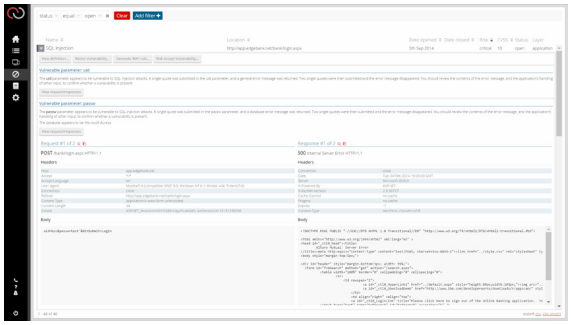
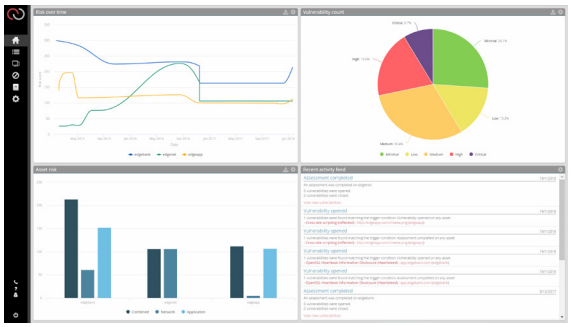
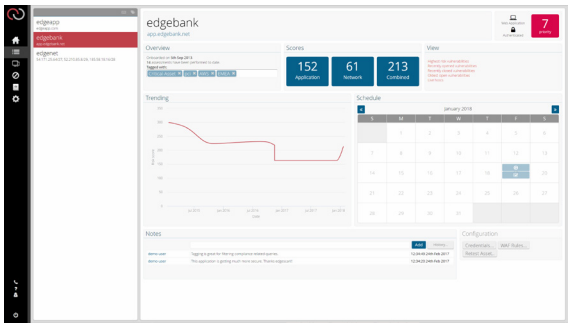
edgescan™

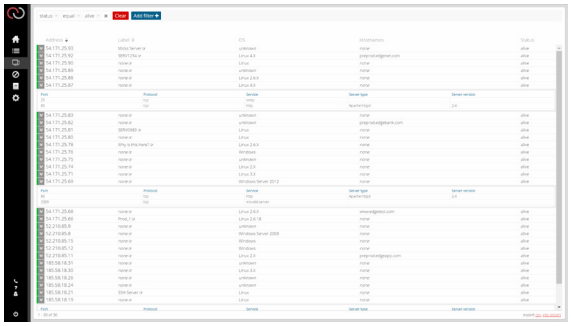
2018
VULNERABILITY STATISTICS REPORT

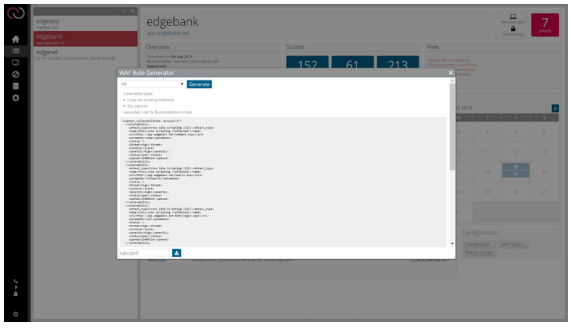
edgescan™ Portal











ABOUT EDGESCAN™

SaaS: edgescan™ is a 'Security-as-a-Service (SaaS)' vulnerability management service which detects vulnerabilities in both web application and hosting infrastructure alike.

Hybrid Scalable Assessments: edgescan™ detects both known (CVE) vulnerabilities and also web application vulnerabilities unique to the application being assessed due to our hybrid approach.

Analytics & Depth: Coupling leading edge risk analytics, production-safe automation and human intelligence, edgescan™ provides deep authenticated and unauthenticated vulnerability assessment across all layers of a systems technical stack. Historical data to measure your risk profile over time. Effortless visibility into your fullstack security posture at-a-glance – Vulnerability Intelligence.

Coverage: edgescan™ provides "fullstack vulnerability management" covering both hosting environments, component & frameworks and developer-written code. Our edgescan advanced™ license even covers business logic and advanced manual testing techniques.

Support: Dedicated expert support from seasoned penetration testers and developers, to provide advice and remediation guidance.

Accuracy/Human Intelligance: All vulnerabilities discovered by edgescan™ are verified by our engineering team to help ensure they are a real risk and prioritised appropriately for our clients. Our analysts eliminate false positives and streamline the remediation process, saving valuable developer time and resources.

Rich API Integration: Our API makes it simple to plug edgescan™ into your ecosystem in order to correlate and reconcile, providing integration with both GRC and Bug Tracking and DevSecOps Systems alike.

One-click WAF: Rule generation supporting a variety of firewalls is also supported, helping you virtually-patch discovered vulnerabilities.

Alerting: Customise Alerting via email, SMS, Webhooks, Slack, API etc, based on custom criteria.

Continuous Asset Profiling: Continuous profiling of the entire Internet-facing estate detecting changes in estate profile and eliminating blind spots.

Scale: Managing estates from one web application to thousands, from a single hosting environment to global cloud infrastructure, edgescan™ delivers continuous vulnerability intelligence, support and testing-on-demand.

Compliance: edgescan™ is a certified PCI ASV and delivers testing covering the OWASP Top 10, WASC threat classification, CWE/SANS Top 25, etc.

edgescan™ Gartner PCI Security Standards Council APPROVED SCANNING VENDOR CIO Review 20 MOST PROMISING ENTERPRISE SECURITY SOLUTION PROVIDERS - 2017 amazon web services Partner Network TECHNOLOGY PARTNER

INTRODUCTION

Vulnerabilities or bugs in software may enable cyber criminals to exploit both Internet facing and internal systems. Fraud, financial, data & identity theft, and denial-of-service attacks are often the result, leaving companies with serious losses or damage to their reputation.

However, some of these issues can be easily avoided or at least mitigated. This document discusses all of the vulnerabilities discovered by edgescan™ over the past year – during 2017.

The vulnerabilities discovered are a result of providing "Fullstack" continuous vulnerability management to a wide range of client verticals; from Small Businesses to Global Enterprises, From Telecoms & Media companies to Software Development, Gaming, Energy and Medical organisations.

The statistics are based on the continuous security assessment & management of thousands of systems distributed globally.

EXECUTIVE SUMMARY – 2017 IN REVIEW

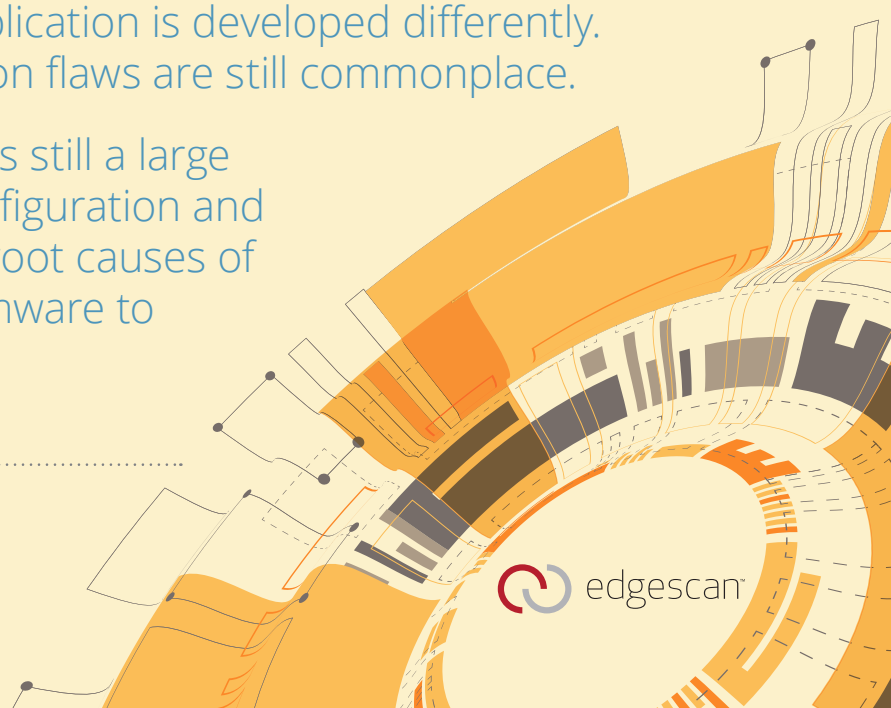
Many of the problems uncovered in 2016 and the year before are still present. In 2017 we experienced some major cybersecurity breaches many of which were a result of a technical security issue.

Both Large global organisations and governments were breached resulting in millions of client records being stolen. Common vulnerabilities are still easy to find due to insecure programming practices.

"Known vulnerabilities" (CVE's) are also pervasive with a high percentage of systems containing multiple CVE's. Old CVE's are still commonplace and could result in a breach or in non-compliance at a minimum.

The Risk density of Web Applications is still an issue due to their uniqueness – every application is developed differently. Cryptographic implementation flaws are still commonplace.

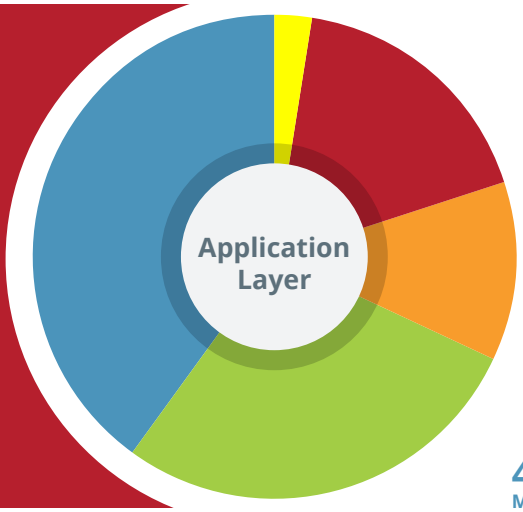
The lack of system patching is still a large source of vulnerabilities. Configuration and maintenance are significant root causes of attacks ranging from Ransomware to data disclosure attacks.



APPLICATION LAYER RISK DENSITY

20% of all vulnerabilities discovered are High or Critical Risk

Every application is unique and developed uniquely which manifests in a high risk density.



2.7% CRITICAL RISK

17.3% HIGH RISK

12% MEDIUM RISK

28% LOW RISK

40% MINIMAL RISK

TIME-2-FIX (WEB APPLICATIONS / LAYER 7)

7 Days	8 – 30 Days	31 – 90 Days	90+ Days
22%	21%	30%	25%

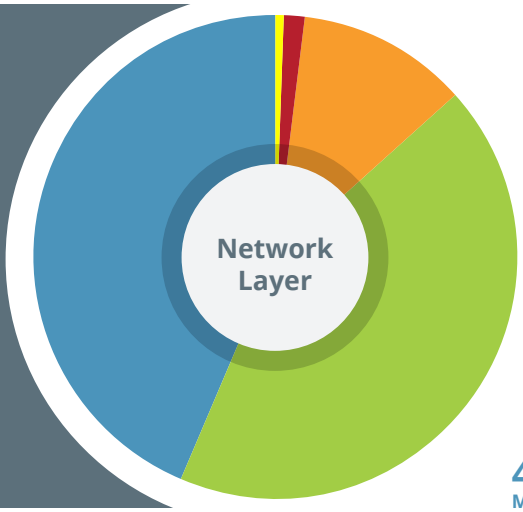
Average time to close a discovered vulnerability is **67 Days**

#ProTip: edgescan™ support helps your development staff understand and mitigate discovered issues. Retest On-Demand via the console or API can help you retest your fixes when required.

NETWORK LAYER RISK DENSITY

2% of all vulnerabilities discovered are High or Critical Risk

Hosting infrastructure and cloud is commoditised and appears to be easier to secure and maintain resulting in a lower percentage of high and critical risk density.



0.6% CRITICAL RISK

1.5% HIGH RISK

11.4% MEDIUM RISK

43.5% LOW RISK

43% MINIMAL RISK

TIME-2-FIX (NETWORK LAYER)

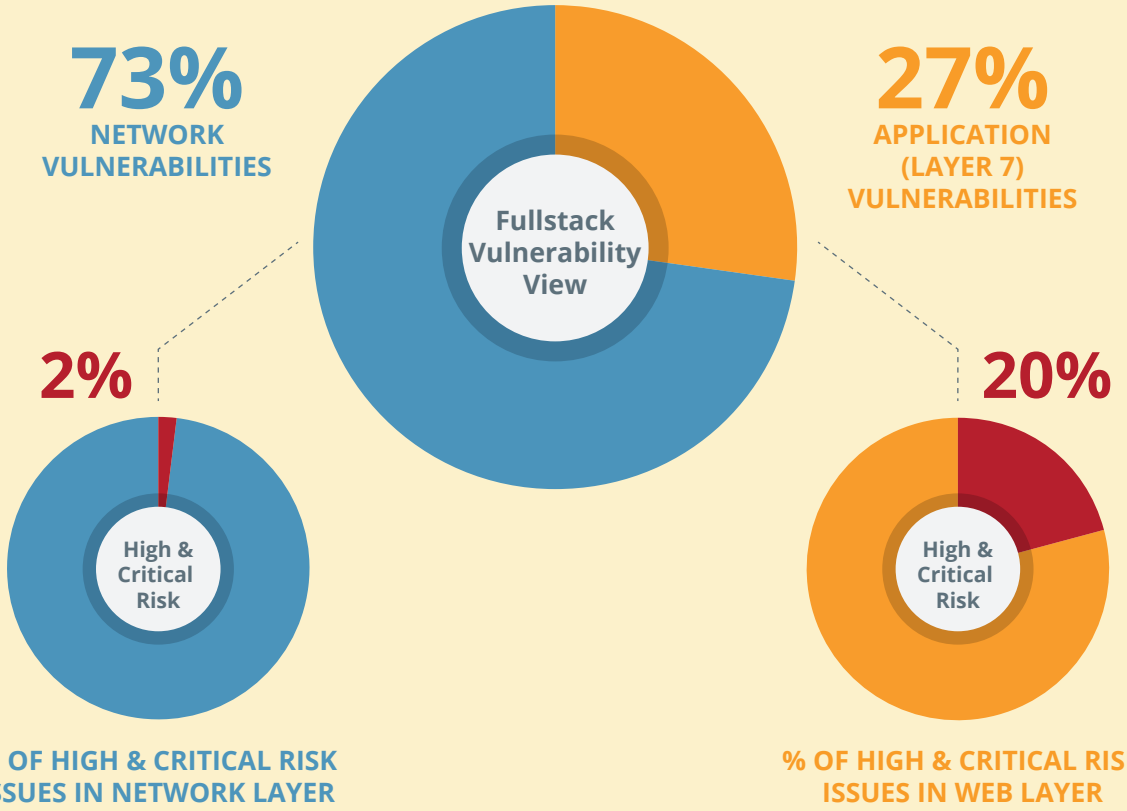
7 Days	8 – 30 Days	31 – 90 Days	90+ Days
6%	35%	37%	21%

Average time to close a discovered vulnerability is **62 Days**

#ProTip: Visibility is key to understanding your technical asset estate and the potential for a vulnerability arising. Alerting, technical support and proactive threat intelligence via edgescan can keep you informed as issues are discovered, helping you fix discovered issues quicker and more efficiently.

FULLSTACK VULNERABILITY VIEW

In 2017 we discovered that on average, 27% of all vulnerabilities were associated with web applications and 73% were network vulnerabilities.



The network has a higher vulnerability density but the web application layer is where the majority of the high and critical risk exposure resides.

This is due to each application being uniquely developed (not commoditised) and apparent difficulties in managing component version control and patching of third party libraries.

#ProTip: Consider component version control to help manage framework vulnerabilities. Open source libraries and framework components, not developed by your development team can be a source of vulnerabilities.

Secure application development practices have evolved significantly over the past 5 years. Integrating security into the development cycle (DevSecOps) and catching issues early is a recommended approach to reducing the potential of vulnerabilities in the production environment.

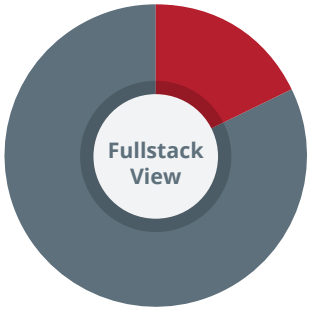
#ProTip: Consider integrating Application layer scanning as part of the QA cycle in your SDLC. This can help catch issues early. Tracking and metrics are also important in order to focus developer awareness.

edgescan™ can integrate into your SDLC via our API and *CloudControl* virtual appliance to help you detect vulnerabilities earlier in the development lifecycle.

PCI ASV VIEW

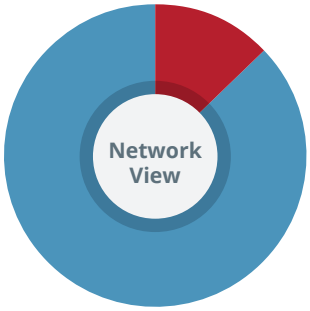
The PCI DSS standard defines that a vulnerability with a base CVSS v2 score of 4.0 or more, is a compliance fail. edgescan™ is a certified PCI ASV and assists clients with PCI DSS compliance by leveraging its fullstack security assessment technology and technical support.

18%



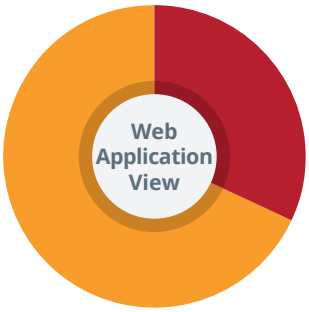
18% OF ALL VULNERABILITIES DISCOVERED IN 2017 HAD A SCORE EQUAL TO OR HIGHER THAN 4.0 – PCI DSS FAIL

13%



13% OF ALL NETWORK LAYER VULNERABILITIES DISCOVERED IN 2017 HAD A SCORE EQUAL TO OR HIGHER THAN 4.0 – PCI DSS FAIL

32%



32% OF ALL WEB APPLICATION VULNERABILITIES DISCOVERED IN 2017 HAD A SCORE EQUAL TO OR HIGHER THAN 4.0 – PCI DSS FAIL

Common Vulnerability Scoring System (CVSS), http://www.first.org/cvss/, base score, as indicated in the National Vulnerability Database (NVD), http://nvd.nist.gov/cvss.cfm (where available)

https://www.pcisecuritystandards.org/pdfs/pci_dss_technical_and_operational_requirements_for_approved_scanning_vendors_ASVs_v1-1.pdf

CVE – COMMON VULNERABILITIES AND EXPOSURES

HTTPS://CVE.MITRE.ORG/

Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cyber security vulnerabilities.

Many systems have a CVE which defines a security issues known to the public. Generally there is a workaround or a patch to mitigate this issue.

Systems with CVE's exposed generally are not being patched regularly. It takes time and effort to patch but it appears patching can still reduce ones exposure to breach and increase security significantly.

CVE's (Known Vulnerabilities) can be detected quickly using a continuous assessment model. Even though your source code does not change, a vulnerability may be discovered which may require your attention; *Continuous visibility* is the key to detecting CVE's.

CVE LANDSCAPE

Oldest CVE: CVE-1999-0517

An SNMP community name is the default (e.g. public) null, or missing.

CVSS v2: 7.5

Most Common: CVE-2004-2761

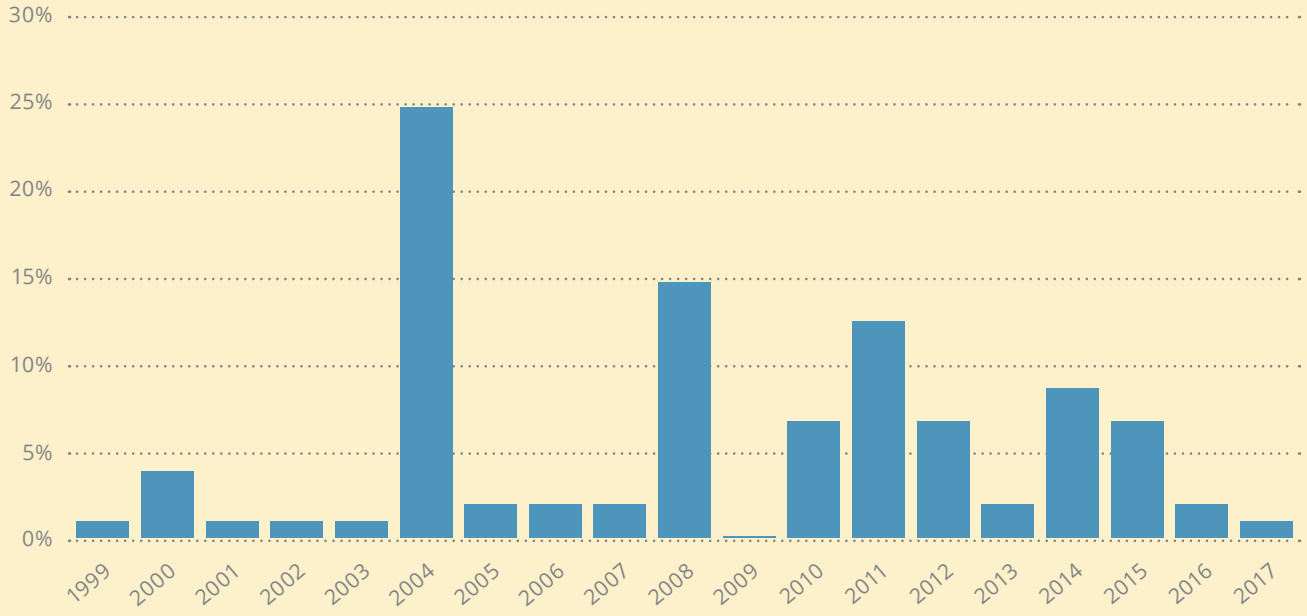
The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.

CVSS v2: 5.0

Systems with Multiple Vulnerabilities

34% of systems assessed had two or more verified CVE's

% OF CVE vs AGE



#ProTip: Patching and version maintenance is still a key part of maintaining a secure posture. Many systems have vulnerabilities which simply have not been discovered yet; once they are, a patch is usually available shortly after. It is recommended to keep pace with patching. edgescan™ can identify vulnerable systems and services and alerting can be used to notify you of any required security tasks or exposed services.

VULNERABILITY TAXONOMY

Previously we have discussed the rates of vulnerability across both Web Applications and Hosting environments. What might be interesting is what type of vulnerabilities are being discovered. The following is a high level breakdown of the types of issues being discovered.

Below Layer 7

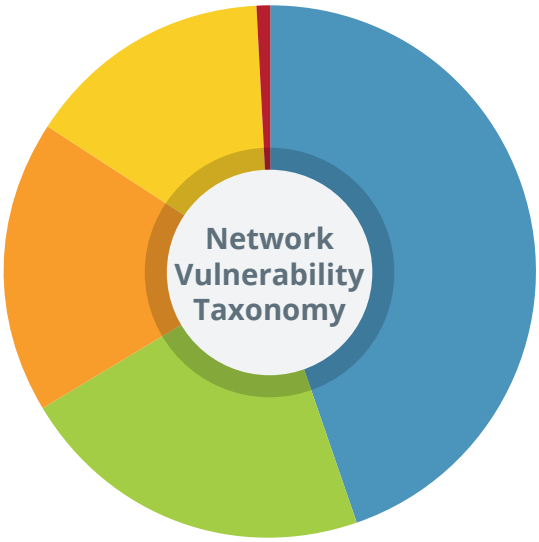
From a Host/Network perspective we still see a large % of issues are related to Cryptography which covers issues such as deprecated protocol support, CVE's and poor implementation.

Weak configuration also gives rise to a significant percentage of discovered vulnerabilities.

Layer 7

From an application security standpoint, insecure configuration is also a significant issue followed by client-side security. Injection attacks are also relatively high given how destructive they can be.

NETWORK VULNERABILITY TAXONOMY



<1%
EXPOSED SERVICES

Admin Consoles
RDP/Terminal Services
File Transfer
Sharepoint
RPC
Databases

15%
UNSUPPORTED

Microsoft IIS
Microsoft Outlook
MS 2003
OpenSSL
Samba
Deprecated SSL
Unsupported Unix
Unsupported Web Servers (IBM, Apache etc)

18%
PATCHING

Apache Vulnerabilities
Cisco Vulnerabilities
DNS Vulnerabilities
Firewall evasion
IKE Security Issues
IPMI Weaknesses
TCP/IP Stack Security
Microsoft Vulnerabilities
Open SSH Vulnerabilities
Open SSL Vulnerabilities
BSD Vulnerabilities
PHP Vulnerabilities
Wordpress Vulnerabilities

45%
CRYPTO

SSL/TLS/SSH – BREACH, SWEET, POODLE, DROWN, BEAST, CRIME
Short Keys Length
Weak Hashing
Weak Ciphers
RC4 Support

22%
CONFIGURATION

Default Credentials
FTP Exposure
HSTS Config
RDP Security
Weak SMB Config
Expired SSL/TLS certs
Misconfigured Certs
Terminal Services Security
Unencrypted/Telnet
Default Pages & Services
Lack of encryption

APPLICATION VULNERABILITY TAXONOMY

29%
INSECURE CONFIGURATION/ INSECURE DEPLOYMENT

- Directory Listing
- Development Files
- Default Documents
- Default/Weak Server/Framework Security Settings
- Debugging Enabled
- Insecure Protocols Enabled
- Insecure HTTP Methods
- Unsupported Frameworks
- Insecure Libraries

24%
CLIENT-SIDE SECURITY

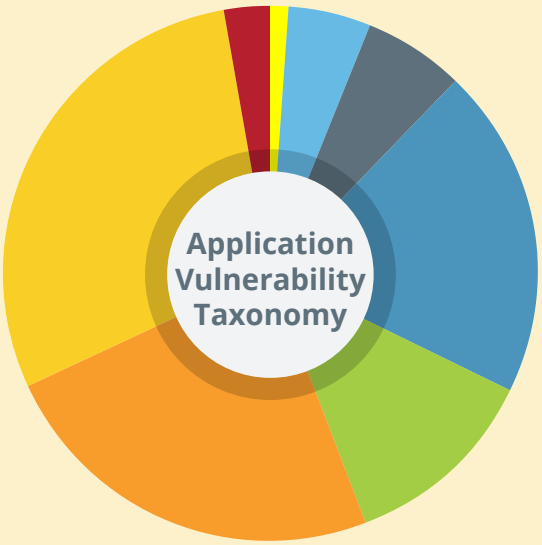
- Cross-Site-Scripting (XSS)
- Clickjacking
- CORS
- Cross-Domain Leakage
- Form Hijacking
- HTML Injection
- Open Redirection
- DOM Security

3%
EXPOSED INTERFACE

- Web Admin consoles
- Malicious file upload
- Exposed S3 buckets
- API's

1%
DENIAL OF SERVICE

- Application Layer DoS



5%
AUTHORISATION WEAKNESSES

- File Path Traversal
- Vertical Authorisation
- Horizontal Authorisation
- Bypass Client-side Controls
- Privilege Escalation

6%
AUTHENTICATION WEAKNESSES

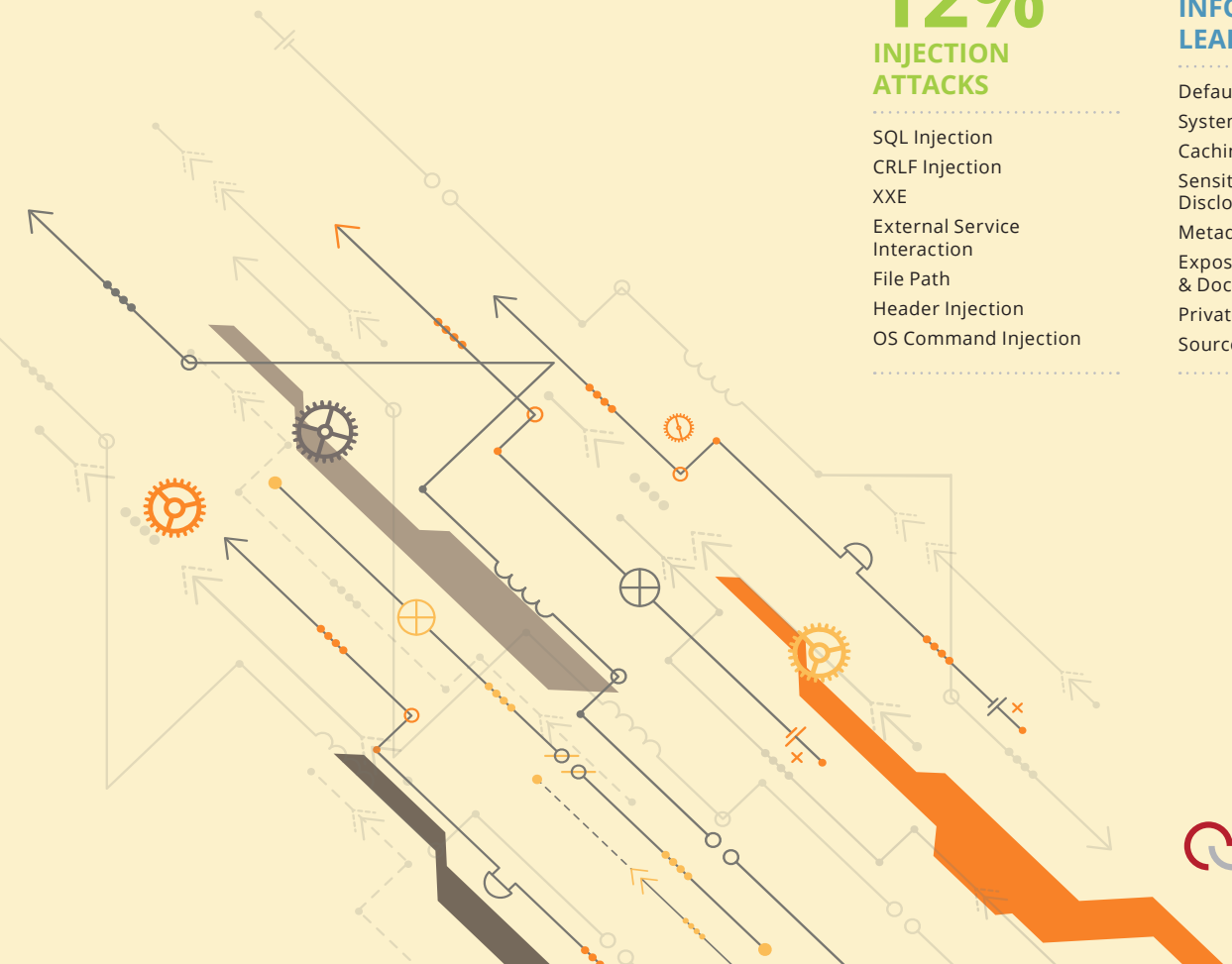
- Bruteforce
- Default Credentials
- Weak Logic
- Weak Password Policy
- Username Enumeration
- Credential transmission without encryption
- Session Management
- Weak Protocol
- No encryption
- CSRF

12%
INJECTION ATTACKS

- SQL Injection
- CRLF Injection
- XXE
- External Service Interaction
- File Path
- Header Injection
- OS Command Injection

20%
INFORMATION LEAKAGE

- Default Error Pages
- System Information Leakage
- Caching
- Sensitive Information Disclosure Weaknesses
- Metadata Disclosure
- Exposed Business Intel & Documents
- Private IP Address Leakage
- Source Code Disclosure



edgescan

CONCLUSION

AWARENESS

Application security needs to become a board-level conversation in your organization, if it is not already.

MEASURE

Management sponsorship for application security should be result-oriented to help raise your organisations security posture.

REWARD

Rewarding of development teams and gamification, including metrics and measuring the security posture of the businesses applications, should be considered.

CAPABILITY

Security champions need to have the resources and services they require to identify and fix vulnerabilities in software and supporting hosting environments faster.

VISIBILITY

Adopt a process of visibility across the entire cyber-estate. Detection of services, ports, patches and protocols supported on an on-going basis is key to understanding change and management of risk.

TEAM

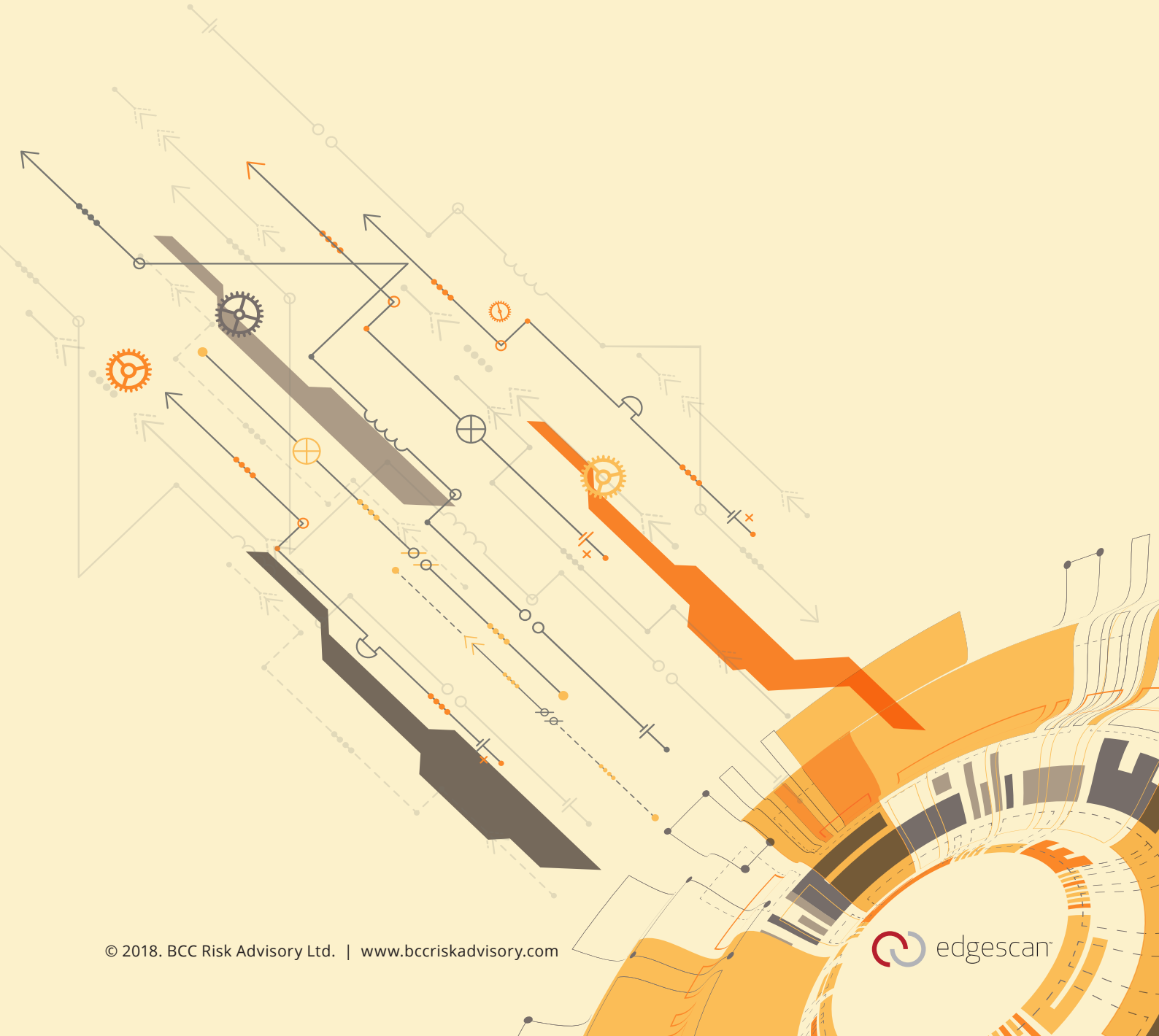
Work with IT and operations to apply scheduled maintenance windows aimed at updating systems and frameworks with security patches using a risk based approach.

BILL OF MATERIALS

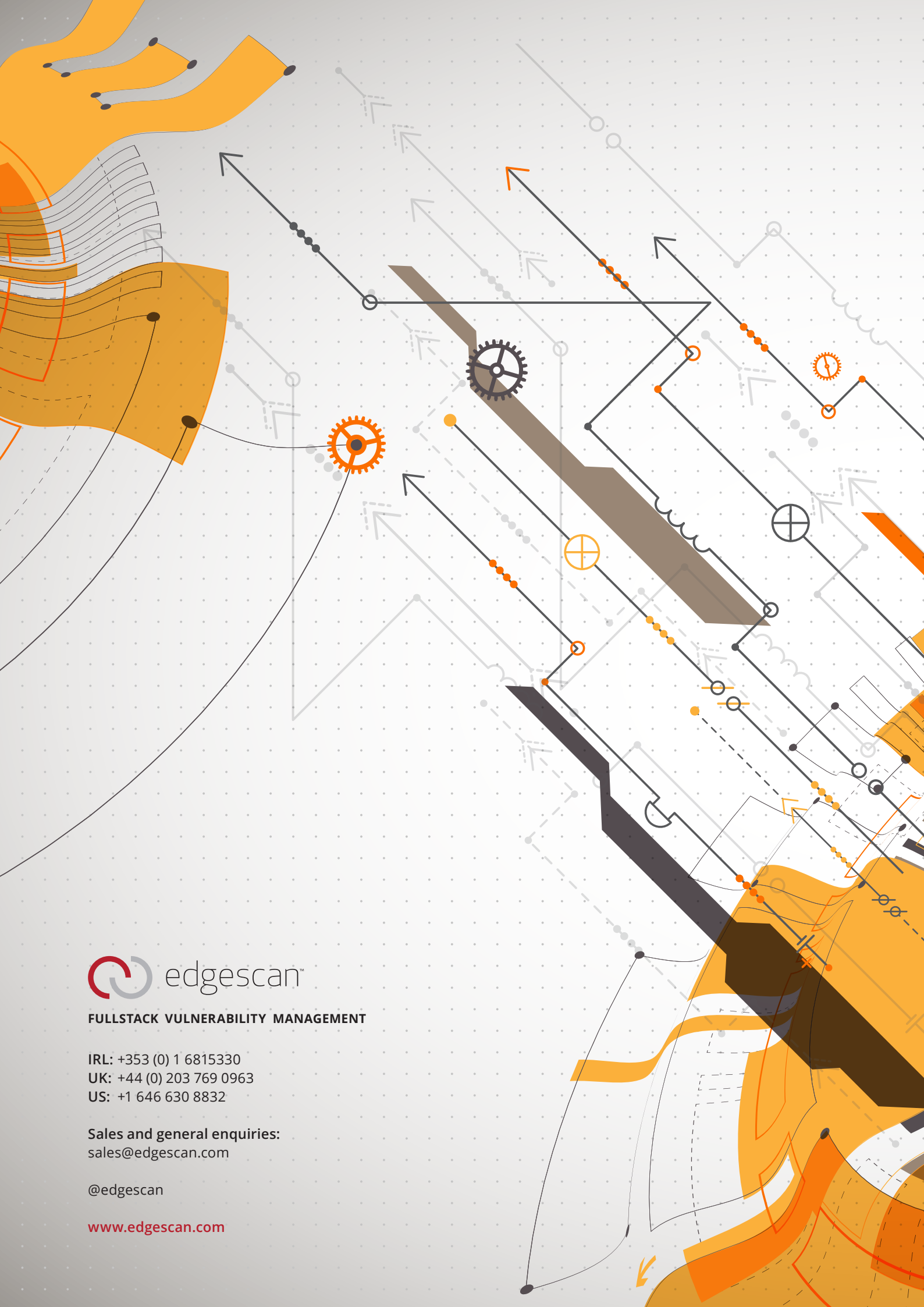
Understand the composition of software applications and prioritize the vulnerable libraries and frameworks for your teams to maintain.

KNOWLEDGE

Developer training, frequent software assessment early in the development lifecycle and security analytics, are key to implementing a security program that compliments your organisation's software development lifecycle.



edgescan



edgescan™

FULLSTACK VULNERABILITY MANAGEMENT

IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

@edgescan

www.edgescan.com