EMC

IT leader stays safe with RSA® CyberCrime Intelligence Service

AT-A-GLANCE

Key Requirements

- Demonstrate leadership in deploying innovative IT solutions to support reputation as industry leader and set high standard for information security
- Enhance visibility of exposure to advanced cybercrime and cyber-espionage attacks
- Improve response capabilities to malicious attacks

Solution

- RSA CyberCrime Intelligence (CCI) service provides details on stolen credentials and compromised machines within the network
- Daily blacklist service highlights existing and emerging threats from malicious URLs
- RSA Live operationalizes intelligence in RSA NetWitness by aggregating information from the global intelligence community and fusing it with organizational data

Results

- Visibility of advanced threats against EMC and its employees now greatly enhanced
- Solution demonstrates organization's commitment to an intelligence-led IT strategy

CUSTOMER PROFILE

> " I trust the solution as it enables us to not just dip our toe into the intelligence needed to protect the organization, but to get knee-deep in it. Without this intelligence we'd be doing our business a disservice and we want to show our internal stakeholders just how critical it is."

JAMES R. LUGABIHL, GLOBAL CIRC SENIOR MANAGER, EMC

EMC is one of the world's leading IT companies. Operating in markets worldwide, it offers a wide range of products and services to help its customers run the most efficient, secure and high-performance data centers.

KEY REQUIREMENTS

As a big name in the IT industry, EMC takes seriously its role as a standard-setter and role model for its customers. This means it makes sure it always has the most innovative technologies in place itself.

James R. Lugabihl, Global CIRC Senior Manager at the company explains: "Our overall strategy is to move towards being a more intelligence-driven organization. We believe Intelligence is King and Context is Queen, meaning the more we know about our own environment, the more pre-emptive we can be in protecting it from threats and attacks."

The organization wanted to boost its visibility of any weaknesses in its security to ensure its own data was protected from threats such as malware and sophisticated hacking attacks. At the same time, it wanted to ensure that employees were protected from fraud and other online threats.

"Employees aren't meant to use their company computers or other resources for personal use, but they inevitably do," explains Lugabihl. "They'll use their work email address to log in to Facebook for example, or have their company credit card details listed online. We needed to ensure these details were kept safe, and the best way to do that is to protect our employees in all their online interactions when they're using one of our machines."

SOLUTION

EMC needed a catch-all way of monitoring its security posture and identifying where threat mitigation was needed. It chose to subscribe to the RSA CCI service, which provides information on corporate machines, network resources, access credentials, business data and email correspondence that may have been compromised by malware.

"The first feature of the service that we made use of was the tracking of stolen credentials," says Lugabihl. "This is a really valuable service for our internal users. We can see exactly what details have been lost, such as a Social Security or credit card number, and who they belong to. We've never had that level of visibility before and it makes our response to these incidents much faster and more targeted."

The service also enables EMC to be more proactive by intervening between a user and a malicious site to prevent exposure to a threat in the first place. It does this by providing a daily list of blacklisted URLs, split into "confirmed threats" (or sites where malicious activity is known to be underway) and "potential malicious threats" (the hosts RSA has identified as being where the cybercriminals may potentially launch their next attack).

"We have 55,000 employees and 20,000 contractors, vendors and temporary workers, all using the Internet every day – that's a lot of potential exposure to these malicious sites," Lugabihl says. "Indeed we have 50 to 60 hits on blacklisted sites every day. However, because we now know which sites are potentially dangerous, we can initiate defensive controls to stop users from accessing them and so minimize our threat exposure."

The final piece of this solution came in the form of the RSA Live Intelligence service and the RSA NetWitness network security analytics platform. The daily blacklist updates provide a live feed into RSA Live, which automatically integrates the latest information in the form of correlation rules, blacklists, parsers, views and feeds with the organization's data via RSA NetWitness.

The information delivered through the CCI credential-recovery service and the daily blacklists enables the organization to identify which of its employees are exposed to threats. The information is then shared with the departments and initiatives responsible for responding to and mitigating the threats.

> " RSA CCI service combined with RSA NetWitness has been hugely beneficial for us. And by automating the distribution of the latest threat data through NetWitness, we're able to eliminate our blind spots and keep the whole organization instantly aware of current and emerging threats. Distributing daily blacklist updates manually would have been massively time and resource-intensive."
>
> JAMES R. LUGABIHL, GLOBAL CIRC SENIOR MANAGER, EMC

RESULTS

"RSA CCI service combined with RSA NetWitness, has been hugely beneficial for us," explains Lugabihl. "And by automating the distribution of the latest threat data through RSA NetWitness, we're able to eliminate our blind spots and keep the whole organization instantly aware of current and emerging threats. Distributing daily blacklist updates manually would have been massively time- and resource-intensive."

Even one simple malware attack needs a mitigation response, so the information fed through this way is able to support numerous tactical responses that add up to a much stronger overall security posture. It also helps ensure that all remediation teams are aligned and following the same approaches.

"With RSA NetWitness we've been able to close the gaps in our visibility of advanced persistent threats and provide a more comprehensive overview of risk exposure and response," concludes Lugabihl. "I trust the solution as it enables us to not just dip our toe into the intelligence needed to protect the organization, but to get knee-deep in it. Without this intelligence we'd be doing our business a disservice and we want to show our internal stakeholders just how critical it is."

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.emc.com/rsa.