating from foreign countries. The security incidents that were hosted in QRadar were investigated for all possible attacks originating from foreign countries.
    - The purpose of the action was due to a false claim about client sites blocking traffic to specific foreign countries.
    - Cyber Analysts investigated the source of the addresses and the email headers to trace the traffic path which took place from a malicious proxy site from within the US, another from a foreign country, and later a valid Google proxy which was being spoofed from a translation site.

QRadar Rule Creation

- Cyber Analysts created new QRadar rules to log an offense for users executing known, potentially malicious, and/or unauthorized files on their workstations in real time.
    - The rule will trigger an alert when users attempt to execute applications specified in the rule and another rule will trigger alerts when the users attempt to launch applications that our team has blocked via the Hostbased IDS.
- Cyber Analysts created new QRadar rules to log an offense for failed logins, this was necessary to increase visibility into user and server failed logins throughout the infrastructure. Thresholds were set to reduce false positives based on anomalous network behavior.

User Authentication and Analysis

- User authentication based on their geographical location type events can be co-related with users travelling outside of the country. On the other hand, detecting such events could mean un-authorized access due to password harvesting attacks or other social engineering attacks.
- Analyzing QRadar flows for different types of user agents utilized by attackers which can result in creating customized IDP/IPS signatures in the future to prevent reconnaissance scans.
- Creating actionable alerts based on malicious behavior detected by network appliances such IDS/IPS systems.
- Examining QRadar Netflows for basic http traffic or decrypted https traffic for content viewed or submitted by end user, i.e., on several occasions cyber analysts detected users visiting password harvesting sites and noticed that they had actually submitted their company username and password to attackers on these sites.

Other Engineering/Administrative QRadar Tasks:

- Create security offense rules
- Software patches/updates
- Log analysis
- Multipoint system integration
- Incorporating to DSMs (Devices Support Modules) for new technologies such as Cylance to properly categorized events in QRadar
- Reviewing system logs for failures and/or process crashes

evolver®

www.evolverinc.com

Ready to Help You

Our work with QRadar is just one example of our innovative cybersecurity solutions. Visit www.evolverinc.com to learn more.

About Evolver

Evolver is a technology company serving the government, commercial, and legal industries for nearly two decades. Specializing in cybersecurity, cloud, infrastructure, application development, end-user support, and legal technology services, Evolver addresses client challenges in the present and transitions clients to the future through the introduction of efficient and effective IT solutions.