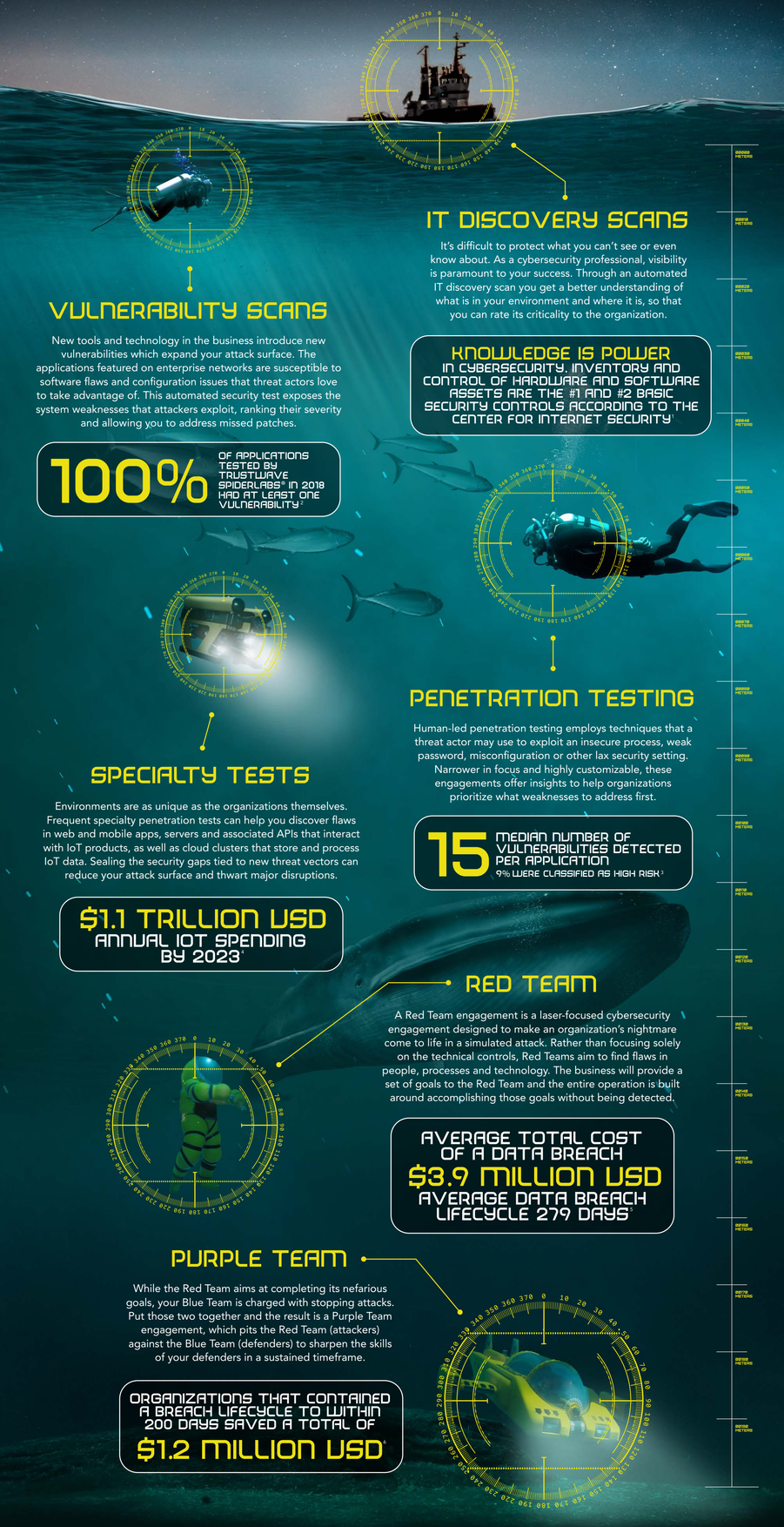
TESTING THE DEPTHS OF YOUR SECURITY



IT DISCOVERY SCANS

It's difficult to protect what you can't see or even know about. As a cybersecurity professional, visibility is paramount to your success. Through an automated IT discovery scan you get a better understanding of what is in your environment and where it is, so that you can rate its criticality to the organization.

KNOWLEDGE IS POWER
IN CYBERSECURITY. INVENTORY AND CONTROL OF HARDWARE AND SOFTWARE ASSETS ARE THE #1 AND #2 BASIC SECURITY CONTROLS ACCORDING TO THE CENTER FOR INTERNET SECURITY[1]

VULNERABILITY SCANS

New tools and technology in the business introduce new vulnerabilities which expand your attack surface. The applications featured on enterprise networks are susceptible to software flaws and configuration issues that threat actors love to take advantage of. This automated security test exposes the system weaknesses that attackers exploit, ranking their severity and allowing you to address missed patches.

100% OF APPLICATIONS TESTED BY TRUSTWAVE SPIDERLABS® IN 2018 HAD AT LEAST ONE VULNERABILITY[2]

PENETRATION TESTING

Human-led penetration testing employs techniques that a threat actor may use to exploit an insecure process, weak password, misconfiguration or other lax security setting. Narrower in focus and highly customizable, these engagements offer insights to help organizations prioritize what weaknesses to address first.

15 MEDIAN NUMBER OF VULNERABILITIES DETECTED PER APPLICATION
9% WERE CLASSIFIED AS HIGH RISK[3]

SPECIALTY TESTS

Environments are as unique as the organizations themselves. Frequent specialty penetration tests can help you discover flaws in web and mobile apps, servers and associated APIs that interact with IoT products, as well as cloud clusters that store and process IoT data. Sealing the security gaps tied to new threat vectors can reduce your attack surface and thwart major disruptions.

$1.1 TRILLION USD
ANNUAL IOT SPENDING BY 2023[4]

RED TEAM

A Red Team engagement is a laser-focused cybersecurity engagement designed to make an organization's nightmare come to life in a simulated attack. Rather than focusing solely on the technical controls, Red Teams aim to find flaws in people, processes and technology. The business will provide a set of goals to the Red Team and the entire operation is built around accomplishing those goals without being detected.

AVERAGE TOTAL COST OF A DATA BREACH
$3.9 MILLION USD
AVERAGE DATA BREACH LIFECYCLE 279 DAYS[5]

PURPLE TEAM

While the Red Team aims at completing its nefarious goals, your Blue Team is charged with stopping attacks. Put those two together and the result is a Purple Team engagement, which pits the Red Team (attackers) against the Blue Team (defenders) to sharpen the skills of your defenders in a sustained timeframe.

ORGANIZATIONS THAT CONTAINED A BREACH LIFECYCLE TO WITHIN 200 DAYS SAVED A TOTAL OF
$1.2 MILLION USD[6]

Trustwave®

TRUSTWAVE.COM

Partner URL

Partner Email

Partner Phone

SOURCES:
1. Center for Internet Security (2019) The 20 CIS Controls & Resources [Online] Available at: https://www.cisecurity.org/controls/cis-controls-list/
2, 3. Trustwave (2019) 2019 Trustwave Global Security Report [Online] Available at: https://trus.tw/l4e
4. IDC (2019) IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Million in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors [Online] Available at: https://www.idc.com/getdoc.jsp?containerId=prUS44596319
5, 6. Ponemon Institute (2019) What's New in the 2019 Cost of a Data Breach Report [Online] Available at: https://www.securityintelligence.com/posts/what-new-in-the-2019-cost-of-a-data-breach-report/