TARGET DEFENSE

MUST-KNOW CYBER STATS FOR 2023

The 2023 Target Defense State of Cyber Security Report examined data from our penetration testing, vulnerability scanning, threat management and compliance services. Here are the key findings of the report, all in one place. For context and more insight, read the full report at **www.targetdefense.com/resources/state-of-cyber-security-2023**

PENETRATION TESTING & VULNERABILITY MANAGEMENT

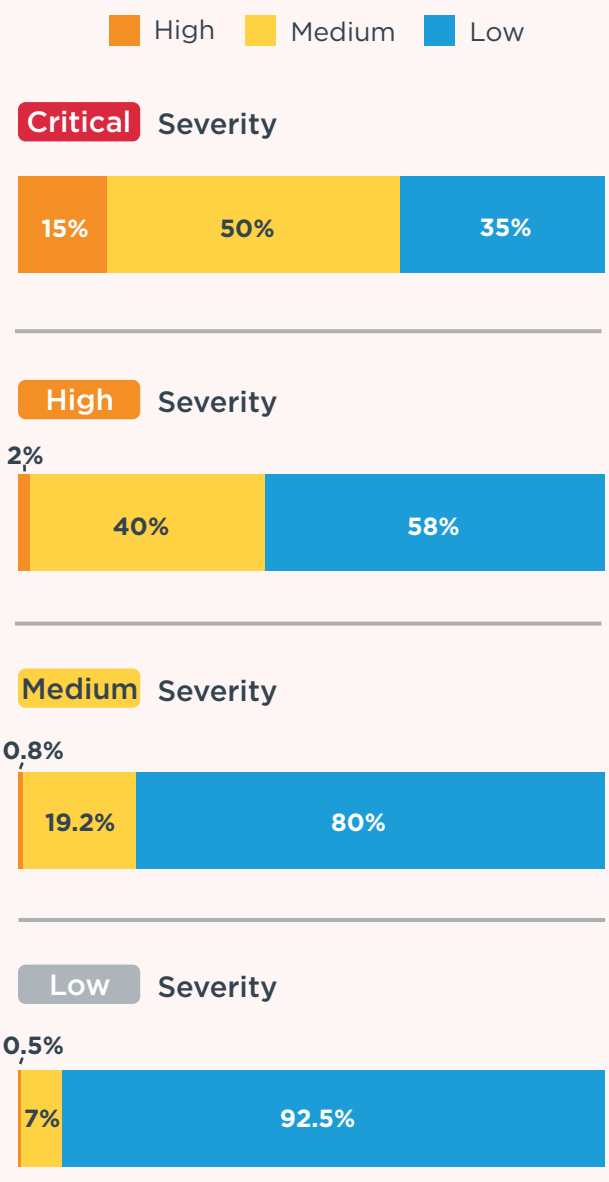
Top 5 Critical & High Threats

The most important security threats uncovered by penetration testing

1. Improper Access Controls
2. Stored/Reflected Cross-Site Scripting (XSS)
3. Unencrypted Protocols in Use
4. Outdated Components
5. SQL Injection

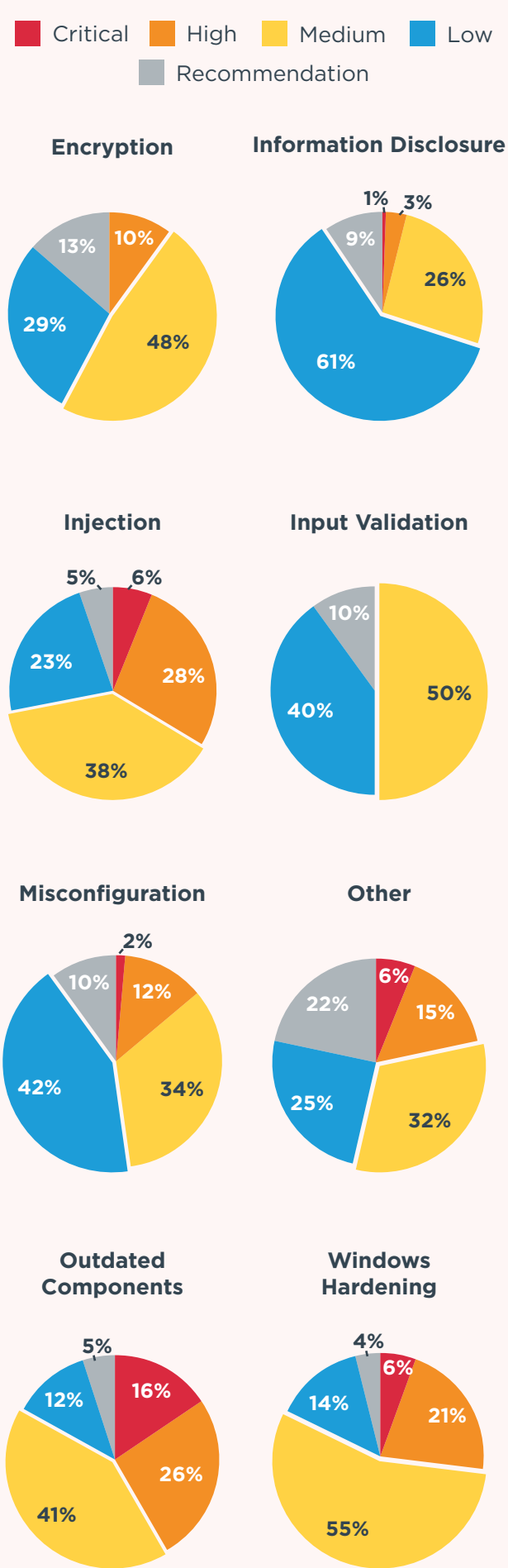
Vulnerability Severity by Effort to Fix

Showing the effort to fix for each severity of vulnerability



Vulnerability Severity by Category

The percentage of severities for each category of vulnerability



Engaging with Phishing Emails

Breaking down how people engaged with a phishing email

SIEM & HONEYPOT FINDINGS

Threat Intelligence

Examining the attack sources and cross-referencing with commercial threat intel

Over 180,000

IP addresses scanned our honeypots

Only 5%

were in commercial threat intelligence feeds

Top 3 Blocked Attacks

The most frequently blocked attacks by our SOC

1. Bruteforce RDP attacks
2. Pentesting Tool
3. Password Stealers

Top 5 SIEM Alerts

Looking at the top 5 alerts from our managed SIEM service

1. Malicious Traffic at Boundary
2. Unexpected Regional Login
3. Multiple Failed Login Attempts
4. Azure Email Sending Limits Exceeded
5. Unexpected Software Installation

Top Attack Origins

Most common points or origin for attacks against our customers and honeypont networks

1. Russia
2. China
3. Brazil
4. United States
5. Bulgaria

COMPLIANCE INSIGHTS

Top Data Protection Officer (DPO) Activity

What activities our DPOs do most often when helping our customers

1. Data Subject Access Requests
2. Breach Support
3. DPIAs and Risk Assessments

Top Cyber Essentials Failures

Top reasons businesses fail Cyber Essentials certification

1. Policies & Procedures
2. Updating Systems
3. Password Management

Top 3 GDPR Failures

Most common problems to achieving GDPR compliance

1. Understanding Consent
2. Recordkeeping
3. Lack of maintenance

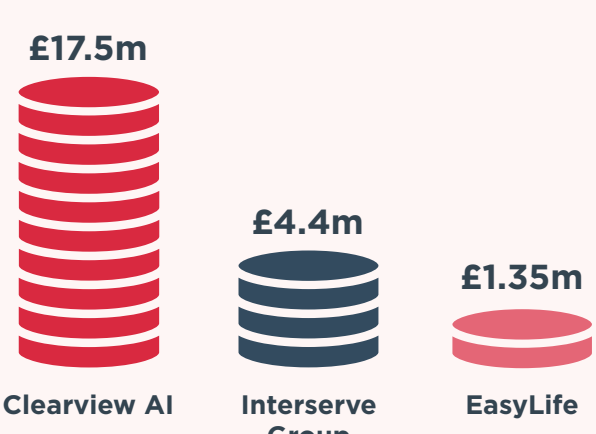
Top ISO 27001 Failures

Biggest stumbling blocks to ISO 27001 implementation

1. No Management System
2. Lack of Support Resource
3. Seen as an IT-only project

Notable GDPR Fines

Find out more about these fines by reading the 2023 State of Cyber Security report



TARGET DEFENSE

FIND OUT MORE IN THE FULL 2023 REPORT

For context and more essential insights into cybersecurity & compliance, download the full report at www.targetdefense.com/resources/state-of-cyber-security-2023

www.targetdefense.com (+1) 888-659-6655 contact@targetdefense.com