



# Enhance Your Reverse Engineering Skills

## Master Binary Ninja with Help from Industry Experts

Stop wasting time and resources on manual reverse engineering tasks. Leave behind IDA Pro's steep learning curve and licensing fee. Learn to use Binary Ninja's rich feature set, solid API and accessible intermediate languages to develop advanced, automated analysis capabilities.

Our modular training offerings can be organized to suit your company's needs. You choose the number of skills and days to spend honing them.

### INTRODUCTORY

---

#### Reverse Engineering with Binary Ninja (1 Day)

Master Binary Ninja's user interface and the basic concepts behind reverse engineering binaries. By the end of this one-day module, students will be able to reverse engineer software and automate simple tasks. Topics include:

- Disassembly and linear views
- Creating and applying types to functions and variables
- The Binary Ninja Intermediate Languages – BNIL
- Installing and using plugins
- Introduction to the Python API and the script console

### INTERMEDIATE

---

#### Automated Reverse Engineering with Binary Ninja (2 Days)

Take your reverse engineering skills to the next level. This two-day training module dives deeper into the Python API. By the end of the module, students will be able to automate common analysis tasks, as well as extend Binary Ninja's built-in functionality with plugins. Topics include:

- Comprehensive coverage of the Python API and best practices
- Building analysis tools on top of both LLIL and MLIL
- Advanced analysis with the ILs' SSA forms
- Automated structure recovery
- Writing pre- and post-analysis callbacks

## ADVANCED

### Automated Malware Analysis with Binary Ninja (2 Days)

Building on the *Automated Reverse Engineering* module, this two-day module provides a toolbox for tackling the advanced techniques that malware uses to hide or obscure its functionality. By the end of the module, analysts will be able to write plugins that detect and deobfuscate strings and control flow to make sense of a binary's functionality, as well as scripting detection routines to identify malicious behavior for batch processing. Topics include:

- Automating string deobfuscation with the IL
- Control flow deobfuscation and recovery
- Behavioral fingerprinting

### Vulnerability Research with Binary Ninja (2 Days)

Building on the *Automated Reverse Engineering* module, this two-day module gives researchers the tools to automate bug-hunting tasks in binary applications, then write exploit payloads in C with Binary Ninja. Exercises are provided as a friendly Capture-the-Flag format. At the end of the module, students will be able to find and exploit vulnerabilities in binary code without access to source. Topics include:

- Automating vulnerability discovery with BNIL
- Triaging and exploiting
- Rapid payload development with the Shellcode Compiler
- Capture-the-Flag

### Custom Loaders and Architectures (1 Day)

This one-day module trains analysts to expand Binary Ninja's support for new file types and architectures. Students will also learn how to extend existing architecture plugins. At the end of the module, students will be able to reverse engineer an instruction set, and implement disassemblers, lifters, and loader plugins. Topics include:

- Extending Binary Ninja with new architectures
- Hooking existing architectures
- Custom loaders for new file formats
- Custom calling conventions
- Platforms and built in types

### Extending Binary Ninja with the C++ API (1 Day)

This one-day module demonstrates the differences between the different APIs and how to write effective Binary Ninja plugins in C++. At the end of the module, students will be able to develop standalone applications that interface with Binary Ninja's core. Topics include:

- Differences between the Python and C++ APIs
- C++ plugin best practices
- Linking binaries against the Binary Ninja Core module

Empower Your Analysts to do More. **Contact Us Today.**

Trail of Bits is an independent cyber security research and development consultancy trusted by many of the technology industry's biggest names. Our trainers' knowledge of the Binary Ninja API and internals is rivaled only by the Binary Ninja core developers.