ENIRA™ technologies

respond.
command.
control.

case study

> *“With the increased complexities of defending a mission critical network and more critical function being added everyday to increase the stakes, it is clear that tools are needed to prevent, detect, and react to problems. The ENIRA product enables BMC to round out our portfolio by adding a strong reaction tool that helps us in our overall goal of ensuring that our IP networks are safe”.*
>
> Darren Dworkin, CTO, Boston Medical Center

Organization Profile

Boston Medical Center (BMC) is a private, not for profit, academic medical center located in Boston, Massachusetts.

To support providing a full spectrum of advanced services, Boston Medical Center has deployed a robust data network. Designed with security and stability in mind, the network is made up of over 10,000 nodes and contains a range of advanced technologies including voice over IP, wireless, and network-enabled medical systems.

Challenges

Despite a large investment in network and host-based cyber-security prevention and detection technologies, BMC still had to respond to the proliferation of viruses, worms, and other cyber-security incidents. Cyber attacks occurred at all hours of the day. Network operators were expected to make rapid decisions under pressure, and to take relevant actions without endangering the availability of business systems or mission-critical traffic flows. While a manual incident response plan had been put in place, the time it took to respond was simply not fast enough. The typical approach was as follows:

1. **Determine appropriate individuals to contact**
2. **Contact a Senior Network Engineer and relay incident details**
3. **Engineer analyzes topology to determine the network devices that could potentially connect to the source of the incident**
4. **Engineer issues commands to potential network devices to identify if the infected node is connected to it. If it is, additional commands are sent to disable the node’s access. (Repeat steps 3 and 4 for each node requiring quarantine)**
5. **Notify IT and business constituents**
6. **Thoroughly document all changes made, if possible**

Rapidly locating and quarantining infected nodes was a struggle and limited to a few senior engineers. By the time an engineer could locate and disconnect the infected node, the attack had propagated exponentially. The associated cost, loss of service, and impact on patient safety from these incidents was too much to ignore.

BOSTON MEDICAL CENTER

About Boston Medical Center

The Boston Medical Center (BMC) is a private, not for profit, academic medical center located in Boston, Massachusetts. Emphasizing community-based care, Boston Medical Center’s mission is to provide consistently accessible health services to all. The largest safety net hospital in New England, Boston Medical also has the largest 24-hour Level 1 trauma center in New England and is the primary teaching affiliate for Boston University School of Medicine.

Boston Medical Center
One Boston Medical Center Place
Boston, MA 02118
http://www.bmc.org

> *"ENIRA supported all of our existing network devices. The fact that no changes to our device configurations were required, and we did not need to deploy any clients or agents on our desktops and servers, was amazing. We were fully operational in just a few hours. Overall, ENIRA was one of the easiest systems I have ever implemented".*
>
> Arsen Khousnoutdinov, senior network engineer, BMC
> responsible for deploying ENIRA. (October 2004)

Available ENIRA Literature:

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

Solution

BMC's goal for the ENIRA Network Response System was to eliminate time-consuming, manual procedures and replace them with a consistent, automated incident response strategy.

Shortly after deploying ENIRA, BMC was hit with a worm infection. This time, the BMC staff was able to use ENIRA to quickly and easily quarantine the infected workstations before the attack spread across the network—meeting and exceeding their primary goal.

With ENIRA this instant and effective response is now the norm, not the exception. Every time, BMC has now been able to quickly contain and isolate infected nodes before any major impact to their critical network. Network Manager, Robert Monks agrees, "Attacks occur despite our IPS/IDS solutions—that is a fact. The quick response capability that ENIRA provided prevented any major damage every single time."

Beyond quarantining nodes, BMC is able to leverage additional staff in the response process through ENIRA's simple web interface. In addition they rely on ENIRA's "self-documenting" feature to ensure all appropriate network configuration changes and incident details are automatically captured in a report.

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