Take Your Application Security to the Next Level With Threat Intelligence

December 2015

Cyberattacks can't be simply wished away

Organizations tend to invest in several different processes, tools and technologies to protect themselves from possible threats. But it takes a great deal of time, money and expertise to fine-tune an effective response to evolving security threats and malicious attack tactics — whether using in-house IT security or technology partners.

Threat intelligence is one of the latest trends in the security landscape, yet it is largely misunderstood as the concept can be interpreted in a variety of ways. And unless an organization has a clearly defined strategy for functional threat management that works for their specific industry and processes, it remains an intangible goal.

With diverse and increasingly destructive cyberattacks occurring every day around the world, companies need an effective and optimized security environment, backed by actionable intelligence, now more than ever.

This white paper outlines the key objectives and strategies of embarking on a comprehensive threat intelligence program.

A well-defined problem is a half-solved problem.

An organization's threat center needs to do more than just detect and block security threats. It also has to monitor, gather and analyze this information for the business to gain actionable insights into the present and the future.

Understanding threat intelligence

Threat intelligence is often mistaken for the techniques used for detecting and blocking bad or unknown IPs, identifying application vulnerabilities or malware signatures, and blacklisting URLs or RSS feeds. However, this is simply source information used to create a comprehensive threat analysis. So what exactly is threat intelligence?

Threat intelligence is data that has been analyzed thoroughly — most often using human-based processes but, in certain cases, can be entirely machine driven. The data includes context, mechanisms, indicators, implications and actionable advice to create a greater understanding of a company's response to possible threats. The results must meet the following three requirements to be defined as intelligence:

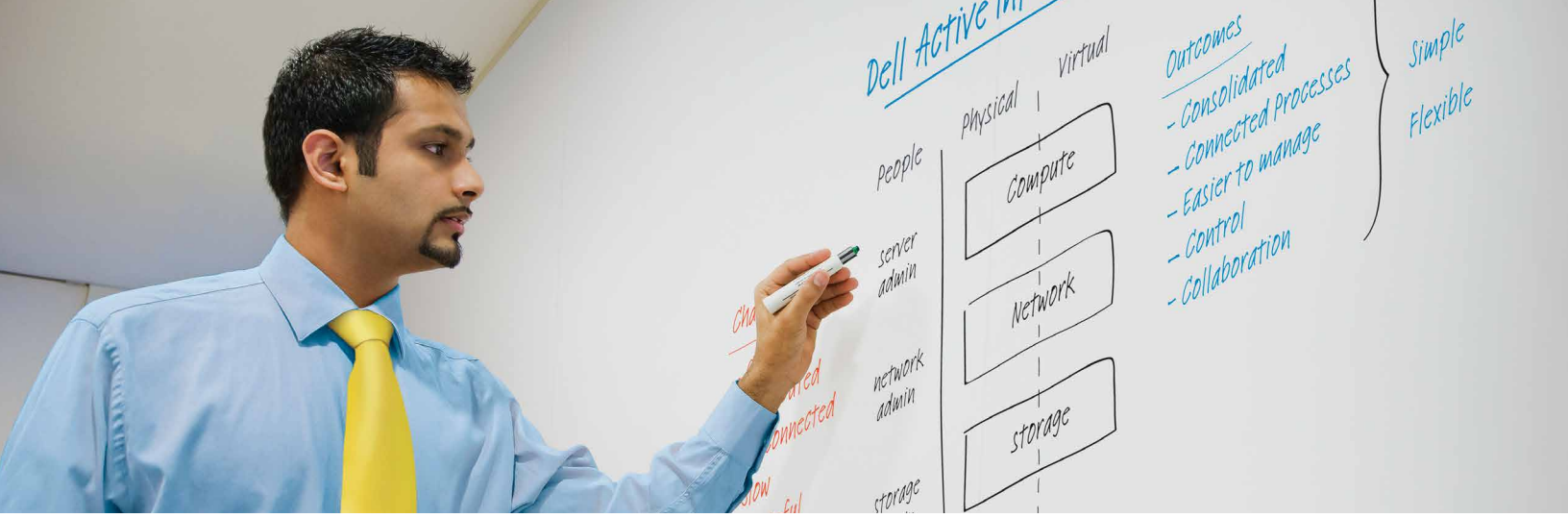
1. **Relevance:** The information must relate to the organization, its industry or its objectives. For example, data gathered on a popular Windows-based security system is completely irrelevant for an organization running a UNIX/Linux environment.
2. **Actionable:** The data must prompt a decision or action, or inform the organization not to act. If a risk assessment report shows the possibility of an advanced threat, but the risk is low, an organization can decide to either mitigate the risk or ignore it. Even the choice to ignore the attack will be an informed decision as it's based on actionable insight.
3. **Valuable:** The information must contribute to a favorable business outcome. For example, gathering redundant information related to network infrastructure and devices will not add value to line-of-business applications.

An organization's threat center needs to do more than just detect and block security threats. It also has to monitor, gather and analyze this information for the business to gain actionable insights into the present and the future.

Why business leaders should think like security experts

Security is not a modern day challenge. It has always been a priority for executives. Today, security has gotten even more complicated as organizations need to connect to systems outside their core network (that aren't in their control), as well as to a variety of devices to power the mobile workforce — from smartphones and tablets to other specialized devices.

Building a threat intelligence program that aligns security measures with other critical business objectives must be one of the top priorities for senior management. In this digital age of hyperconnectivity, every aspect of a business is affected by security threats, from the ability to grow revenue and reduce operating expenses to compliance with industry and federal regulations.



While keeping in mind market complexities and emerging technologies, enterprise leaders need to ask themselves serious questions about threat intelligence, such as:

- What is the primary reason for investing in threat intelligence capabilities? Is it to gain compliance to regulations or to reduce business risk?
- What are the main responsibilities of this threat intelligence program?
- What are the quantifiable risks and benefits of having such a solution?
- How will the security team measure the program's performance?
- How will the organization justify the initial investment?

Before embarking on the creation of a threat intelligence program, enterprises need to come up with convincing answers to these questions. The failure to do so will lead to an uneven program that may or may not provide the results organizations desire from effective threat intelligence.

The most common objectives of a threat intelligence program are to:

- Prevent and identify threats
- Increase compliance while reducing regulatory risks
- Reduce the risk of data loss or a breach
- Decrease online fraud

Where does security begin?
Security starts by setting clear organizational objectives and goals.

Patching application vulnerabilities or defending against hackers is only a small part of the overall solution. A security business objective should be broader and align with the overall business objectives by reducing external/internal threats incidents, implementing a proactive security strategy and mitigating the risks of data loss. If an organization's objective is to minimize the risk of an external data breach — since such an event could affect the organization's reputation, leading to a loss in customers and revenue —then the security threat planning should include:

- Prioritizing and managing vulnerabilities
- Classifying sensitive data or implementing data loss prevention
- Monitoring systems to track movement of sensitive data

After determining an objective, an organization needs to identify the key areas of focus for their threat intelligence program. For example, understanding hackers and their tactics, techniques and procedures is extremely important. Using real-world scenarios, the organization should explore how hackers attack an organization. How did a recent breach occur? What was the motivation, and how did the company cope? What tactics were used?

Any threat intelligence program would be incomplete without learning from previous attacks and gaining insights from industry reports. This intelligence also needs to be disseminated to the staff. Maintaining a staff that is up to date on security measures and recent threats is an easy way to increase security without having to invest in an array of expensive security solutions and tools.

Determining what works best
Today, there are several ways for an organization to turn information into intelligence — but the basic steps remain the same. An organization needs to first collect information and then group and categorize the information. They can then match the data to the applicable targets (such as applications or devices). Most importantly, organizations need to provide leaders with the resulting intelligence so they can make an informed business decision.

One of the biggest dilemmas is making the decision either to build a threat intelligence program in-house or to go for an off-the-shelf product. While both options have their own merits, most chief technology officers today would rather obtain the service from a vendor to reduce the risk of maintaining a comprehensive threat intelligence program in-house.

An industry-leading technology partner can help organizations customize a best-in-class solution to meet their unique requirements.

Making the right choice

There are countless security products and solution providers around the world. So how do you find the one that works for you?

When searching for a technology partner, organizations should evaluate based on the following criteria:

- **Quality:** This is a tricky aspect because vendors measure quality differently. Deciding what are the most important quality parameters — such as regional/industry expertise, percentage of compliance, problem resolution time or service-level agreements — will help organizations narrow down their list of prospects.
- **Uniqueness:** When there are multiple vendors who all provide good data, the decision has to be based on what a vendor can bring to the table that others can't. For example, a vendor that is able to deliver information much faster (and more cost effectively) than other vendors can easily differentiate themselves.
- **Values:** The benefits that a vendor can offer an organization — in terms of expertise, experience and resources — needs to play a key factor during selection.
- **Flexibility:** In order to meet an organization's requirements, such as transparency and vendor-neutral software selection and processes, flexibility needs to be a main factor in the selection process.

Measuring the effectiveness

Metrics and reports help determine the effectiveness of any application support program and its impact on an organization's risk. Beyond full management support, a successful threat intelligence program needs to prove operational effectiveness with comprehensive metrics and evaluations.

While a lot of programs can easily report technical data, such as the total number of searches, the number of notification triggers or the number of investigations, this information is not always vital from a security standpoint. Metrics for a threat intelligence program need to be able to directly correlate with the organization's overall objectives.

Providing metrics that make business sense to management or stakeholders is the key to success of any threat intelligence program, as an effective program can help facilitate quick decision-making and mitigate corporate risks.

Dell can help

Understanding what makes an organization a desirable target for cyberattacks goes a long way in establishing an effective protection plan. A mature security unit in an organization will cover application security, security architecture, governance, and employee development and retention.

Dell has the proven experience and in-depth knowledge of security processes to deliver services that are tailored to fit any requirements. Our security intelligence services can help you gain actionable insights to protect your critical data.

Powered by Dell intellectual property and research, our services reduce risk considerably by quickly minimizing your exposure to threats, allowing you to devote more time to remediating the risks most pertinent to your organization.

Our security intelligence services are based on an effective five-step model of planning, consultation, process, analytics and dissemination. Using these intelligence-driven phases, you'll be able to take proactive steps to defend against security attacks.

Dell has always been passionate about security and is among the very few in the industry to offer end-to-end security solutions. In fact, our application security solutions and frameworks have a built-in threat analytics engine that captures pertinent information required based an organization's current application landscape. This solution can help discover assets, identify platforms (including technology) and proactively monitor threats to assets.

Conclusion

Gone are the days when organizations used to wait for security breach alerts to respond with an effective strategy. Today, a short delay in incident response could translate to a loss in revenue, loss of trust or loss of intellectual property, none of which is acceptable.

The need of the hour is not just detection and having adequate response capabilities, but to develop a strong security strategy that takes inspiration from the latest threat intelligence and tactics.

Organizations must also realize that to move from a traditional approach to next-generation security intelligence takes considerable time and dedicated efforts. An effective threat intelligence strategy begins with setting clear business objectives as the foundation for an effective and efficient security ecosystem.

For more information about any of our services, visit our Application Security page or email Application_Services@Dell.com to contact a Dell representative.

Written by:
Rohit Baryha
Software Dev Senior Advisor, Dell

Scan or click this code to learn how Dell Services can help your organization.