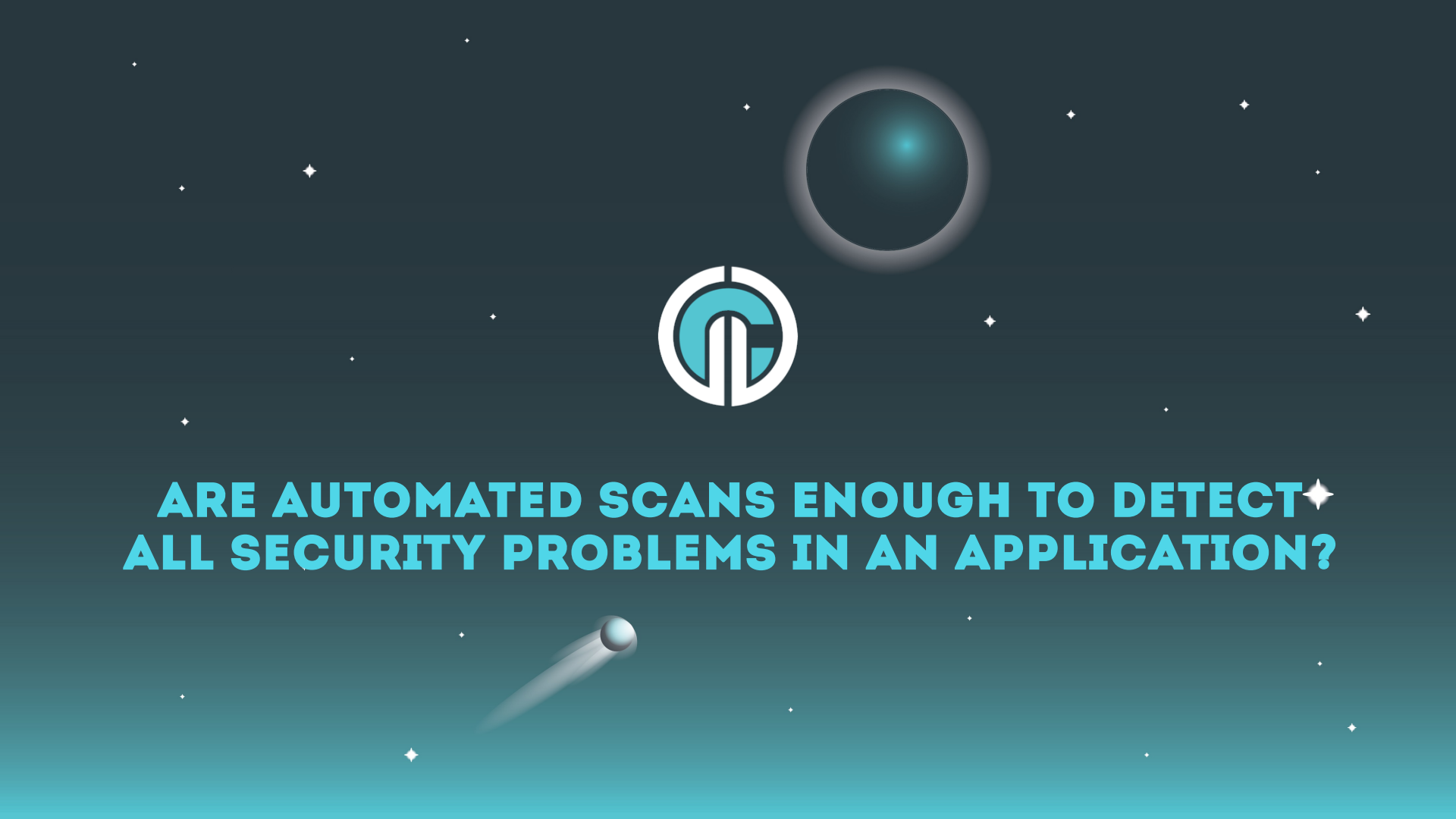

ARE AUTOMATED SCANS ENOUGH TO DETECT ALL SECURITY PROBLEMS IN AN APPLICATION?

Different Types of Scanners

- There are two main types of automated scanners
  - Static Analysis Scanning Testing (SAST) scanners
  - Dynamic Analysis Scanning Testing (DAST) scanners
- One sub-category that we're going to talk about
  - Payment Card Industry (PCI) scanners
    - PCI scanners are generally DAST, but many SAST scanners have a PCI setting

In short, no. Automated scanners alone cannot cover all aspects of an application security plan.

What Are the Differences Between SAST and DAST Scanners?

- Both have different strengths and weaknesses
- SAST scanners
  - ❖ Run against source code
  - ❖ Good at finding certain types of vulnerabilities, such as hard-coded passwords or unencoded inputs
- DAST Scanners
  - ❖ Run against a running application
  - ❖ Can check for issues that are hard for SAST scanners to find
  - ❖ Can check web server configuration
- Both integrate well with the Secure Software Development Lifecycle (SDLC)

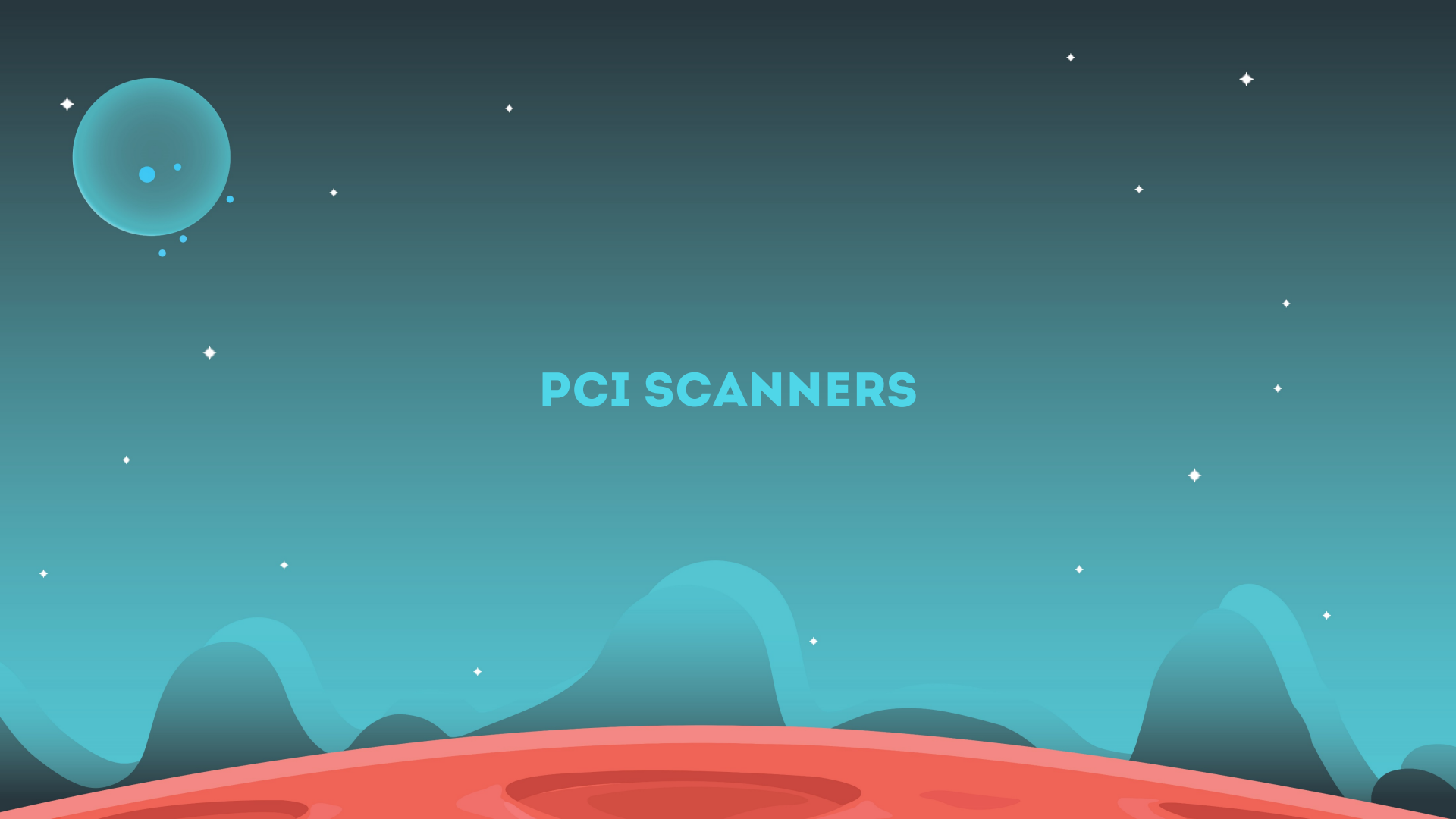
Your security team can spend time on more difficult issues

Why Are Automated Scanners Not Enough?

Automated scanners fall short in several areas

- Scanners frequently miss authentication and authorization vulnerabilities
- It's not possible for an automated scanner to assess the design of an application, nor is it possible to check a business or logic flow
- Automated scanners frequently return false positives, due to this, any findings must be validated

- **For more details on Authorization and Authentication, please check out our article featuring the differences and examples**


PCI SCANNERS

PCI Scanners – Part 1

What is a PCI Scanner

- Automated security scanner that looks for issues that prevent applications from meeting data security standards set in the PCI Data Security Standard (PCI DSS)
- Most often DAST scanners
- Currently, PCI scanners must identify OWASP Top 10 vulnerabilities

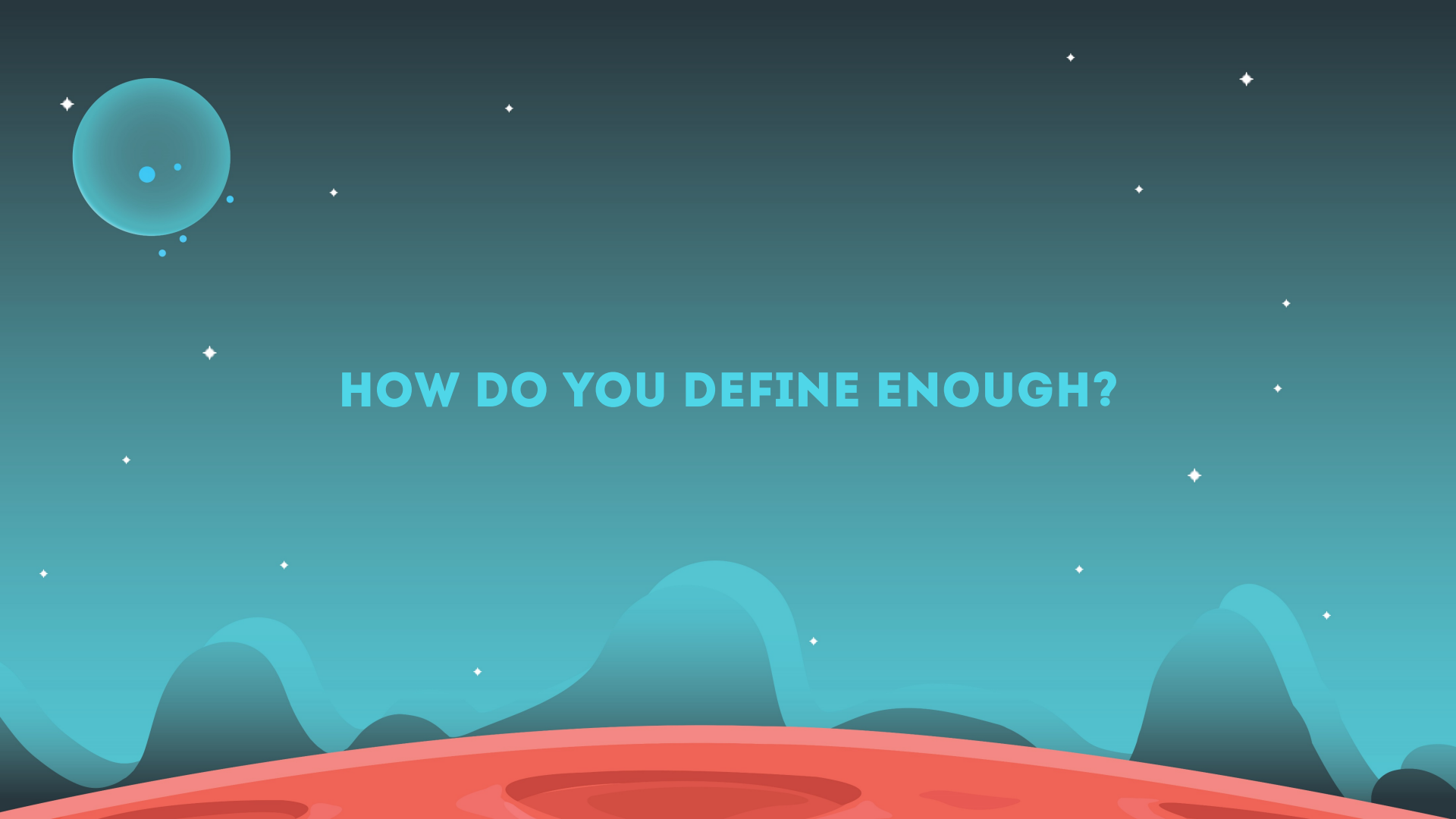
The OWASP Top 10 – 2017	
A1: Injection	A6: Security Misconfiguration
A2: Broken Authentication	A7: Cross-Site Scripting (XSS)
A3: Sensitive Data Exposure	A8: Insecure Deserialization
A4: XML External Entities (XEE)	A9: Using Components with Known Vulnerabilities
A5: Broken Access Control	A10: Insufficient Logging & Monitoring

PCI Scanners – Part 2

Is Using a PCI Scanner Enough?

- Just like other automated scanners, no
- PCI scanners have an explicit focus on checking PCI compliance, not general security
- PCI compliance does not mean that an application is secure
- Even if a PCI scanner comes back clean, it does not mean that the application is free of vulnerabilities

This also applies on the network side. A clean PCI scan against a network does not *necessarily* mean that the network is secure.


HOW DO YOU DEFINE ENOUGH?

How Do You Define Enough?

- Automated scanners are an effective way to reduce security risk
- However, they lack certain qualities that a human tester possesses
- The best approach combines automated scanners and manual testing
- This works even better in the context of the Secure SDLC

Ultimately, it's up to the individual or organization to determine how many resources they want to devote to security, and what level of risk they are willing to accept.

About Cypress Data Defense:

Our goal is to help organizations secure their IT development and operations using a pragmatic, risk-based approach. The diverse background of our founders allows us to apply security controls to governance, networks, and applications across the enterprise.

Contact us to learn more!

https://www.cypressdatadefense.com/contact/

Email: info@cypressdatadefense.com

Phone Number: 720.588.8133

REFERENCES:

"OWASP Top 10 - 2017" https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf