From knowledge to action with vulnerability intelligence
Every company in the world faces rapidly growing security threats based on their enterprise software vulnerabilities. Exploitation of those vulnerabilities by cybercriminals has resulted in some of the largest security breaches in recent history, exposing credit card information and sensitive data about billions of customers, putting businesses and their reputations at risk.

Companies are fighting back, to be sure, but traditional tools deployed against cybercriminals are proving insufficient to detect and prevent attacks. Companies need to leverage the right tools to not only detect and respond to cyber events but also to anticipate and predict vulnerabilities.

Proactively mitigating security risk and limiting an organization’s threat exposure requires staying ahead of software vulnerabilities and related exploits that threat actors use to breach networks. Vulnerability and patch management is a critical component of an enterprise’s security policies and procedures, but merely managing them is not enough. To stay ahead of threats, companies need actionable vulnerability intelligence, complete with recommended best practices for prioritizing and taking action to mitigate those vulnerabilities. In this way, cyberattacks based on vulnerability exploits can be stopped.
Getting to actionable

One can think of security vulnerabilities in a couple of ways. First, an organization may not be aware of a particular threat. A recent Ponemon Institute research study found that 62 percent of corporate security victims were unaware that their organizations were vulnerable prior to the data breach.¹

Second, companies may know of vulnerabilities, but not in a way that enables them to take focused, timely action. From the same research, 60 percent of breach victims said they were breached due to a known vulnerability where a patch was not applied.² The CISO of a large utilities company told us recently that he performs a vulnerability scanning for his entire network once a month. That’s great, but when the results come back saying the network has 6 million vulnerabilities, what are you then supposed to do? Where do you start? What’s truly actionable about that knowledge?
A more effective approach: Vulnerability intelligence

We believe a better approach is what is called “intelligence-driven security” or “vulnerability intelligence.” The “intelligent” aspect of vulnerability intelligence tools is that they can take an organization from general information (e.g., six million vulnerabilities) to increasingly granular and specific information that ultimately supports timely action. In combination with leading-edge IT service management platforms such as ServiceNow, vulnerability intelligence and up-to-date asset information and valuation can be quickly combined to provide a much more holistic view of the threat exposure of the organization.

Getting more specific, in this case, means focusing on questions such as:

- Is the vulnerability actually being exploited? Can a malicious actor use that vulnerability to do damage to the network?

- Is the threat actor part of a group that is known to target an organization’s particular industry? That would then raise the profile even higher and increase potential risk to the company.

With these capabilities, a vulnerability management team can prioritize vulnerabilities in order of severity, and take action depending on which vulnerabilities pose the most risk to the business.
Staying ahead of vulnerabilities and threats

Acquiring actionable vulnerability intelligence involves deep analysis of vendor-issued and zero-day software vulnerabilities. Analyses of zero-day vulnerabilities can be made available long before a public fix is issued by the vendor community. This allows companies an opportunity to work on defense responses even before a threat actor has developed an exploit. In most situations, staying ahead of vulnerabilities can mean staying ahead of threats, thereby reducing an organization’s risk exposure.

Accenture’s iDefense services, for example, provide access to intelligence covering vulnerabilities of more than 1,000 technology vendors, malware tools and techniques, indicators of compromise, target organizations and verticals, threat actors and their motivations, and phishing campaigns.

In addition to vulnerability intelligence, companies need to be able to tie into many other data sets—things like asset inventories, configuration management databases and other more traditional governance risk and compliance tools with more detail about the overall valuations of company assets and their risks.

Companies can also get details of the IT service management components so they can start tying into ticketing workflows and remediation workflows, and then ultimately the accounting of those to make sure that action was taken.

Questions answered by vulnerability intelligence

• What is the severity (CVSS version 2 and 3) of a vulnerability?
• What technologies does the vulnerability affect?
• What malicious files are known to exploit a vulnerability?
• What detection signatures identify an exploit?
• What domains or URLs are associated with delivering exploits for a vulnerability?
The value of an effective vulnerability management platform

A leading-edge vulnerability management platform helps organizations respond faster and more efficiently to vulnerabilities, connect security and IT teams, and provide real-time visibility. It connects workflow and automation capabilities with vulnerability scan data from leading vendors to give teams a single platform for response that can be shared between security and IT.

Accenture Security and ServiceNow Vulnerability Response, for example, offer vulnerability management and response capabilities that can help to prioritize vulnerable assets by impact, using a calculated risk score, informed by Accenture cyber threat intelligence. In this way, teams can focus on what is most critical to the business and automate workflows to quickly remediate vulnerabilities. The risk score can include multiple factors in its calculation, including the CVSS score of the vulnerability and whether the vulnerability can be easily exploited.

When critical vulnerabilities are found, vulnerability response technologies can automatically initiate an emergency response workflow that notifies stakeholders and creates a high-priority patch request for IT. Once the patch has been completed, organizations can initiate a follow-up scan with their vulnerability management system to confirm the fix. This results in a coordinated remediation strategy for vulnerabilities with the added benefit of visibility across IT, security and risk teams.

Visibility into workflow automation technologies is also provided through reports and dashboards. Dashboards for the vulnerability manager provide visibility into the organization’s risk posture and team performance to quickly identify issues. Trending and predictive analytics can forecast future performance. For the remediation specialist, a separate dashboard displays task prioritization to work on the items that are critical or provide the greatest benefit first.
Conclusion: Becoming proactive with vulnerability intelligence

Vulnerability intelligence provides actionable insights and relevant decision support to detect, analyze and mitigate threats before attacks impact the business. It helps organizations focus on adversaries and threats—understanding threat actor motives and capabilities, as well as actual threats to the business and where to allocate resources effectively. It helps prioritize threats and vulnerabilities that need to be monitored, creating intelligence-driven and automated courses of action that map to security controls and enable business continuity.

Finally, vulnerability intelligence supports organizations in anticipating, detecting and remediating. Companies can gain a current and historical perspective of threat activity, understand how attackers operate and disrupt adversarial operations to enable a proactive security posture.
Mike Betts
Global Play Lead, IRM and Cyber Defense, Accenture
michael.betts@accenture.com

Maria Hart
Sr. Practice Development Manager, Security and IRM, ServiceNow
maria.hart@servicenow.com

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 505,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at www.accenture.com

References

1 Ponemon Institute, “Costs and Consequences of Gaps in Vulnerability Response.”
2 Ibid.
3 ServiceNow, “ServiceNow Vulnerability Response”