ENIRA technologies

respond.
command.
control.

case study

ENIRA in the Government

ENIRA Technologies recognizes the unique operational and political challenges Federal Government organizations face regarding cyber-security response. Our cutting edge technology is currently deployed in several of the largest Federal Government Departments with great success. This case study is a snapshot overview of one of these deployments.

For more details on how ENIRA Technologies can enable your Federal Department to instantly respond to any cyber-security event, please visit our website at www.enira.com.

"Since we deployed ENIRA over a year ago, we have been able to quarantine all cyber security attacks before any major damage has taken place".

Systems Engineer
Federal Government Customer

The Organization

This major Federal Government customer is composed of divisions responsible for policy formulation and the overall management of a large Federal Department of the US Government.

The Challenge

Like any complex, network-centric environment, this Federal Government customer struggled against an increasingly challenging and pervasive cyber-security landscape. Once the cyber-security team identified incidents, responding was a tedious, time consuming process. A senior engineer would start off with a list of identified infected nodes, but by the time they found them and quarantined them, additional lists of newly infected nodes had already been created. "Just keeping track of the network configuration changes we were putting in place to stop an infection was a challenge" said the Systems Engineer in charge of Network Management Tools. The organization looked to the ENIRA Network Response System to decrease response time and institute a clearly defined, repeatable, and auditable response process.

The Results

ENIRA's unique technology communicates with and leverages existing network infrastructure devices (routers, switches, WAPs, etc.), so it does not require any clients or agents to be installed throughout the enterprise. It also does not have to sit inline. This architecture enables a quick and easy deployment. "Putting together the documentation for the implementation was actually more challenging than the implementation itself!" noted the person responsible for deploying ENIRA.

With the implementation of ENIRA, the Federal Government customer's response process has dramatically changed. Now, infected nodes are located and isolated from the network within seconds, before they have a chance to propagate. Since deploying ENIRA, their response is so efficient that all cyber-security incidents have been quarantined before any major damage occurred.

ENIRA also provides an Investigate feature that quickly tells the user the exact location and system details of any node, located anywhere in the network. This feature is leveraged regularly to investigate sources of suspected malicious traffic, enabling the NOC to weed out false positives before actually quarantining nodes.

ENIRA has enabled this Federal Government organization to be in command and control of the cyber-security network response process.

Available ENIRA Literature:

- ENIRA Product Overview
- ENIRA Technical Specifications
- Distributed ENIRA Datasheet
- White Paper
- FAQ
- Customer Success Story

Summary

ENIRA has enabled this Federal Government organization to be in command and control of the cyber-security network response process. By reducing the complexity of the response process, their capabilities are now based on a broader, better-enabled team. Now, Senior Engineers have the time to architect and engineer, rather than consuming their time chasing viruses and worms across the network.

This Federal Government customer is a strong example of an organization that has embraced and leveraged technology to replace manual, time consuming processes. They have even held several demonstrations for other Federal Departments to evangelize their new approach to cyber-security incident response.

About ENIRA Technologies:

Founded in 2002, ENIRA Technologies' mission is to eliminate the challenges that many Network Organizations face, from managing day-to- day operations to reacting to mission critical events in your network.

ENIRA Technologies was founded by network engineers who were driven to break through the barriers of lengthy manual and error prone processes. They invented and implemented "Expert Technology" to fully automate these processes and interactions within the network.

ENIRA has eliminated the manual and frustrating process that customers had to accept in the past. ENIRA's multi-vendor, multi-technology foundation focuses on improving the effectiveness and efficiency of enterprise network security and operations, giving its customers confidence in their ability to respond and stay in command and control.

ENIRA Technologies 11921 Freedom Drive Two Fountain Square, Suite 550 Reston, VA 20190
www.enira.com (888) 277-7638 sales@enira.com