CYBERSECURITY

FOR A RESILIENT DIGITAL SOCIETY

IN 2022, LATIN AMERICA AND THE CARIBBEAN RESPONDED TO **360 BILLION** OF CYBER ATTACKS

+2,200 MALWARE ATTACKS PER MINUTE

GROWTH IN ATTEMPTED ATTACKS OF **25%** YoY

WHY SHOULD WE TALK ABOUT CYBERSECURITY?

**"The cybersecurity of an organization is only as strong as its weakest link"

NO ISOLATED NETWORK ANYMORE

- Internal threats
- External network connections
- Non authorized connections
- BYOD concept and laptop maintenance
- External media and USB drives

The moment a person is placed in front of a device or workstation or connected to things within the customer's network, they become vulnerable to threat vectors that can increase risk.

QUESTIONS TO CONSIDER WHEN THINKING ABOUT CYBERSECURITY

- If someone was accessing your network in this moment to damage it, would you be able to detect it?
- Are your most important systems and services safe from ransomware or other malware within the network?
- Are you able to know what your vulnerabilities are today?
- Are you able to detect abnormal behavior on your network?
- Can you frequently deploy necessary operating system updates?
- If you were to suffer an attack right now, how would you respond?

ACTIVEEYE

Gain full visibility into all security activity through a single view with our ACTIVEEYE security platform. Request a demo.

*Based on data from the FortiGuard Labs 2023 Global Threat Landscape Report

**(page 59, CCoP_for CII_Second Edition)

USE CASES

RANSOMWARE

THE "DRIVE BY" SYSTEM COMPROMISE

An officer is investigating a case and visits a website targeted by malicious actors. Content on the site has been corrupted with malware, which exploits the officer's workstation the moment he visits the website, without any warning. Access to that workstation will then be sold to a crime ring, which will in turn use it to search for data and download ransomware.

SOLUTION

ACTIVEEYE platform processes an alert for potentially malicious software detected by the endpoint security agent (EDR). Analytics determine this alert requires investigation and the ActiveEye "virtual analyst" automation collects data on the attack attributes, the system history and other known instances of this type of attack. A SOC Analyst reviews the situation and quickly issues a command from ActiveEye to remove the file from the system.

This mitigates the potential ransomware attack before it progresses to a full-blown incident.

EMAIL COMPROMISE

THE EMAIL SOCIAL ENGINEERING COMPROMISE

A fake password reset email was sent to an officer who completed the action without realizing they were being duped. The malicious actors then accessed the officer's email account and set up email policies to avoid detection. The account was then used to request sensitive information from other individuals in the police department.

SOLUTION

ACTIVEEYE platform monitors the Department's Office 365 accounts for suspicious forwarding rules. A SOC analyst reviewed the new forward rule and determined the keywords were suspicious. The SOC analyst opened a security case and recommended resetting the user credentials. The police department avoided the potential exfiltration of sensitive information.

INSIDERS

MONITORING ADMINISTRATIVE ACTIONS OF AN INSIDER

An organization was terminating an individual with high level administrative access to mission-critical systems. The organization was concerned that the individual could use their system privileges in a malicious manner..

SOLUTION

The security leader configured some queries in **ACTIVEEYE** to monitor administrative actions and filtered them by this individual's username. These queries were added to a 'Daily Email Summary'. The security leader could now review the daily email summary to easily see if there were any hits on the queries. If there were, simply clicking the query name would display a list of all the actions and details in **ACTIVEEYE**portal. The queries can be removed once the user account access is terminated.

INSECURE NETWORK CONFIG

MONITOREO DE APLICACIONES EN USO EN LA RED

ASTRO radio system operators installed a third-party location system in the CEN. It was configured to use both port 80 and 443 to communicate outbound through the firewall to the Internet. The port 80 traffic was not encrypted, which allowed attackers on the Internet to probe the device looking for vulnerabilities to exploit.

SOLUTION

The **ACTIVEEYE** network detection sensor deployed to the CEN immediately reported external communications on the insecure port. The organization's IT team was able to quickly identify that system as the location server and realized the configuration was incorrect. They closed the port 80 access on the firewall to prevent any issues.

ROGUE DEVICE COMPROMISE

DISCOVERY OF UNMANAGED EXTERNAL ACCESS

A third-party contractor installed an unmanaged VPN to access an ASTRO system they were working on to complete configuration remotely. After the maintenance, the VPN was left in place. Compromised credentials from an unrelated breach exposed login information, allowing attackers to access the ASTRO network.

SOLUTION

The **ACTIVEEYE** network detection sensor identified external traffic coming in to the ASTRO network. Investigation uncovered that the IP address of the VPN was not in the network plan. Additionally, log monitoring identified administrative access into the firewall to remove logs.

Based on these discoveries, the unmanaged VPN was identified and shut down, eliminating the attacker's external access. Firewall configuration changes were brought back into known-good configuration, and internet access to the VPN IP was blocked. Log analysis confirmed that no other changes were made before the attack was detected.

MALWARE DE DISPOSITIVO REMOVIBLE

MONITORING OF REMOVABLE MEDIA

A call handler working in a VESTA environment plugged their phone into the workstation to charge it. The phone was compromised with malware, and it transferred files onto the device. If run, the malware will grant access to a threat actor who may use it to establish ransomware or exfiltrate sensitive data.

SOLUTION

ACTIVEEYE log analysis tied together the insertion of a new removable device with a process executing from the new drive. In many cases, this can contain malware at the point of initial access.

If the malware attempts to achieve persistence via scheduled task or system service, these will also produce alerts. Attempts for malware to spread through the VESTA system, for example via SMB, and any command-and-control traffic will be identified by network detection alerts. Detection of this kind of spread allows the **ACTIVEEYE SOC** to quickly contain infections and reduce blast radius.

WHY MOTOROLA SOLUTIONS FOR YOUR CYBERSECURITY NEEDS?

Purpose-built & integrated approach to end-to-end cyber resilience

LMR, LTE, SOFTWARE & VIDEO SYSTEMS

World leaders with

90+ years

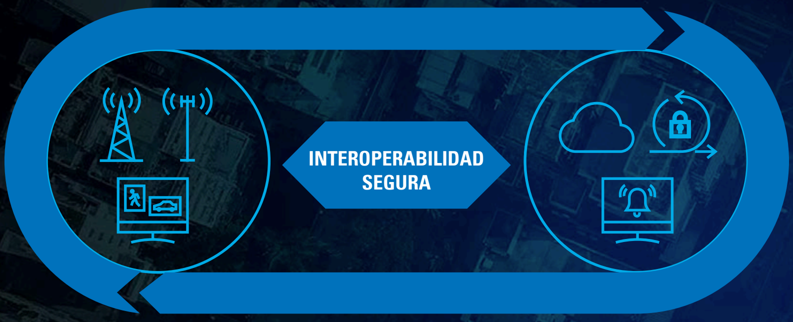
of experience in providing LTE/LMR, Video, Software, Radio technologies across 100+ countries

ENTERPRISE IT - NETWORK, CLOUD, ENDPOINTS

líderes en ciberseguridad con

20+ years

of developing advanced threat detection and response technologies for sophisticated security incidents



DIFFERENTIATORS

STRATEGIC CYBER PARTNERSHIP

- Complete solution
- Cloud based: low cost of ownership

PUBLIC SAFETY THREAT INTEL

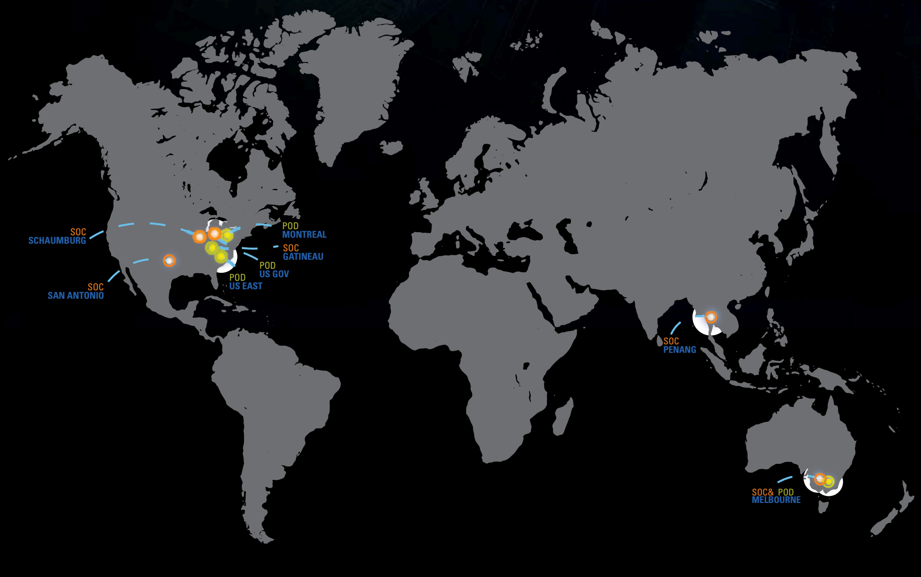
- Continuous scan of dark web
- Data from hundreds of global sites

ACTIVEEYE CYBER PLATFORM

- Analytics prioritize critical threats
- Automation drives fastest response

SECURITY OPERATION CENTERS (SOC)

Our Security Operations Centers (SOC) provide 24/7 coverage, staffed by experts with a wide range of knowledge, experienced in identifying, validating and responding to cyber attacks.



EDUCATION

- Information Science
- Cyber Security
- Information Systems Security
- MBA
- Information Assurance
- Computer Science
- Information Technology
- Technology Management

CERTIFICACIONES

- GIAC
- Sec+
- CISSP
- GCIA
- GCIH
- Linux+
- Network+
- CEH

OUR CUSTOMERS SUPPORT US

NEW ORLEANS PUBLIC SAFETY

MISSION CRITICAL SYSTEM DOWNTIME IS NOT AN OPTION

"The unknown excites me. I can have a day scheduled but at any moment, it's over, that schedule is out the window. An incident happens - I need to have backup plans. I thrive in that unknown, that thinking on your feet, making quick decisions. [After the attack, Motorola] offered their support in any way. They were here on the ground with us, getting things back up and running."

TYRELL T. (TYRELL LASHLEY) MORRIS
Executive Director
Orleans Parish Communication District

WAUKESHA COUNTY DEPENDS ON PATCH MANAGEMENT TO MINIMIZE CYBER THREATS

"The reason why we chose the SUS (Security Upgrade Service) was really to prevent against ransomware attacks. What we try to do is make it more difficult for those people that are wearing black hats to get into our system to impact the functionality."

CHRIS PETTERSON
Manager of the Waukesha County
Radio Services

READ MORE HERE

PSAP LEVERAGES MOTOROLA SOLUTIONS RISK STRATEGY AND ASSESSMENT SERVICES TO HELP MITIGATE CYBER THREATS

"Today, it's no longer adequate to merely have antivirus scanning and a firewall in your facility and think that you're suitably prepared for cyber attacks.
When it comes to network security, we should also be using policy to drive how we prepare for cyber attacks on a day to-day basis."

RAY HASIL
Director, Mason-Oceana 9-1-1

CUSTOMERS WHO ALREADY USE OUR SERVICES

- ★ Argentina
- ★ Bahamas
- ★ Brazil
- ★ Cayman Islands
- ★ Chile
- ★ Colombia
- ★ Costa Rica
- ★ Ecuador
- ★ Haiti
- ★ Jamaica
- ★ Mexico
- ★ Panama
- ★ Peru
- ★ Virgin Islands

Mexico
Bahamas
Haiti
Virgin Islands
Cayman Islands
Jamaica
Panama
Costa Rica
Colombia
Ecuador
Peru
Brazil
Argentina
Chile
● Most attacked countries

CYBERSECURITY RESOURCES

ADVISORY

RISK ASSESSMENT & TRAINING

MANAGED SECURITY

VULNERABILITY ASSESSMENT

PATCH TESTING & DEPLOYMENT

THREAT DETECTION AND RESPONSE

RECOVERY

INCIDENT RESPONSE, PLANNING AND RECOVERY

PUBLIC SAFETY APPLICATIONS | IT ENTERPRISE INFRASTRUCTURE

MOTOROLA SOLUTIONS GLOBAL PRESENCE | EXPERIENCE IN PUBLIC SAFETY AND THREAT INTELLIGENCE | CO-MANAGED SECURITY PLATFORM

OUR CYBERSECURITY APPROACH

ADVANCED AUTOMATION PLATFORM

Identify the most critical threats and automate manual tasks to provide mitigation as quickly as possible

CYBERSECURITY EXPERIENCE

Continually increase the breadth and depth of our analysts as they practice their talents daily

PUBLIC SAFETY THREAT INTELLIGENCE (PSTA)

Actively learn from real-time data investigation and analysis and threat actor objectives

STRATEGIC PARTNERSHIP APPROACH

Comprehensive set of solutions and ongoing involvement of experts in public safety issues and solutions

CYBERSECURITY TRAINING

CREANDO UNA FUERZA DE TRABAJO PREPARADA Y CONSCIENTE

CYBER ESSENTIALS

This course provides your entire workforce with end-user awareness training. It focuses on the specific threat landscape impacting public safety today and provides best practices to guard against these threats.

CYBER FUNDAMENTALS ONLINE EDITION

This course provides a high-level overview of the various aspects of cybersecurity in the context of a modern and internet-connected environment.

CYBER INCIDENT RESPONSE

This self-directed, self-paced computer based training (cbt) program shows you how to effectively prepare for, defend against and respond to cyber attacks.

RISK MANAGEMENT FRAMEWORK (RMF) FOR DOD SECURITY CONTROLS ASSESSOR (SCA)

Understand how to use various security documents and validate nist sp 800-53 rev 4 security controls to meet the requirements for the assessment and authorization phases of the it system.

COMPREHENSIVE OVERVIEW OF NIST 800-171 UPDATES

This course offers a primer on exactly what constitutes controlled unclassified information (cui), along with a detailed discussion of the 14 domains of compliance implementation and verification.

PUBLIC SAFETY THREAT ALLIANCE (PSTA)

FREE MEMBERSHIP FOR ALL GOVERNMENT INSTITUTIONS

- Secure portal to share information.
- Vulnerability and threat warnings.
- Biweekly, monthly and quarterly reports.
- Quarterly webinars.
- Monthly analyst calls.

REGISTER HERE!

KNOW MORE ABOUT OUR CYBERSECURITY SOLUTIONS HERE

For more information, visit:
motorolasolutions.com

SAFER AND TRUSTED CITIES

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**

MOTOROLA SOLUTIONS