

Threat Intelligence Program

By Jason Leake

Security professionals review countless vulnerabilities but have no systematic method for assessing, qualifying, prioritizing and remediating these threats.

Too many threats + Not enough relevance = So little intelligence

The equation above is becoming all too common in the field of Information Security. On a daily basis security professionals review countless vulnerabilities delivered to them by multiple disparate sources, but have no systematic method for assessing, qualifying, prioritizing and remediating these threats. This often leaves organizations with too much Fear, Uncertainty and Doubt (FUD) and not enough tangible results, usually prolonging the risk of exposure to critical threats. A solution for reducing an organization's increased exposure to threats is to implement a Threat Intelligence Program. However, introducing this program in an effective and efficient manner can be somewhat overwhelming in the beginning, as many organizations may not know where to start. There will be challenges and many organizations may find it easier to turn a blind eye and take the approach, "If it isn't broke, then don't fix it." The problem with this mode of thought is that, with the recent wave of regulatory compliance standards that organizations must meet and the increased media attention given to data security breaches, this is no longer an option.

Ultimately, the goal throughout this article is to provide security professionals a road map, which can assist in prioritizing and coordinating their efforts to reduce exposure to threats and vulnerabilities. It is highly recommended that the proper processes are developed when implementing the program so that vulnerabilities and threats that have an impact on an organization can be properly assessed, qualified, prioritized and remediated. A major benefit of a threat intelligence program is the ability to focus on the threats that are most relevant to your organization, while providing a method to achieve consistent and systematic results.

A threat intelligence program consists of the following five main components:

- **Threat Alerting Service** – Where we receive information on emerging threats and how we use it to make timely and relevant decisions
- **Internal and External Vulnerability Assessment** – What we do to determine the threats that currently exist in our environments

- **Threat Rating System** – Why certain threats are more important, based on the relevance to our organization's environments
- **Threat Prioritization Policy** – When we act on the information we are receiving in order to make the best decisions
- **Threat Remediation** – How we apply this information to keep our current and future systems up-to-date

Threat alerting service

This is usually the first place that security professionals will turn in order to determine what vulnerabilities potentially affect their organization. There are two categories of alerting services:

- **Public Alerting Service** – When an organization signs up for a public (free) alerting service, it will receive numerous, unqualified alerts for all of the affected software applications within the industry. Many organizations find the deluge of alerts from this type of service to be unmanageable and a major detriment to the efficient qualification and assessment of threats. In addition, alerts are usually sent on a time delay and contain limited details on the threat, requiring organizations to spend additional resources in researching the vulnerabilities.
- **Commercial Alerting Service** – A commercial alerting service allows an organization to create a unique technology list focused on the operating systems, applications and services deployed within the organization. The alerts issued by commercial services are current and contain in-depth technical details, allowing security professionals to effectively and efficiently assess a vulnerability. The benefits of this type of service will come at a cost, but overall, an organization's time and costs are reduced since qualification effort is minimized.

Currently, most organizations receive their alerts by email (or XML), but quite often these alerts continually pile up in an employee's inbox. While these alerts by themselves pro-

vide no real value, they allow organizations to be aware of new threats and determine subsequent steps to take.

Receiving the alerts is only the first step, and while getting this information is important, having an efficient qualification process is vital. However, many organizations do not have a quantitative way of addressing these vulnerabilities and will usually accept the ratings applied by the vendors. While vendors do a reasonable job at rating the vulnerabilities, they are unable to adequately rate them for relevance within a given organization's environment. This leads to a decentralized qualification process and when you include various teams that may receive the alerts, mitigating systems (AV, Firewalls, IDS/IPS) and other tools for determining risk, there is an additional layer of complication, which can be easily alleviated through the use of a threat rating system.

Internal and external vulnerability assessment

By current standards, most organizations have their network environments segmented into three zones: fully-trusted, semi-trusted and un-trusted. Along with each network environment comes a tolerance for risk, even though by convention risk is equal across all types of environments. However, many organizations look at the access methods, protocol flows and type of function that a system is used for, *regardless of which zone it is located in*, when assessing risk tolerance. The fully-trusted internal network is typically assigned a moderate to high level of risk tolerance, since this environment is not directly accessible from un-trusted networks. Whereas, systems located in the semi-trusted or non-trusted zones have a much lower risk tolerance assigned to them, since they are continually exposed to threats and compromise.

Vulnerability assessments should be conducted on all operating systems, applications and appliances. The reason for this is that almost all systems are inherently flawed, due to software developers' inability to identify and correct all known and unknown vulnerabilities that exist within a given product. In terms of vulnerability assessments, these are usually accomplished through the scanning of hosts through either a network or host scanning application. In today's market there are multiple applications available, either for free or at a cost, which perform thorough vulnerability assessments while providing a great overall view of the security posture for a network. Your organization should consider evaluating multiple scanning applications before choosing one to determine which features and benefits are best suited for the types of environments that you will be assessing. While in your test phase, it should be noted that vulnerability scanners are very powerful tools and if used incorrectly can cause network outages and may even break certain functionality of the systems being scanned. Once your organization has chosen a scanning application, you can then determine how granular you would like the scanning assessment to be, which relates back to the overall risk tolerance that has been applied to your environments.

When the vulnerability assessments are complete, a report containing all vulnerabilities will be generated. These reports can be quite lengthy, so a suggestion for organizations that are just starting out is to narrow the scope of the scan to report on higher rated vulnerabilities which allows for immediate prioritization. Once the assessments have identified vulnerabilities which have a high severity rating, you can use the threat rating system, described below, to validate that these vulnerabilities are truly relevant to your environment. This can lead to further prioritizing these vulnerabilities to ensure the highest risks to your organization are remediated immediately.

Threat rating system

Once received, what do security professionals do with new threat alerts and results that have been discovered through the vulnerability assessments? Better yet, how can the vulnerabilities be assessed (rated) and prioritized in a consistent and objective manner? A threat rating system is the solution that provides the ability to accomplish this.

The process of using a threat rating system is normally the most misunderstood component of the threat intelligence program. It is usually the one section where major gaps exist and consistency is lacking within organizations; but is the most important component that connects the threat intelligence program together.

This can be seen when scan data is correlated with the information in new or updated alerts, which in turn helps determine increased levels of risk due to new viruses or exploits being created, additional technical details becoming available, or an attack scenario being issued. These and many other factors can be accounted for in the threat rating system, but if organizations attempt to rate vulnerabilities without the use of a rating system, it usually becomes a major task to maintain accuracy of ratings since there is no repeatable or consistent process, which usually leads to no one wanting to take on this responsibility.

Properly rating vulnerabilities, for the relevance of your internal structure, can make a noticeable difference in when, where and how you react to vulnerabilities. Two methods that an organization can use to accomplish the assessment of vulnerabilities in a centralized environment would be through the design and implementation of an application or by using a company that provides a threat rating system as a service. By doing so, it removes the subjectivity portion of the assessment and applies pre-determined quantitative and qualitative properties to the analysis. The appropriate vectors within the threat properties and mitigating factors can be selected to achieve an overall risk rating, which helps identify where high or critical vulnerabilities exist within your organization. This information can then be leveraged towards the remainder of the threat intelligence program in order to prioritize the time and effort spent on informing the appropriate groups and completing further research/investigations, thus leading to the remediation of the vulnerability.

Threat prioritization policy

Once we have been able to apply an overall risk rating to the alerts and vulnerabilities, we can look at the process of prioritizing these threats, determined by your tolerance to risk. Threats can pose a major risk to your environments and once you have qualified the threat with a rating, typically from low to critical, a policy should be in place which states the time lines and appropriate methods (patching, workarounds, etc.) for remediating the threat. Risk tolerance varies from company to company and environment to environment. Documenting the time lines and the methods considered acceptable to fix the problem will ensure risk is managed in a consistent and effective manner. For example, an organization's prioritization policy could be as follows:

- All *Critical* rated vulnerabilities must be remediated within seven days
- All *High* rated vulnerabilities must be remediated within thirty days
- All *Medium* and *Low* rated vulnerabilities can be consolidated and remediated within three months (or sooner)

In order to achieve a level of success with a threat prioritization policy, many other factors will need to be addressed, such as change management processes, patch management tools, departmental buy-in and acceptance of additional workload. The main goal is – once you have adopted a policy for threat prioritization – Stick with it! Of course, there will be instances where remediating a threat within the stated time line is not possible. This can occur due to no patch or workaround being available or that more time is needed to properly evaluate a threat. In these situations, an organization must remain vigilant with continual monitoring of the threat through the threat rating system and address it immediately once an updated alert, patch or workaround becomes available.

Threat prioritization can be subjective, as there is a level of detail required to determine how the security posture is arranged within your organizations environment. This will require cooperation from other departments to implement this type of policy; but, once a policy for threat prioritization is in place and executive buy-in cascades down to the rest of the organization, it should help streamline the threat intelligence program.

Threat remediation

Threat remediation is the actual application of patches and configuration changes to systems to help mitigate the risk that an organization's systems will be compromised. The idea behind implementing threat remediation, in a timely manner, is to limit an organization's exposure to threats since compromised systems can be more complicated to fix and are much more costly than if the system had been protected beforehand. As well, organizations can create good practices

by maintaining a fully patched image for a particular system in the event that a system does become compromised.

Before an organization starts its remediation efforts to the affected environments, it is important to designate an individual or team to test all changes before they are deployed. This is crucial, as any patch or configuration changes can have adverse effects to an otherwise operational system. The recommendation here is to have test systems with the applicable software and applications installed to determine if any functionality of the system becomes unstable. When it has been determined that the configuration or system patches will not cause any major side effects, you should be able to deploy these changes with a level of confidence.

The tools and processes used for remediation are dependent on each organization. Regardless of the size of your organization, it is clearly more efficient to use a patching tool that automates the remediation workflow. With the number of threats and vulnerabilities increasing on a daily basis, there are an equal amount of important system patches being released by the vendors. Because of this, automated patching is becoming a necessity and whether you do this through a hardening disc that is scripted, or you deploy an agent to push down the patches at set intervals, a decision will need to be made to help streamline the patching process.

In Conclusion

Your threat intelligence program will help assess, qualify, prioritize and remediate the constant onslaught of threats your organization faces. Through the effective implementation of each component, the program can provide direction in threat mitigation, with positive results being realized in time-savings, focused efforts and efficiency.

About the Author

Jason Leake, Security+, CCNA, Post-Graduate Network Specialist, is a Security Analyst for Emergis Inc., a provider of managed security services and the first Canadian company to be certified by PCI to provide compliance services. To contact Jason, please email him at jason.leake@emergis.com.