Assess Yourself Against Key Verizon 2016 DBIR Findings

Defend against today's biggest IT security risks

Automate Assessment, Identify Threats, and Take Action with SecurityCenter Continuous View®

- **Comprehensive visibility** – Quick identification of the top threats and vulnerabilities identified in the Verizon DBIR that exist in your environment.
- **Actionable threat intelligence** – Pre-built Assurance Report Cards (ARCs) enable executives to quickly assess conformance with DBIR recommendations; dashboards help IT security analysts quickly detect, prioritize, and respond to key DBIR findings and recommendations.
- **Unified data** – Unique and comprehensive combination of active scanning, agent scanning, integrations with third-party systems, passive listening, and host data automates DBIR-related data collection and analysis.
- **Improved communication** – Visually display security effectiveness and policy conformance, enabling you to translate the DBIR's recommendations and guidance into an action plan IT leaders and business executives can understand.

Investment in sophisticated security solutions and experienced staff is higher than ever, but major data breaches still occur regularly – with devastating results on corporate finances and brand reputations. Why do these attacks continue to be so successful?

How confident are you in your ability to protect your organization against a major data breach?

Assessing Against DBIR Findings is Challenging

Data breaches are an unfortunate reality in IT security. Each year, the data scientists at Verizon compile the Verizon Data Breach Investigations Report (DBIR) to help organizations of all sizes learn from the experiences of others and to provide key insights into how to manage risks and avoid security failings. While the DBIR is full of practical insights, organizations still struggle to determine if they are potential victims of identified attacks and vulnerabilities. For the report to be useful, organizations must first gather the essential data from their environments and iteratively search and filter that information so it can be compared against the DBIR findings.

Tools that aggregate logged events, monitor for suspicious user behavior, and analyze huge amounts of data to detect anomalous patterns or events all promise to help address this challenge. However, they often present an incomplete view of your network or require specialized knowledge in areas like packet analysis, malware, and threat intelligence.

Common Attacks Succeed Year After Year

As in previous years, the Verizon 2016 DBIR notes that the vast majority of all attacks continue to fall into a few basic patterns. Because attackers are relying largely on common attack methods, you can use the Verizon DBIR to dramatically reduce the success of breach attempts by identifying these patterns on your network - helping you stop a breach before it occurs.

Without a comprehensive, continuous view of security across all of the platforms and devices in your environment, you don't have the visibility to identify possible issues. You also need the right set of tools to provide context, so you can connect the dots in your mountains of security data to determine which events present a real threat and which are just noise. By focusing action on the events that matter most, you have a much higher likelihood of identifying attackers before they are able to find sensitive data.

Common Vulnerability Exploitation Continues

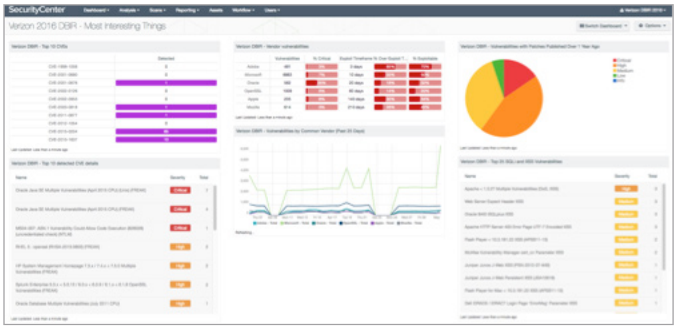
Attackers use what works, and the oldies are still the goodies because effective vulnerability mitigation remains a challenge for most organizations.

Patch management and vulnerability mitigation is still extremely reactive. Security teams lose time waiting on monthly vulnerability scan results before taking action. Even more time is wasted by playing the IT security equivalent of "whack-a-mole," rushing to try to determine the potential risk the latest threat poses, at the expense of implementing a sound, methodical vulnerability management strategy that focuses on consistency and coverage.

At the end of the day, most attackers succeed because vulnerabilities that can lead to breaches persist far too long. This year's Verizon DBIR continues to show that most organizations don't have foundational vulnerability management controls in place. Implementing a repeatable, time-bound, policy-based vulnerability management process that includes automated, near real time assessments is critical, so you can understand the degree of risk DBIR findings pose to your organization and remediate issues before breaches occur.

Assess Yourself Against Key Verizon 2016 DBIR Findings

Tenable enables you to assess yourself by providing a unique combination of active scanning, agent scanning, integrations with third-party systems, passive listening, and host data, whichautomatically feed and correlate security data from across your environment into ARCs and dashboards. This helps you to quickly identify whether the top vulnerabilities and threats in the Verizon DBIR are in your environment.



Pre-built dashboards identify if specific vulnerabilities from the 2016 DBIR exist in your organization.

Take Action to Protect Yourself Against Future Threats

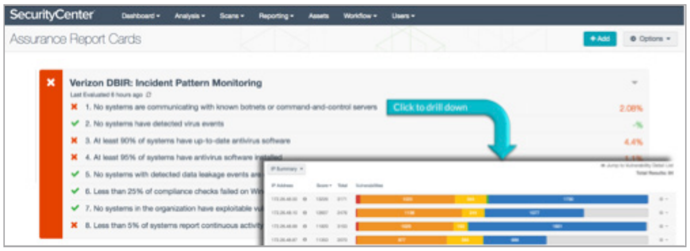
Tenable takes the vulnerability and threat information in the Verizon 2016 DBIR and makes it actionable. Pre-configured Assurance Report Cards (ARCs) and dashboards based on Verizon findings and recommendations are purpose-built to help you identify and defend against the most common attacks and vulnerabilities.

Tenable Verizon 2016 DBIR ARCS and dashboards give you the visibility and context you need to analyze how well your organization conforms to many of the recommendations and best practices highlighted in the Verizon DBIR. You can then use this information to quickly take decisive action, applying the findings in the Verizon DBIR to better protect your organization against threats.

With Tenable, you can identify if your assets are protected with the latest updates, detect unusual user and network activity, discover data exfiltration patterns, and deliver meaningful reports to stakeholders that communicate your security posture in relation to the Verizon 2016 DBIR findings, recommendations, and best practices.

Measure Security Investment Effectiveness

Use Tenable ARCs to measure the effectiveness of your IT security investments. Tenable ARCs align the findings and recommendations of the Verizon DBIR to your IT security program using a policy-based approach. Each ARC maps to a key area of the DBIR, so executives can quickly grasp the relationship between IT security team efforts, investments, and policies and Verizon DBIR findings and recommendations.



Verizon DBIR: Incident Pattern Monitoring

Last Evaluated 6 hours ago

✗ 1. No systems are communicating with known botnets or command-and-control servers 2.08%
✓ 2. No systems have detected virus events -%
✗ 3. At least 90% of systems have up-to-date antivirus software 4.4%
✗ 4. At least 95% of systems have antivirus software installed
✓ 5. No systems with detected data leakage events are
✓ 6. Less than 25% of compliance checks failed on Wi
✓ 7. No systems in the organization have exploitable vu
✗ 8. Less than 5% of systems report continuous activity

ARC policy statements show how effectively security programs are at meeting 2016 DBIR recommendations.

ARCs allow security teams to measure and communicate the status of their security program investments within the context of DBIR findings, using business terms IT security leaders and the business understand. Use the sample policies based on the 2016 DBIR findings, or customize ARC policy statements as needed based on your organizational requirements.

Incorporate 2016 DBIR Findings Into Your Security Program

Verizon 2016 DBIR ARCs and dashboards give analysts and executives the visibility needed to quickly detect, prioritize, and respond to key findings and recommendations from the Verizon DBIR - helping you shut down breaches before they happen.

About Tenable

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact