PIXIEPOINT SECURITY

Our Specialised Security Solutions for Your Advanced Security Threats

Our Services

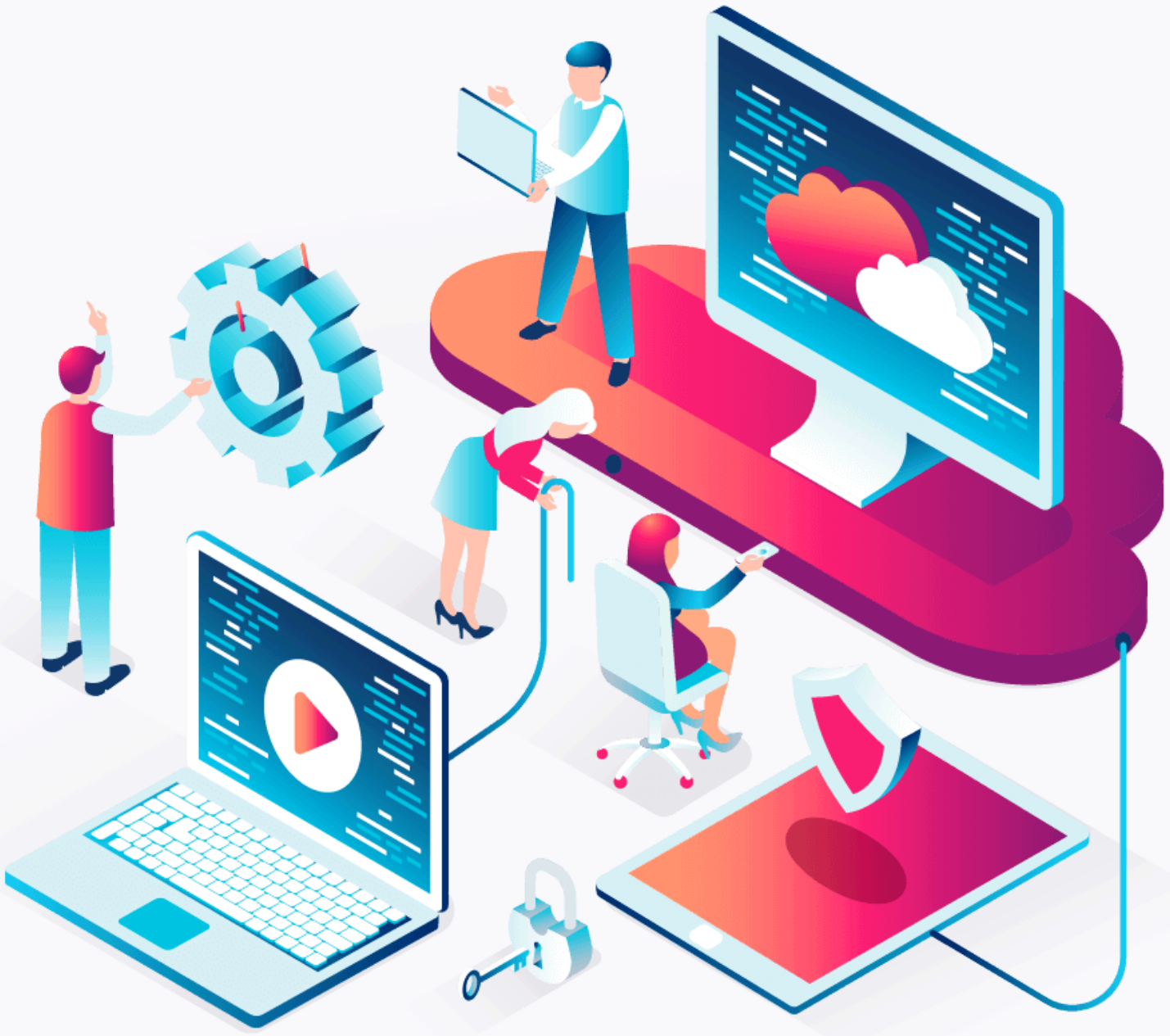
PixiePoint Security is a cybersecurity consultancy boutique that offers niche and bespoke research services. Our researchers thrive on applying our multi-disciplinary technical expertise to deliver the intelligence, capabilities and knowledge for your organisational cybersecurity challenges.

Please contact us to find out how we can help your organisation.

Our Services | Contact Us

Twitter | GitHub | LinkedIn

Our Services



Vulnerability Discovery

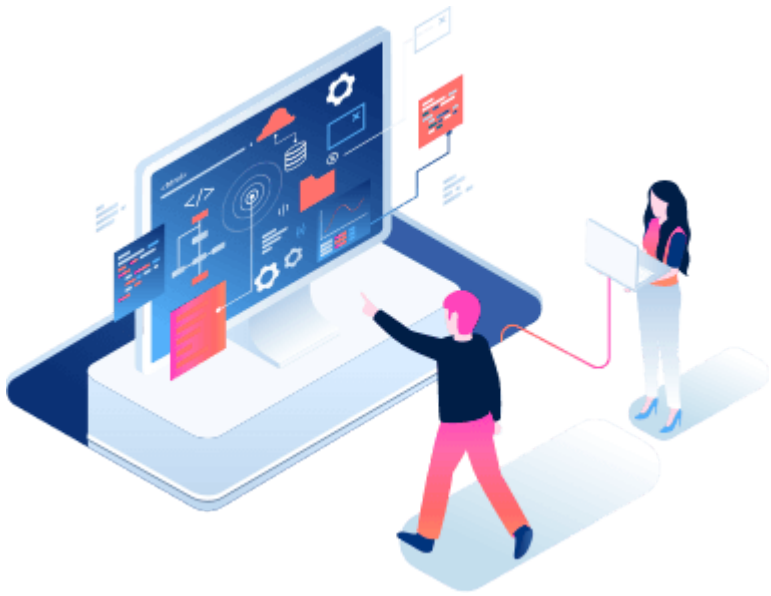
Description | Methodologies | Deliverables

The vulnerability discovery service aims to provide you with the **(offensive) intelligence** of target software systems. It is an in-depth security assessment with the end-goal of discovering and demonstrating critical 0-day and N-day security weaknesses. To achieve this, our experienced researchers will utilize our custom set of methodologies and program analysis strategies.

This service can be useful to complement the software-development-life-cycle (SDLC) prior to products shipping for vendors, or as independent security evaluation prior to products purchase for enterprises.

The pricing of vulnerability discovery service varies on the complexity and thoroughness of assessment. We will work with you closely to manage the costs. Please contact us for additional information.

Contact Us →



Malware Analysis

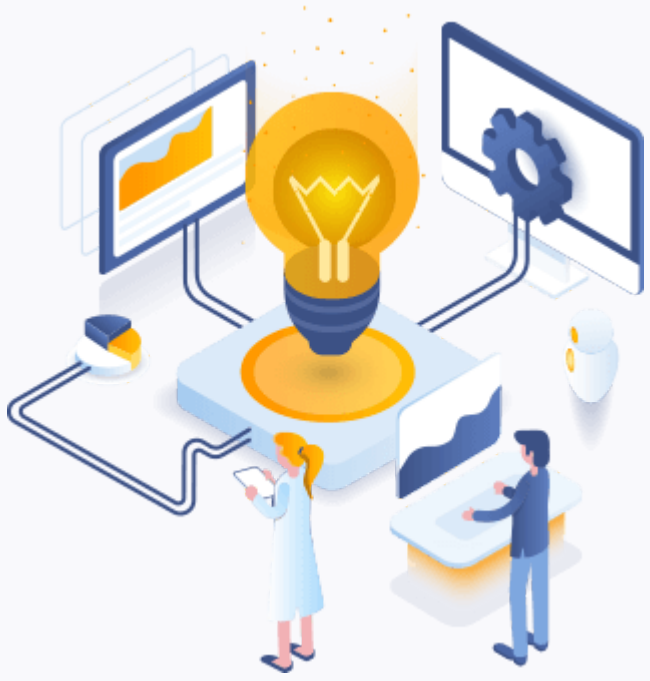
The malware analysis service aims to provide you with the (defensive) intelligence of hostile code in your systems and infrastructure. It is an in-depth assessment of suspicious applications to determine potential malicious behaviour. Combining both static and dynamic reverse-engineering techniques, our experienced researchers will gain insights to such activities and details:

- Obfuscation and deobfuscation techniques
- Evasion and hiding techniques
- Code injection techniques
- Persistence mechanisms
- Host and network traffic analysis of targeted data, harvesting and exfiltration
- Host and network traffic analysis of beacon to command and control servers
- Host and network traffic analysis of further infection to more systems

The deliverables for this service are assessment reports describing malicious behaviour and indicators-of-compromise. This service can be useful to complement existing incident response procedures or to offer second-opinion assessments.

The pricing of malware analysis service varies on the service level and duration of engagement. We will work with you closely to manage the costs. Please contact us for additional information.

Contact Us →



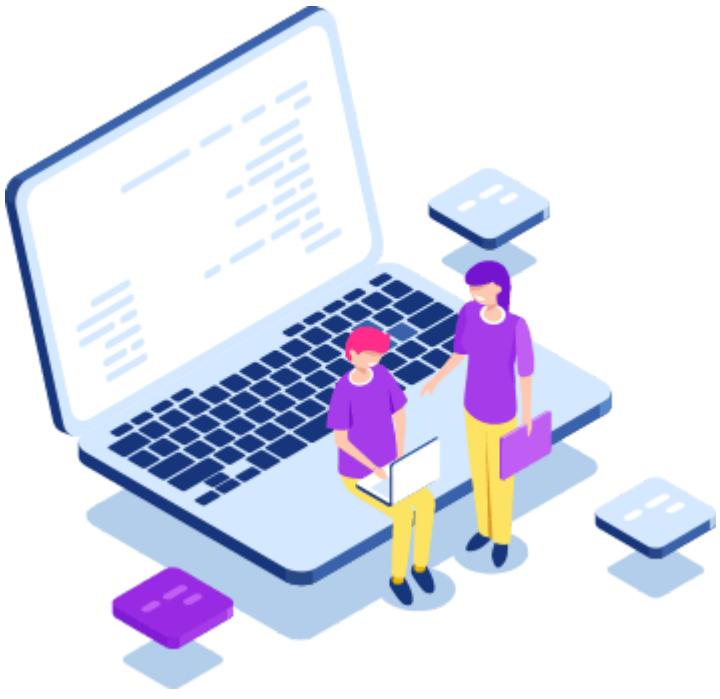
Security Tools Development

The security tools development service aims to provide you with custom capabilities to improve your existing assessment workflow and processes. As both developers and users, our experienced researchers understand that tools have to be functional, practical, efficient, stable and easy-to-use all at the same time. In addition to development, we value-add by sharing our experiences with different technologies to conceptualise your custom tools. Examples of security tools that we develop includes:

- Vulnerability static analysis tools
- Vulnerability dynamic analysis tools
- Vulnerability testing tools
- Vulnerability triaging tools
- Malware analysis tools
- Malware families classification tools
- Penetration-testing and red-teaming tools

The pricing of security tools development varies on the complexity and scale of tool-requirements. We will work with you closely to manage the costs. Please contact us for additional information.

Contact Us →



Trainings and Workshops

We offer vulnerability discovery and malware analysis training classes and workshops for all technical levels to share our knowledge and expertise. Training classes are structured learning with planned syllabus consisting of theoretical and practical components. As these are intended for students who may be new to the topics, the practical component will not exceed 40% of the schedule. The class syllabus may be custom-tailored to address specific requirements of your organization.

Workshops are 100% custom-tailored classes with unstructured learning and maximal practical component. Before commencement of the workshop, we will work closely with you to set the objective (eg: "assess the security of application X") and learning format (eg: duration of each task). During the workshop, we will lead the students in brainstorming, identifying, shadowing and executing individual tasks. Any discoveries made during the class will belong to you. As these are more hands-on in nature, workshops are intended for students who are already familiar with the theoretical knowledge.

The pricing of trainings and workshops varies on the syllabus and duration. Please contact us for additional information.

Contact Us →

PIXIEPOINT SECURITY

About

PixiePoint Security is a cybersecurity consultancy boutique that offers niche and bespoke research services.