OWASP
NEW
ZEALAND
owasp.org.nz

State of AppSec in New Zealand

2022 Survey Report

Volume 1 – Executive Summary

Contents

Introduction

In 2021, as group of OWASP®* New Zealand volunteers discussed application security (AppSec) awareness and training in New Zealand, the idea formed within the group that it would be useful to have some *metrics* regarding the AppSec attitudes and practices of New Zealand organisations. Given the unique nature of New Zealand's information technology industry, they recognised the various "State of XXX" reports published in other parts of the world are not representative of the situation here, and undertook to fill that gap.

Over the next several months, this group of volunteers put together the inaugural State of AppSec in New Zealand Survey, the results of which are summarised in this document. In this volume, we present an overview of the survey development and data collection process, accompanied by highlights from the collected responses.

The companion document to this one (Volume 2) presents further information on the survey's structure and design, along with a complete listing of the questions presented in the 2022 survey, and the responses received.

Both documents can be found on the OWASP® New Zealand Chapter's website at: https://owasp.org/www-chapter-new-zealand.

Survey Design

The State of AppSec in New Zealand Survey seeks to gather insights from New Zealand organisations of all types, and across all industries and sectors. In designing the survey, the project team worked to ensure the survey would be meaningful and relevant to any New Zealand organisation that develops or uses software – in short, any New Zealand organisation.

To this end, the team created the survey to adapt to the type of organisation about which a response is being submitted. Each respondent is presented one of four distinct-but-similar series of survey pages, based on the general nature of their organisation's approach to software development/acquisition and deployment. In response to the question "Which of the following statements best describes your organisation?" the respondent was required to select one of the following options:

- We use only "off-the-shelf" commercial software
- All our development and deployment of custom applications is outsourced
- We outsource development, and deploy applications in our own environment
- We develop applications in house

Based on their response to this question, the respondent was then presented with a predetermined subset of the survey's questions.

It's important to note that the survey focuses on organisations. While it may be informative to learn about individuals' perceptions and attitudes around AppSec, that is not the purpose of this survey. To be included in the survey's results, therefore, each respondent was required to indicate the organisation about which they were submitting their response; any submission lacking that information was excluded from the results.

Data Collection and Clean-up

The 2022 survey was published in mid-May, and the first response was received on the 24th of May. The survey remained open for responses through the 31st of July, with the last response recorded on the 18th of July.

A total of 91 responses were received. 17 responses were removed from the data set, due to meeting one or more of the following conditions:

- The response was superseded by a later response submitted by the same individual;
- The response did not contain an organisation name;
- The response was completely blank; or
- The response contained an intentionally invalid name (e.g., “Test User”).

Of the 74 individual responses remaining, 45 were the singular response for an organisation. An additional 11 organisations were represented by two (6 organisations), three (3 organisations), or four (2 organisations) responses, accounting for the remaining 29.

After consolidating multiple responses, the final data set contained responses representing 56 distinct New Zealand organisations. This fell significantly short of the project team’s target of at least 100 organisations in the final data set. Given the small overall sample size represented, caution should be exercised in basing conclusions or projections on the results presented herein.

For questions presented to only a portion of the respondents, the number of responses received was significantly less than the total. This should be recognised as a further limitation of the results presented herein – questions for which only a small number of responses were received are unlikely to be representative of New Zealand organisations on the whole and great care should be taken in basing inferences on those results.

Survey Highlights

While it is true the 2022 survey results represent only a small fraction of New Zealand organisations, the responses received are nonetheless informative.

Several notable statistics from the 2022 Survey:

- **96 percent** of organisations expressing an opinion (79% of the total) feel there is a technology skills shortage in New Zealand. Specific skills identified as gaps for organisations in the coming year include:
    - DevSecOps: 64%
    - Cloud Security: 63%
    - Threat analysis: 52%
    - Risk assessment and management: 48%
    - Security operations: 46%
- **79 percent** of organisations[†] maintain a Risk Register, in some form.
- **73 percent** of organisations have, or are building, a vulnerability and patch management program for bespoke applications.
- **63 percent** of organisations utilise centralised logging for their applications.
- **58 percent** of organisations define security requirements for the applications they build or acquire from a requirements framework and/or compliance-related standards.
- **56 percent** of organisations perform penetration testing on their applications at a regular cadence.
- **54 percent** of organisations have a secure coding standard in place.
- **43 percent** of organisations incorporate automated security checks in their deployment processes.
- **36 percent** of organisations have a complete inventory of applications they use and know which of those are most critical to the organisation.
- Only **20 percent** of organisations have a vulnerability disclosure or Bug Bounty program in place – either formal or informal.

[†] In each case where 'organisations' is used in relation to survey results, it should be taken to mean "organisations responding to the 2022 Survey."

Organisation Type

As noted earlier, each respondent was required to select one of four options to describe their organisation's approach to developing or acquiring software. **73 percent** of the organisations responding to the 2022 Survey develop software applications in-house.

Response	Count	Proportion
We only use "off-the-shelf" commercial software	6	11%
All of our development and deployment of custom applications is outsourced	5	9%
We outsource development, and deploy them in our own environment	4	7%
We develop applications in-house	41	73%

Governance, Risk, and Compliance

The survey asked whether organisations maintain a complete list of all applications they use. **82 percent** of organisations reported they maintain a list of some sort but, for **46 percent** of organisations, the list is either incomplete or not prioritised.

Do you have a list of all your applications, especially your critical ones?	Count	Proportion
Yes, we have a complete list and know which applications are critical	20	36%
Yes, but the list is incomplete	17	30%
Yes, but our applications are not prioritised	9	16%
No	4	7%
Don't know / No response	6	11%

When asked if they maintain a Risk Register, **70 percent** of organisations reported they maintain a formalised Risk Register in either an application for the purpose or as a spreadsheet.

Do you maintain a Risk Register?	Count	Proportion
Yes, in an application	19	34%
Yes, in a spreadsheet	20	36%
Partially, in emails or similar formats	5	9%
No	5	9%
Don't know / No response	7	12%

When asked if they have a vulnerability and patch management program for their bespoke applications, **73 percent** of organisations reported they either have one in place or are actively working on one.

Do you have a vulnerability and patch management program for your customised applications?	Count	Proportion
Yes	26	46%
It's a work in progress	15	27%
No	7	13%
Don't know / No response	8	15%

Security Requirements

When asked how they go about defining security requirements for their applications – whether purchased "off the shelf," outsourced, or developed in-house – **58 percent** of organisations reported they base those requirements on either an existing requirements framework or compliance-related standards.

How do you define Security Requirements for your applications?	Count	Proportion
Based on a requirements framework	7	13%
Based on standards and/or regulatory compliance	25	45%
We perform threat modelling exercises	10	18%
Based on the knowledge of our team members	10	18%
We don't define security requirements	3	5%
Don't know	1	2%

Penetration Testing

When asked about their approach to penetration testing, **77 percent** of organisations reported they perform at least some penetration testing.

What is your approach to penetration testing?	Count	Proportion
We perform penetration testing at a regular cadence based on criticality of the applications	31	56%
We perform penetration testing only for new applications	1	2%
We perform penetration testing to meet compliance requirements	7	12%
We perform *ad hoc* penetration testing	4	7%
We don't perform penetration testing	6	11%
No response	7	12%

Application Security Program

When asked about their application security (AppSec) programs, **59 percent** of organisations reported they have one. However, it's managed as a separate program (from broader security and/or development programs) in fewer than half of those organisations

Do you have an Application Security program?	Count	Proportion
Yes	14	25%
Partial, AppSec is a responsibility of wider security team	9	16%
Partial, AppSec is a responsibility of development teams	10	18%
No, there isn't an AppSec program	5	9%
Don't know / No response	18	33%

Security Testing

When asked if security testing is a part of development, **53 percent** of organisations reported at least partial coverage of security tests. Organisations also reported using a variety of security testing methodologies.

Is security testing a part of the development phase?	Count	Proportion
Yes	18	32%
Partially	12	21%
No	7	13%
Don't know / No response	19	34%

Which of the following testing methodologies do you use during the development phase?	Count	Proportion
Test scripts to verify security requirements	23	41%
Automatic testing for security regressions	20	36%
Randomisation or Fuzzing	8	14%
Abuse case testing, from functional requirements	11	20%
DOS and Security denial of service	5	9%

Deployment and DevSecOps

Interestingly, only **4 percent** of organisations reported they implement automated security checks in their deployment pipelines and halt deployment ("break the build") when a check fails. Another **39 percent** of organisations reported they implement security checks, but *do not* halt deployments on security check failures. Organisations reported using a variety of practices and tools in application deployments, along with a variety of security testing tools. **41 percent** of organisations reported they integrate tools into their CI/CD pipelines.

Do you implement automated security checks in your deployment process?	**Count**	**Proportion**
Yes, we have tools and we break builds based on testing	2	4%
Yes, we have tools and they are part of the build processes	22	39%
No	8	14%
Don't know / No response	24	43%

Which of these practices do you use to deploy your applications?	**Count**	**Proportion**
Automation (CI/CD)	32	57%
Infrastructure as Code (IaC)	29	52%
Cloud Native tools	22	39%
Containers	29	52%
Serverless / Function as a Service	21	38%
Secrets Management	26	46%
Application Security Testing (AST) tools	23	41%
Code Repositories	32	57%
Open-source dependency verification	23	41%
I don't know	3	5%

Which of the following AppSec tools does your organisation utilise?	**Count**	**Proportion**
SAST - detects issues in the code we write	21	38%
DAST - detects issues in a running application	13	23%
IAST - detects issues by monitoring the testing process	7	13%
SCA - detects issues in third-party libraries used	16	29%
Web Application Firewall - sits in front of the application to protect against attacks	28	50%
Application Risk Management - prioritises remediation of vulnerabilities and exposures	15	27%
Operating System / Network Vulnerability scanner	25	45%
Cloud Security Posture Management (CSPM)	20	36%
Infrastructure as Code (IaC) scanning	16	29%
Container scanning	22	39%

Are security tools integrated into the CI/CD pipeline?	Count	Proportion
Yes	23	41%
No	12	21%
We don't have CI/CD pipelines	1	2%
No response	20	36%

Cloud Security

Not surprisingly, **77 percent** of organisations reported they use cloud services to deploy applications they use. Cloud deployment strategies varied, with **45 percent** of organisations reporting they utilise multiple cloud service providers (CSPs) in either cloud-only or hybrid solutions. **68 percent** of organisations also reported they leverage security tools – native tools provided by the platform, third-party tools, or both – to monitor the security of their cloud-based workloads.

How do you manage your application workloads?	Count	Proportion
Cloud only, with multiple cloud service providers	6	11%
Cloud only, with a single cloud service provider	8	14%
Hybrid, with multiple cloud service providers	19	34%
Hybrid, with a single cloud service provider	7	13%
On-premise only	1	2%
Don't know / No response	15	26%

Do you use security tools that are native to your cloud provider?	Count	Proportion
Yes, we rely exclusively on native security tools available on the CSP's platform	10	18%
Yes, but we also deploy third-party security tools	23	41%
No, we only use third-party security tools	5	9%
No, we don't use any security tools to protect our cloud environment	1	2%
Don't know / No response	17	30%

Technology Skills

When asked if they feel there is a shortage of technology skills in New Zealand, 96 percent of those expressing an opinion (44, or 79%, of the survey respondents) reported they do. Organisations reported a variety of security-related skills as areas of anticipated shortage, along with several noteworthy tactics for bridging the gaps.

Do you feel there is a technology skills shortage in New Zealand?	Count	Proportion	Proportion (excl. 'No response')
Yes	44	79%	96%
No	2	4%	4%
No response	10	18%	---

What are the important skills needed?	Count	Proportion
General information security	28	50%
Security operations	26	46%
Risk assessment and management	27	48%
Threat analysis	29	52%
Network security	18	32%
DevSecOps/AppSec	36	64%
Cloud Security	35	63%
Other (Diplomacy)	1	2%
Other (Supply Chain Risk Management)	1	2%
Other (Everything)	1	2%

How are you addressing the skills shortage?	Count	Proportion
We are able to hire internationally	20	36%
We are utilising third parties/contractors	29	52%
We are hiring more interns and graduates and providing training	26	46%
We are upskilling existing team members	33	59%
Other (Market recruitment)	1	2%
Other (We train developers)	1	2%
Other (Making do with what we have)	1	2%

Acknowledgements

DATACOM

The State of AppSec Survey Project team wishes to acknowledge the support provided by Datacom Systems Limited (NZ), without which this project would never have happened. Datacom provided access to their Survey Monkey subscription, which was used to create and deliver the survey. In addition, members of Datacom's Application Security Services team were granted "release time" to work on the Survey in 2022.

The project team also wishes to acknowledge the contributions of the following volunteers, who contributed significantly to the Survey's development and execution:

- Kevin Alcock
- Raafey Khan
- Amith Murthy
- John-Paul (JP) Sikking