The Annual State of Cyber 2025

Backed by Triskele Labs' reports, revealing the tactics, trends, and takeaways shaping the year ahead.

DFIR GRC MDR Offensive

Behind the Breach: Triskele Labs' 2025 DFIR Findings

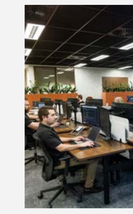
Contrary to popular assumptions, most malicious activity did not originate from traditionally expected locations such as Russia, China, or parts of West Africa. Instead, Threat Actors frequently leveraged infrastructure based in more trusted regions to evade suspicion and avoid geo-blocking.

Ransomware and Business Email Compromise dominated, accounting for more than 75% of all cases. Ransomware activity doubled, yet only 4.8% of victims paid a ransom, reflecting improved resilience.

BEC cases surged by 86%, driven by session token theft and persistence within Microsoft 365. DFIR investigations revealed recurring weaknesses in remote access controls, monitoring, and password management, particularly in healthcare and finance.

Read full report

DFIR GRC MDR Offensive



Misguided Advice and Missed Opportunities

Despite positive headlines suggesting progress, Australia's cyber security landscape remains deeply divided. Larger organisations, equipped with resources and expertise, continue to strengthen their defences and influence government policy.

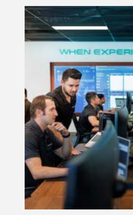
Meanwhile, small- and medium-sized businesses struggle under the weight of compliance requirements and generic advice that fails to reflect operational realities.

As "trickle down" security pressures mount, smaller firms are forced to chase certifications and frameworks without addressing fundamental risks, leaving them vulnerable to opportunistic threat actors.

To close the gap, the focus must shift toward practical, accessible, and contextual cyber advice.

Read full report

DFIR GRC MDR Offensive



A year of smarter detection, faster response and measurable improvement.

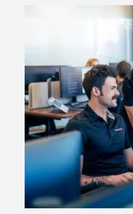
FY25 marked another year of growth and operational excellence for the Triskele Labs Security Operations Centre (SOC). As cyber threats continued to evolve in sophistication and scale, our focus remained on delivering rapid, intelligence-led detection and response across every client environment.

During the year, the SOC processed more than 260,000 alerts — a 40% increase on FY24 — driven by expanding client coverage across finance, health, education, construction and critical infrastructure.

Despite this uplift, alert density per client remained stable, underscoring the efficiency of our tuning, correlation and automation initiatives.

Read full report

DFIR GRC MDR Offensive



Exposed: What 500+ Pen Tests Reveal

Triskele Labs' State of Cyber — Offensive Report 2025 reveals key shifts in the threat landscape following more than 500 penetration testing engagements conducted across critical sectors during FY2024.

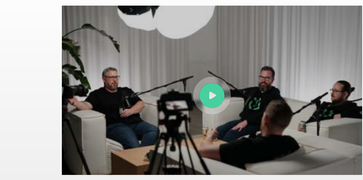
The Offensive Security team identified 3,887 vulnerabilities —averaging eight per engagement—while observing a significant decline in critical findings, indicating the value of ongoing testing and remediation programs.

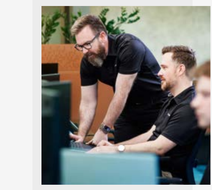
However, persistent weaknesses remain, with low-severity vulnerabilities rising and recurring flaws in broken object authorisation, authentication, and misconfiguration continuing to dominate results.

Read full report

SPECIAL EDITION OF CYBERS: STATE OF CYBER

Behind the Breach: Triskele Labs' FY25 Findings





How not to get hacked?

We examine your systems, networks, and processes to uncover vulnerabilities and weak points before attackers do.

"How Not to Get Hacked" is our high-value - targeted and quick external security review, designed to uncover what attackers see when they look at your business. We identify exposure across your internet-facing infrastructure, Microsoft 365 configuration, VPN security, and then deliver practical, prioritised advice to close the gaps before threat actors find them.

- Based on real incidents
- Straightforward advice, non-technical language
- Applicable to finance, healthcare, legal & more

Enquire today

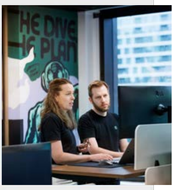
Benchmarking Microsoft 365 Security in Australian Organisations

Understanding Your Microsoft 365 Security Posture

Gain a rapid, high-impact assessment of your Microsoft 365 environment. Triskele Labs' Microsoft 365 Baseline Security Review benchmarks your configurations, licensing, and identity management against industry best practice, helping you uncover the weaknesses attackers target most.

The result — a clear, actionable snapshot of your organisation's Microsoft 365 security posture, with practical recommendations to strengthen your defences and align with standards such as the ASD Essential Eight and CIS benchmarks.

Book your M365 Baseline Review



We are the only cybersecurity experts you'll ever need to talk to.

We consider every business we work with a partner — not just a customer. At Triskele Labs, we work with you to understand your risks, goals, challenges and culture to develop Cyber Security solutions tailored to your business. With us by your side, you can be confident that your data and systems are secure — and that you have a trusted, responsive and experienced partner to protect your business.

First name*
Last name
Work Email*
Phone number
Any further information

Submit

Our podcasts
YouTube Cybers
You Tube TL Blue

State of Cyber Archive
State of Cyber 2024

Let's Connect
How Not To Get Hacked
M365 Baseline Review

Global Incident Response
1300 26 CYBER
info@triskelelabs.com

Copyright ©2025
Privacy Policy | Terms

DFIR

Digital Forensics and Incident Response (DFIR) is the process of identifying, preserving, analyzing, and reporting on digital evidence to understand and mitigate cyber incidents. This guide covers the core phases of DFIR, from initial compromise to post-incident analysis, with a focus on ransomware and business-email compromise (BEC) investigations.

Executive Summary
Background
Contributors
Incident Statistics
Incident Types
Industries Affected
Case Study: Healthcare Provider
Ransomware Investigations
Stages of a Typical Ransomware Attack
Ransomware Groups
Initial Access
Exploit Vulnerabilities
External Facing Services Abuse
Credential Theft Attacks
Phishing Attacks
Malware Delivery
Ransomware Payments
Ransomware Timeline
Lack of Logging
Persistence Mechanisms
Business-Email Compromise (BEC) Investigations
Overview
Understanding Business-Email Compromise
Stages of a Business-Email Compromise
Initial Access
Persistence
Credential Harvesting
Inbox Manipulation
Fraudulent Transfer
Detection
Detection Gaps
Missed Detection Points
Mailbox Rules
MFA Tokens
Session Token Theft
Log Retention
Emerging Risks
Lack of Visibility
Ransomware
Exploitation
Endpoint Compromise
Credential Theft
Ransomware Evolution
Ransomware Ecosystem
Ransomware Tactics
Conclusion

Executive Summary

Ransomware Remains the Dominant Threat

Ransomware continues to be the most impactful threat observed in incident response engagements, affecting organizations across multiple industries and causing significant operational disruption and financial loss.

BEC and Credential Compromise Are Critical Enablers

Business-email compromise and credential compromise remain critical enablers for ransomware and other cyber incidents, providing initial access and persistence for threat actors.

Credential and Access Gaps Are Recurring

Credential theft and access gaps are recurring issues observed across incidents, facilitating lateral movement and privilege escalation.

Internal Detection Gaps Often Allow Threats

Internal detection gaps often allow threats to persist undetected for extended periods, increasing the impact of incidents.

Logging and Visibility Are Critical for Investigations

Logging and visibility are critical for effective investigations, but are often insufficient or incomplete in compromised environments.

Background

Contributors

Incident Statistics

Incident Types

Industries Affected

Case Study: Healthcare Provider

Initial Compromise via External Remote Services

Ransomware Investigations

Overview

Stages of a Typical Ransomware Attack

Ransomware Groups

Initial Access

Exploit Vulnerabilities

External Facing Services Abuse

Credential Theft Attacks

Phishing Attacks

Malware Delivery

Ransomware Payments

Ransomware Timeline

Lack of Logging

Persistence Mechanisms

Business-Email Compromise (BEC) Investigations

Overview

Understanding Business-Email Compromise

Stages of a Business-Email Compromise

Initial Access

Persistence

Credential Harvesting

Inbox Manipulation

Fraudulent Transfer

Detection

Detection Gaps

Missed Detection Points

Mailbox Rules

MFA Tokens

Session Token Theft

Log Retention

Emerging Risks

Lack of Visibility

Ransomware

Exploitation

Endpoint Compromise

Credential Theft

Ransomware Evolution

Ransomware Ecosystem

Ransomware Tactics

Conclusion

© Threat Labs
Threat Labs Home Blog Contact Subscribe
Threat Labs Home Blog Contact Subscribe
Threat Labs Home Blog Contact Subscribe

GRC

If you only look at the flashy headlines, the cyber security industry is winning. Ransomware numbers are down. RedLine stealer has been dismantled. The head of LockBit identified. The Medibank hacker (sic) publicly shamed. But in an industry where winning and losing is defined by one question - are we enabling all companies to become more secure, the reality is far more complicated.

The Illusion of Progress
Why Australia's businesses are still losing the cyber war
The growing divide
Lack of Awareness
Compliance without context
Industry accountability
Lifting the supply chain
The real challenge

The Illusion of Progress

Why Australia's businesses are still losing the cyber war

If you only look at the flashy headlines, the cyber security industry is winning. Ransomware numbers are down. RedLine stealer has been dismantled. The head of LockBit identified. The Medibank hacker (sic) publicly shamed. But in an industry where winning and losing is defined by one question - are we enabling all companies to become more secure, the reality is far more complicated.

The growing divide

The divide between companies with effective and ineffective cyber security programs is significant. The top players have the expertise and the resources to engage with Government agencies and contribute to the profession.

The rookies aren't even making it past the starting line. Snowballing compliance burdens and ill-fitting expert advice are preventing companies with fewer resources from making progress. Much to the exasperation of the Federal Government, small- and medium-sized businesses remain naïve and inexperienced regarding the dangers they face using modern I.T. infrastructure.

> "The divide between companies with effective and ineffective cyber security programs is significant."

Lack of Awareness

The family-run winery does not understand the significance of allowing lax configurations to remain in their environment. What does "disabling legacy authentication in Microsoft365" mean anyway?

Adding to this lack of expertise, over the last 12 months we have witnessed the troubling trend of "Trickle Down Cyber Security." As larger companies become more regulated, they are implementing third-party risk management programs and pushing onerous compliance burdens down the supply chain.

Compliance without context

Does your small- or medium-sized business want to bid on a contract? Please send over your ISO 27001 certificate, SOC 2 Type 2 Report, and your business continuity plan. This is a common introduction to cyber security for many small- or medium-sized Australian businesses if they have been lucky enough to avoid getting hacked.

Now aware of the requirements, the person at the SMB who was unfortunate enough to Google ISO 27001 is tasked with implementing the ISMS, organising certification, and responding to the UpGuard questionnaires.

The net result is a cumbersome and unworkable information security framework implementation. Significant resources spent to win a contract, but lack of attention to basic technical controls means the business is no more secure than it was before the addition of 30 new policies and procedures.

> "Significant resources spent to win a contract, but lack of attention to basic technical controls means the business is no more secure than it was before."

Industry accountability

The cyber security industry is also to blame for this boondoggle. Too many organisations are out looking to make a quick buck and provide generic guidance without taking the time to understand the organization's I.T. infrastructure or how their business operates.

Governments must take a hard look at the programs and initiatives they are rolling out. If the intended recipients don't understand how to apply the advice, or worse yet, even where it find it, it's a wasted effort. Guidance needs to be written in plain English, contextualised to the size and maturity of the business, and delivered through channels that business owners actually use.

Threat actors are aware of this security gap, and they are looking for low-hanging fruit. They need their payday, after all. When threat actors discover that no multi-factor authentication exists on remote connection services, firewall access is exposed on the internet, or systems are out-of-date and insecure, they see dollar signs. Smaller companies make easier targets, and they tend to suffer more severe consequences.

Lifting the supply chain

If we want supply chain security to meaningfully improve, larger organisations must invest in educating their suppliers, providing funding or resources where possible, and adjusting their expectations based on the realities of operating a small business.

Otherwise, we're just creating compliance theatre that checks a box but doesn't lift the security needle. True uplift means rolling up sleeves and getting involved, and not outsourcing accountability to the nearest procurement team. Just the other day the Victorian Government was asking a three-person startup if they had completed an IRAP assessment.

Lastly, the security community must do better in making cyber advice accessible and relevant. That starts by understanding that a five-person accounting firm doesn't have a CISO and can't afford a GRC consultant. Advice needs to be pragmatic, actionable and based on real-world environments, not ideal-state architectures or what the ISO standard says.

The real challenge

If we can't bridge the gap between what's technically perfect and what's practically possible, we'll keep seeing the same headline: "Family business crippled by ransomware, pays ransom".

This is the biggest challenge the industry faces now.

Provide practical, easy to implement cyber security programs to those businesses that do not know they need them.

> "Smaller companies make easier targets, and they tend to suffer more severe consequences."

© All Rights Reserved. Triskele Labs

MDR

A year of smarter detection, faster response and measurable improvement.

SOC Performance and Growth
Record alert volumes, expanding client base, and continued operational efficiency through automation and tuning.
Client Growth and Sector Expansion
Efficiency at Scale
Context in the National Threat Landscape
Detection and Response Performance
Rapid detection, targeted response, and continued refinement of alert quality underpin SOC efficiency and resilience.
Detection Efficiency
Alert Quality and False Positives
Mean Time to Detect (MTTD)
Mean Time to Respond (MTTR)
Mean Time to Conclusion (MTTC)
High MTTC
Cases by Source
SIEM remains the foundation of SOC visibility, enabling comprehensive threat detection beyond the endpoint.
Overview
Case priority breakdown
Strategic Importance of SIEM
Complementary Role of EDR
Interesting Statistics
Alert volumes continue to grow while detection accuracy and true positive rates improve year-on-year.
Overview of Alert Volumes
Ticketing and Escalation Trends
Determination Accuracy and Quality
Key Takeaways
Top 10 Cases
Initial access and authentication anomalies remain dominant vectors incident environments.
Overview
Strategic Insight
Cases by Vertical
Finance, Health, and Critical Infrastructure sectors remain the most targeted industries under SOC monitoring.
Overview
Strategic Insight

SOC Performance and Growth

Record alert volumes, expanding client base, and continued operational efficiency through automation and tuning.

Client Growth and Sector Expansion

In FY23, the Triskele Labs Security Operations Centre (SOC) processed approximately 26,000 alerts — a significant increase from nearly 185,000 in FY24. This growth aligns with a 69% year-on-year rise in active Managed Detection and Response (MDR) clients across fully managed and DFIR monitoring services.

The SOC's reach expanded across several new sectors, including construction, education and logistics, while maintaining strong representation in established industries such as finance and insurance, health and community care, professional and business services, retail, FMCG and consumer services, not-for-profit, and industrial sectors.

Efficiency at Scale

Despite a sharp increase in threat activity, the average volume per client remained steady at around 220 alerts per month. This stability underscores the effectiveness of Triskele Labs' ongoing investments in correlation tuning, environment baselines, and suppression logic.

When isolating manually triaged cases, excluding those managed by in-house automation, the figure reduced further to an average of 181 alerts per client per month, reflecting the success of automation initiatives in improving efficiency and analyst focus.

Detection and Response Performance

Rapid detection, targeted response, and continued refinement of alert quality underpin SOC efficiency and resilience.

Detection Efficiency

The Triskele Labs SOC continues to demonstrate strong internal detection capability, identifying and acting on critical incidents within a median of 13 minutes. This performance reflects significant investment in tooling, automation, and analyst workflows that enable rapid validation and containment across client environments.

For context, Mandiant's M-Trends 2025 report indicates that only 37% of breaches are typically detected internally, with the remainder identified through external notification. The SOC's ability to consistently triage Mean Time to Detect (MTTD) highlights the maturity of its detection engineering and triage models, particularly across higher-risk sectors such as finance, healthcare, and professional services.

Alert Quality and False Positives

Alert fidelity remains a strategic focus. Internal analysis indicates that approximately 75% of alerts processed do not translate into actionable security incidents, a proportion consistent with broader industry experience.

Through targeted rule tuning, suppression logic, and continued enrichment, the SOC continues to reduce noise and direct analyst attention toward meaningful activity. Client-specific suppression rules and enhanced routing within the case management platform have further improved accuracy and workflow efficiency.

These measures have maintained analyst throughput and helped mitigate operational fatigue, even as telemetry volumes increase. Continuous tuning remains central to sustaining detection accuracy and response speed.

Mean Time to Detect (MTTD)

Median MTTD for critical incidents improved to **13 minutes** in FY24–25, down from 61 minutes in FY22–23. High priority incidents averaged between **30–35 minutes**, remaining well within benchmark industry performance.

This improvement reflects Triskele Labs' ongoing investment in detection engineering, threat model refinement, and enriched telemetry pipelines that accelerate context delivery to analysts.

Mean Time to Respond (MTTR)

Median MTTR for critical incidents fell to **5.6 minutes**, improving on **6.7 minutes** the previous year. This metric captures the process from detection and containment action, such as host isolation or user disablement, reflecting the speed and precision of containment workflows.

For high priority cases, MTTR rose modestly to **5.8 minutes** from **5.5 minutes**. This change is attributed to increased analyst caution and deliberation during containment actions, rather than operational delay. It also reflects success in tuning and enrichment, where non-actionable alerts are increasingly filtered before analyst engagement.

Mean Time to Conclusion (MTTC)

MTTC, the sum of detection and response time, remained well within internal thresholds of **≤60 minutes for critical** and **≤120 minutes for high** incidents.

FY24: Y24 =3.60 → 15.69 minutes
FY25: T27 =7.72 → 10.99 minutes

High MTTC

FY24: H=73 =3.56 → 23.29 minutes
FY25: TR38 =5.62 → 25.00 minutes

With internal MTTC thresholds of ≤60 minutes for critical and ≤120 minutes for high, Triskele's SOC remains well under target across both categories.

These figures demonstrate consistent containment speed and reinforce the operational maturity of Triskele Labs' SOC model — balancing automation, detection precision, and human response.

Cases by Source

SIEM remains the foundation of SOC visibility, enabling comprehensive threat detection beyond the endpoint.

Overview

Analysis of FY25 case distribution shows that **87%** of alerts originated from the **Security Information and Event Management (SIEM)** platform, **12%** from Endpoint Detection and Response (EDR/XDR), and 1% from Dark Web monitoring. Phishing triage contributed a negligible volume during the period.

These figures reinforce that while EDR solutions play an important role in endpoint-level visibility, SIEM remains the backbone of effective Security Operations Centre (SOC) and Managed Detection and Response (MDR) capabilities.

Case source distribution showing SIEM as the primary detection engine, providing comprehensive visibility beyond endpoint telemetry.

Case priority breakdown

Non-actionable alerts represent expected activity within customer environments — operationally relevant but with minimal security impact. As shown below, nearly 75% of alerts processed in FY25 were originating tools as Low or Medium severity.

Strategic Importance of SIEM

Modern cyber threats rarely remain confined to a single endpoint. Attackers increasingly exploit credentials, cloud services, misconfigurations, and legitimate cloud and SaaS identities. In this landscape, an endpoint-only view is insufficient.

A well-tuned SIEM aggregates and correlates telemetry from across the environment, including identity providers, network devices, cloud applications, and security controls. This unified perspective enables analysts to detect cross-domain activity and identify high-impact threats that would otherwise go unnoticed in isolated systems.

Complementary Role of EDR

EDR platforms remain an essential component of Triskele Labs' detection ecosystem, providing deep forensic insight and rapid containment capability at the device level. However, their scope is inherently limited. Without correlation with broader environmental data through the SIEM, incidents that span multiple vectors, such as lateral movement or privilege escalation, may evade detection.

The strong ratio of SIEM-driven detections highlights the continued value of a correlated, context-aware defence model that integrates endpoint, network, and cloud telemetry into a single operational picture.

Interesting Statistics

Alert volumes continue to grow while detection accuracy and true positive rates improve year-on-year.

Overview of Alert Volumes

Total alerts processed by the SOC increased slightly to 267502 in FY25, maintaining stability following a major uplift in FY24. The majority of cases were categorised as Medium and **Low** severity, reflecting a mature and proactive monitoring posture rather than a reactive one.

High severity alerts accounted for approximately **16%** of total cases, while **Critical** alerts continued to represent a small but strategically important proportion at around **2%**. This profile aligns with expected trends in mature SOC environments, where strong preventive controls reduce the frequency of high-impact incidents.

Ticketing and Escalation Trends

The total number of ticketed cases rose modestly to **18,442**, representing **6.2%** of total alerts. While this percentage is lower than FY24's 8.4%, it reflects improvements in automation, correlation, and suppression logic that are successfully filtering non-actionable alerts before analyst intervention.

Ticketing rates for **Critical** incidents remained high at 100, consistent with operational prioritisation policies, while **Medium** and **Low** cases saw a proportional decline due to enhanced rule tuning and enrichment processes. This indicates that the SOC is increasingly focused on high-value, actionable events rather than volume-driven escalations.

Determination Accuracy and Quality

Accuracy metrics show continued improvement in detection quality. The proportion of **True Positives** increased to 24.26% in FY25, up from 24.01% in FY24 and 18.67% two years prior, a clear indicator of ongoing refinement in correlation rules and enrichment accuracy.

Meanwhile, **False Positive** rates decreased to 59.52%, continuing a downward trajectory year on year. This reduction highlights the effectiveness of continuous tuning initiatives and the integration of automation in triage workflows. Informational outcomes dropped to just 0.39%, underscoring improved clarity in alert disposition and case resolution.

Key Takeaways

- **Stabilised alert growth** following last year's expansion suggests sustained operational maturity and effective capacity management.
- **Reduced false positive rates** reflect strong analytical discipline and refined logic.
- **Critical and high alerts remain tightly managed**, demonstrating effective prioritisation and triage discipline.

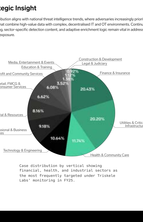
Top 10 Cases

Initial access and authentication anomalies remain dominant vectors incident environments.

Overview

Analysis of the top 10 case types across all clients shows that initial access and credential based anomalies continue to dominate SOC workloads. Cases such as **Suspicious Logins**, **Multi-Factor Authentication Network Behaviour (Fortinet/Azure)** and **Multi-Country Impossible Intermediaries**, together accounted for nearly **half of all observed cases**.

These findings reinforce that adversaries are frequently exploiting authentication pathways and misconfigured access controls to establish footholds within client networks. The prominence of "First Ingress Authentication from Country" and "Attacker Behaviour Detected" further highlights the sophistication of lateral movement and reconnaissance techniques observed throughout the year.



Top 10 detections across clients highlight initial access, credential misuse, and anomalous cloud behaviour as key risk drivers in FY25.

Strategic Insight

This pattern underscores that identity and cloud telemetry are now the primary attack surfaces. Strategic control frameworks around multi-factor authentication, geolocation policies, and privileged account monitoring continue to be essential in mitigating this risk.

The persistence of Lateral Movement – Local Credentials and Brute Force Activity within the top ten reinforces the need for ongoing investment in **detection engineering and identity telemetry correlation** across clients.

Cases by Vertical

Finance, Health, and Critical Infrastructure sectors remain the most targeted industries under SOC monitoring.

Overview

Case distribution by industry shows that **Finance and Insurance** sector continues to record the highest case volume, representing approximately 28% of all monitored activity. This is followed by Health and Community Care (17%), Technology and Engineering (15.5%), and Professional and Business Services (10%).

These sectors consistently appear among the most targeted across Australia due to their **data sensitivity, operational criticality, and interconnected digital ecosystems**. Finance and Health in particular face sustained targeting from both financially motivated and state-aligned actors.

The **Industrial and Resources** and **Consumer Services** sectors also contributed notable case volumes, reflecting growing attacker interest in operational technology (OT) and supply chain environments.

Strategic Insight

This distribution aligns with national threat intelligence trends, where adversaries increasingly prioritise sectors that combine high value data with complex, decentralised IT and OT environments. Continuous monitoring, sector-specific detection content, and adaptive enrichment logic remain vital in addressing this evolving exposure.

Case distribution by vertical showing Finance, Health, and Critical Infrastructure as the most frequently targeted under Triskele Labs' monitoring in FY25.

Offensive

Triskele Labs have the privilege of working with clients through a multitude of sectors, including Government & Defense, Financial Services, Industrial, Healthcare & Life Sciences, Retail & E-commerce, Information Technology & Telecommunications, Energy & Utilities, and Education & Research.

Introduction
Eight vulnerabilities per engagement
Severity analysis
Likelihood definitions
Consequence definitions
Vulnerability analysis
Most Common Test Types
Web Applications and Application Programming Interfaces (APIs)
External Networks
Internal Networks
OWASP Top 10
Emerging Sectors
The Emergence of AI In Cyber Security

Introduction

Eight vulnerabilities per engagement

Triskele Labs have the privilege of working with clients through a multitude of sectors, including Government & Defense, Financial Services, Industrial, Healthcare & Life Sciences, Retail & E-commerce, Information Technology & Telecommunications, Energy & Utilities, and Education & Research.

During the last financial year, as global cyber threats intensified, our team conducted over 500 engagements. Although the number and severity of findings varied considerably across these assessments, we identified a total of 3,887 vulnerabilities, an average of nearly eight per engagement and fifteen new vulnerabilities each day.

Upon further analysis, several notable trends emerged. The incidence of critical vulnerabilities has declined, while the number of longstanding clients engaged in continuous testing has grown. This relationship highlights the direct impact of regular penetration testing and the implementation of its recommendations on reducing overall risk within client environments.

Severity analysis

All identified issues are assigned a risk rating to allow for prioritisation of remediation efforts. Triskele Labs utilises a custom risk rating framework to identify risk level, built from tried and trusted processes and experience. The Triskele Labs framework is detailed below.

Impact			
	Major	Moderate	Minor
Likely	Critical	High	Medium
Possible	High	Medium	Low
Unlikely	Medium	Low	Low

These Can be derived from the following principles:

Rating	Example Characteristics	Resolution
Critical	• Previous compromise • Definite sensitive information disclosure • Critical systems impacted • Complete compromise • Trivial exploitation • Authentication bypasses	Within 7 days
High	• Possible sensitive information disclosure • User account compromise • Trivial exploitation • No countermeasures	Within 30 days
Medium	• Possible limited information disclosure • Requires a skilled attacker • Custom exploits or code • Some countermeasures in-place	Within 90 days
Low	• Critical data not at risk • Requires several attack vectors • Difficult to exploit • Countermeasures in place to prevent	Within 180 days
Info	• Notification of a quirk or bug with no impact • Best practice recommendation that may improve security posture.	

- **Risk:** Likelihood + Impact.
- **Likelihood:** Vulnerability + Threat.
- **Vulnerability:** An error or weakness in the design, system implementation or system.
- **Threat:** A person (internal/external) or something that can cause damage to an asset.

Impact: Loss of confidentiality, integrity, availability & accountability. It can consist of ease of vulnerability being detected, exploited, and discovered or information leakage.

Likelihood definitions

UNLIKELY: Although a flaw or weakness exists, this flaw is either exceedingly difficult to exploit, would require a highly skilled attacker, needs to be combined with other vulnerabilities in order for exploitation to occur, or is otherwise affected by factors which reduce the likelihood, such as hardening or protections.

POSSIBLE: An attacker with a moderate level of skills and knowledge may be able to exploit this flaw or weakness, however the flaw is not widely exploited.

Likely: The flaw is well-know and exploitable by a novice or inexperienced attacker.

Consequence definitions

Minor: The result of exploiting the flaw or weakness is a small gain for the attacker. This could include access to information that may assist other attacks which is not highly sensitive. The business should experience little impact as a result of exploitation of this flaw.

Moderate: Exploitation of the flaw would result in the attacker gaining access a low level of access to a resource, or access to sensitive information, however there are limitations and restrictions on this access.

Major: Exploitation of the flaw results in a high level of access to the attack, or a major change impacting the business. This is a position from which significant damage can be caused. This includes access to highly sensitive information.

Vulnerability analysis

The following provides a broad overview of trends and assessments conducted by Triskele Labs.

Metric	Prior to 2024	Post 2024
Average vulnerabilities per assessment	7.5	7.76
Assessments with at least 1 Critical vulnerability	11	6
Assessments with at least 1 High vulnerability	82	138

Severity Breakdown	Prior to 2024	Post 2024
Critical	18 (0.8%)	10 (0.3%)
High	198 (8.3%)	304 (8%)
Medium	573 (24.1%)	872 (22.8%)
Low	1219 (51.4%)	2072 (54.2%)
Informational	365 (15.4%)	567 (14.8%)

Key takeaways:

- Overall volume and density are almost identical: ~7.5 to 7.76 vulns per workspace in both timeframes.
- Critical issues are proportionally rare post-2024 (0.3 % vs 0.8 %), and fewer engagements identified any Critical findings.
- High severity issues remained at ~8 % of all vulnerabilities for both periods, however a higher number of engagements post 2024 (138 vs 82) saw at least one High finding, reflecting the larger sample.
- Medium & Informational vulnerabilities reduced slightly in share; while Low risk findings rose from ~51 % pre-2024 to ~54 % post-2024.

Most Common Test Types

Consistent with previous years, the three most common types of penetration testing include the following:

Web Applications and Application Programming Interfaces (APIs)

Designed to identify and exploit vulnerabilities in web applications and their supporting APIs, from small, single page brochure style web applications, to large, complex, Customer Relation Management (CRM) software. The primary goal is to evaluate the

application's resilience against common threats. This testing involves a combination of automated scanning and manual techniques to assess business logic, input validation, access controls, and more. Inclusions typically cover OWASP Top 10 vulnerabilities.

External Networks

Focuses on assessing the security posture of an organization's internet-facing assets, such as firewalls, VPN gateways, email servers, and public IP ranges. The primary goal is to identify and exploit vulnerabilities that an external attacker could leverage to gain unauthorized access to the internal network or sensitive systems.

Internal Networks

A controlled assessment that simulates an attacker who has already gained access to an organization's internal environment, whether through physical access, social engineering, or as a rogue employee, in what is known as an "assumed Breach" scenario. The primary goal is to evaluate the effectiveness of internal security controls in preventing privilege escalation, lateral movement, and unauthorized access to critical systems and sensitive data

OWASP Top 10

Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within organizations into one that produces more secure outcomes.

Our 2024 analysis highlights five security gaps as repeat offenders:

- Broken Object Level Authorisation has risen to the top as attackers still exploit simple ID manipulation in APIs and web applications to harvest or tamper with data, placing customer records at constant risk.
- Broken Authentication continues to enable credential stuffing and session hijacking, turning weak login flows and long-lived service tokens into fraud and compliance penalties
- Server-Side Request Forgery remains critical because cloud workloads that fetch URLs on behalf of users allow adversaries to reach internal metadata services and steal keys that can compromise entire environments.
- Security Misconfiguration still plagues mature teams, with default credentials, open buckets, and verbose error pages giving intruders easy footholds that quickly escalate to full outages
- Improper Assets Management exposes untracked or outdated hosts, leaving known vulnerabilities unpatched and hidden data flows unmonitored so lack of real-time asset inventory can undermine every other control.

Emerging Sectors

Two key emerging fields which are experiencing the highest rate of testing growth are environments which contain Operational Technology (OT).

Transport, healthcare, and infrastructure are growing at a rapid pace, and are naturally a more prominent target for cyber security related threats. As these sectors routinely utilising unique hardware for highly specialised tasks and capabilities, conducting frequent and thorough testing has become paramount to ensuring operational stability, and protection of customer information.

While Operational technology holds significant importance, not all specialised tools are "air-gapped" or sufficiently segmented. This has a direct relationship with the second emerging field, being red team, or "adversarial simulation" style testing. This testing ensures that, alongside all the default internal network, active directory, and network segmentation best practices are well designed, architected, and adhered to, but that the Security Operations Centre teams are operating with full visibility and responsiveness to incoming threats of a more stealthy and targeted approach.

These tests have highlighted the importance of adherence to the more baseline principles such as credential management, Multi-Factor Authentication (MFA), which are still the most common access vector in the majority of real world attacks, and penetration testing exercises.

The Emergence of AI In Cyber Security

An ever-increasing aspect within cyber security is the implementation of Artificial Intelligence, Machine Learning, and Large Language Models within the security landscape. This pertains not only to the creation of applications via LLM assisted codebase creation, but also within defensive and offensive tools used to conduct automated testing and automated assessment. These tools should be treated with caution, as they are disruptive and may introduce a multitude of potential vulnerabilities, with the emphasis on creating a "working baseline" with no emphasis on security best practices.

About:

The Offensive team at Triskele Labs is recognised as an industry leader in identifying and sharing critical vulnerability insights on both local and global scales. Supported by highly qualified specialists, we conduct in-depth trend analyses to ensure comprehensive coverage of both established and emerging techniques within the continually evolving threat landscape.

Our expert penetration testers work diligently to ensure the efficacy of security implementations of clients' networks and environments, both physical and virtual. The main priority of penetration testing is to reveal potential entry points before malicious actors can exploit them and provide our clients with clear, prioritized, and actionable recommendations for remediation.

© All Rights Reserved, Triskele Labs