APPLICATION NOTE

THREATQUOTIENT™

REDUCE CYBER RISK

Accelerate Security Operations by Correlating Threat Intelligence and Vulnerabilities

Most cyber criminals exploit known vulnerabilities to launch attacks. With the number of vulnerabilities discovered and announced on the rise, you can't patch every vulnerability fast enough, and that opens you up to risk. The challenge is focusing your resources on addressing the known security weaknesses in your environment that adversaries are using in their current campaigns to compromise your organization.

Even after two decades, it may seem like you're constantly hearing about a new attack method or cyber threat in the world. But the reality is that cyber criminals take the path of least resistance, reusing exploits and tools that have been effective in the past, making slight deviations to continue to evade detection, and exploiting known security weaknesses – a vulnerability that has been publicly disclosed and for which a patch is currently available.

RISK = VULNERABILITY × THREAT × CONSEQUENCE

Calculating risk is a complex process of assessing threats and various attack scenarios against your defenses and vulnerabilities to accurately define a risk score or prioritization map. Addressing every vulnerability as quickly as a patch is issued may not be feasible or cost-effective for your organization. Allocating staff to test a patch and assess and manage the operational impact on production software, not to mention waiting for review and approvals to proceed, takes time and skilled personnel, which typically are in short supply. This is why it is important to have visibility and understanding into the vulnerabilities that leave your infrastructure most exposed so you can focus your efforts where the risk is greatest.

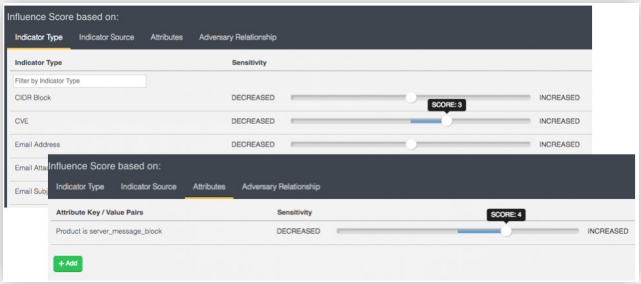
With ThreatQ's™ threat intelligence platform, organizations aggregate, contextualize and prioritize both threat and vulnerability data from internal and external sources based on the Common Vulnerabilities and Exposures (CVE) standard. This enhances ThreatQ's Threat Library™ to incorporate information on vulnerabilities to identify exploits involved in current ongoing campaigns so you can better protect against these types of attacks.

THE POWER OF UNITING THREAT INTELLIGENCE & VULNERABILITY DATA

- Correlate vulnerabilities to threat actors and tactics, techniques and procedures (TTPs)
- Assess risk with greater accuracy
- Enhance incident response to help track down susceptible hosts
- Facilitate threat hunting by mapping out common attack paths
- Improve vulnerability management processes

BRIDGING THE GAP BETWEEN VULNERABILITY AND THREAT

It's not enough to know the vulnerabilities within your organization. You must also know the threats to your organization and be able to correlate those threats to potential vulnerabilities. Looking at vulnerabilities through a filter of adversaries, indicators and files allows you to focus your limited time and resources and accelerate security operations. ThreatQ combines threat data from multiple internal and external sources to gain insight into the tools and exploits the adversaries are utilizing.

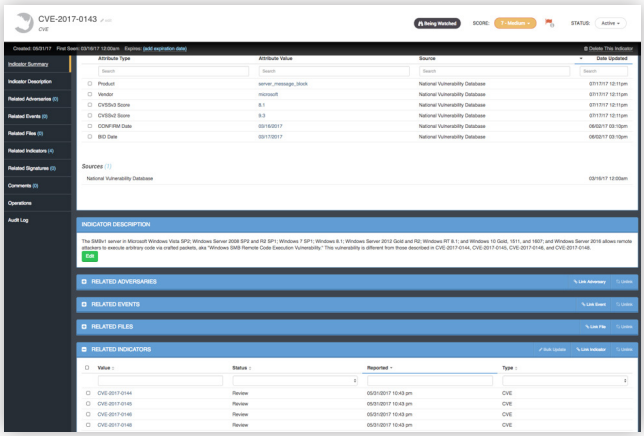


Scoring rules based on CVE details

Correlating this external data on threats, adversaries and indicators with events and associated indicators from SIEMs and log repositories inside your environment provides the context you need to understand and prioritize action. For example, with the ability to correlate a specific vulnerability to an IOC and, in turn, an IOC to an event within the SIEM, SOC and IR teams can streamline investigation and response. Meanwhile, threat analysts can tie an adversary to a vulnerability or an IOC to better detect and prevent attacks.

THREATQ AND VULNERABILITY DATA AT A GLANCE

- Investigate adversaries and the vulnerabilities they exploit
- View internal assets susceptible to a certain vulnerability
- Aggregate, analyze and prioritize the entire National Vulnerability Database (NVD)
- Investigate a vulnerability and related indicators, files and adversaries in a single view
- Correlate and pivot across indicators with related vulnerabilities
- Link vulnerabilities to alerts within your security infrastructure



CVE indicator details

THE THREATQ ADVANTAGE

By uniting threat intelligence and vulnerability data together, ThreatQ provides more data and context so your respective teams can make more informed decisions and prioritize actions to address specific security measures. You gain more from your existing team and infrastructure – threat intelligence and vulnerability management – while accelerating security operations and strengthening security posture.

ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

TQ_ThreatQ-Vulnerability-App-Note_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Sales and General Inquiries: +1 703 574-9885