IndexData:

SECURITY CONSULTING

Folio Test

West Coast Headquarters

123 Mission Street

Suite 900

San Francisco, CA 94105

415-293-0808

East Coast Headquarters

48 West 25th Street

Fourth Floor

New York, NY 10010

646-362-9666

For more Information Contact:

Name: Brett Arpaia

Email: Brett.Arpaia@nccgroup.com

Phone: +1 646-362-9613

nccgroup

Table of contents

Executive summary

Understanding your needs

We are the trusted security adviser to more than 1750 clients worldwide.

For IndexData, the security and integrity of your data and information systems is vital – a breach could have a major impact on both your Folio platform and your brand. You have therefore approached us to provide an independent program of penetration and security assessments, which will allow you to understand your vulnerabilities and risks and take action to address them.

You will be in very safe hands with NCC Group. Our team of penetration testing experts will deliver bespoke testing in line with your requirements and give you clear, actionable, recommendations for change. You can be confident that our testing methodologies and technologies are state of the art.world class.

Scope

IndexData has requested a proposal for a Penetration Test of the Folio Platform. NCC Group appreciates the opportunity to present a proposal to address IndexData's requirements.

NCC Group proposes a day assessment of the IndexData Folio Test to be performed against a development instance, which mimics the production codebase. NCC Group's plan for this engagement is to conduct a source code assisted penetration test, focusing on the following major areas:

- The Okapi WSPT
- Web-REST Web Services.
- Review of cryptographic implementation of secure storage and transmission of sensitive data.
- Review of multi-tenancy security concerns.
- REST API implemented in Folio that occupies Okapi endpoints.
- Authorization and authentication controls surrounding the different roles and sub-roles.

The time estimated for your program of penetration testing is based on the detail supplied here. If we discover areas that may require additional investigation while performing this test, we will inform you immediately. You will then be given the opportunity to confirm whether you require the scope of work to be expanded.

Whats in this proposal

This Proposal provides an overview of NCC Group, the services we provide and our proposed approach should you decide to proceed with the services set out in this proposal.

This document does not include, and does not constitute, the terms and conditions on which we will provide the services to you. Should you decide to proceed, we will provide you with our Master Services Agreement and technical Statement of Work for you to review, which set out the terms and conditions that will govern the services we provide. Please note that services cannot commence until the Master Services Agreement and SOW have been agreed and signed.

IndexData is one of the commercial partners in defining and devloping the open-source Folio project, which is building an OSS library-management system. They're nearing the point where they're going to have their first pilot deployment (in July 2019) and want to get some security assessment of the system.

The system is architected as a large number of Java-based microservices that are accessed thru a central API gateway called Okapi. Multitenancy is provided by Postgres; each tenant gets their own schema to keep them logically separated. IndexData provided a spreadsheet that lists all the repos they wanted to get security tested, which included 56 repos (about split in half between client-side and server-side code). However, on the call we discussed focusing on only the server-side code, and specifically the security critical code, which brought the count down to 9 repos (10, with dependencies). There is also a "Securing Okapi" page, which gives instructions on how to enable the access controls that only uses Okapi and 4 other modules.

You have questions

We have answers.

If you have any questions or would like to go ahead, simply get in touch with Brett Arpaia. We have provided contact details below.

We estimate that the project can be completed within one month of the start date.

We very much look forward to hearing from you.

Brett Arpaia

Brett.Arpaia@nccgroup.com

+1 646-362-9613

Our proposed approach

Overview

NCC Group has performed a multitude of application penetration tests and other associated security services. During the years of testing, NCC Group constantly improves the assessment process, making it as efficient and thorough as possible.

For the budget constraints the client provided (around $30k), I feel we can reasonably cover the "Securing Okapi" set of repos - they don't really have a test instance set up, so if we take 2d to spin up our own local copy of it all, that'd leave us 10d to test the web services of 94 APIs with ~ 38kloc Java code. We may need to spin up parts of their demo/reference UI to make it easier to use, but if so, those parts should be out of scope.

Technical dependencies and assumptions

NCC Group will require the following from IndexData, plus any additional items as agreed in the Statement of Work, in order to start on time with the minimum of disruption:

General:

- A technical point of contact who will be familiar with the environment being assessed and able to resolve or escalate any access or performance problems with it.
- All necessary change requests raised and approved for the nominated consultant(s) on the requested testing dates to enable access for testing.
- Confirmation that any third parties (such as hosting providers) have been made aware of and consent to testing.
- The full address of any site where on-site testing is to take place.
- NCC Group does not know where the equipment is physically located within the site or which access points it is possible to plug into to enable testing, so it is important for a technical contact to be available at site who:
    - Is aware of the environment.
    - Can inform us where the hardware is physically located.
    - Can inform us where connections can be made for testing, either side of the in-scope devices.
    - Can inform us the IP addresses of the in-scope devices.
    - Has an understanding of the project requirements.

Timescales

NCC Group operates a robust account management process by selecting the appropriate number of experienced and capable team members, commensurate with the demands of each project. The team is headed by a Tech Lead, a senior member of the group, who directs the project and would liaise with IndexData points of contact. The IndexData team can be supported by a Project Manager who schedules kick-off calls, status calls, and the final “readout call” to cover findings. This level of project management detail ensures NCC Group delivers a thorough assessment that continues a tradition of excellent results for our clients.

Key elements of Assignment Management Process

You will be assigned an account manager, who will be Brett Arpaia. Brett is your first point of call in arranging for project initiation and matters of a commercial nature. It is Bretts’ responsibility to ensure that the relationship between our two organizations is successful and that you are comfortable with the standard of work that is being delivered.

Key elements of Team Structure and Roles

You will be assigned a Lead Consultant who will conduct initial aspects of the project and direct the delivery team. All assignments are initiated through a formal project initiation exercise conducted with you by the Lead Consultant. They will be responsible for successfully managing and controlling your project. They will identify, track, and manage any project issues and proactively disseminate project information to all the stakeholders. They will be accountable for the overall schedule of testing, and responsible for ensuring that your project is assigned and completed to the expected standard and to the agreed timescales. All work is subject to our internal peer-review processes and quality assurance before being released.

We are committed to delivering a high quality service to you, but in the unlikely event of an issue arising there are formal escalation procedures to help you quickly bring your issue to closure. Post-assignment reviews are carried out and the results are monitored by the senior management.

Pricing, schedule, and logistics

Component	Days	Cost
Web Application Penetration Test	12 person days	$30,000
Project Management	2	$2,400
OPTIONAL: Retesting	$2,500/day	TBD
Client Facing Document	Letter Of Engagement	Included
	Total	$32,400

Professional fees

NCC Group proposes to offer these services on a fixed time/fixed price contract. NCC Group will provide full time senior technical consultants for 12 person days for the application penetration test. The consultants will be working full-time days (9am to 5pm local hours) on an off-site basis over the duration of the engagement. If more time is required, or additional resources are requested, the identified team may be staffed at the same rate. Any additional resources will first be requested and approved by the IndexData team.

Implementation/set-up costs

There are no anticipated implementation/set-up costs for this project.

Expenses / other fees

If travel is required, NCC Group will require reimbursement for reasonable travel expenses, and will discuss this with you so that all expenses are incurred and process in accordance with the agreed Master Services Agreement and Statement of Work

Protection of IndexData's information

NCC Group will conduct all initial discussions and scoping exercises under NDA if required, however the Master Services Agreement contains extensive confidentiality obligations to ensure that your confidential information remains safe and secure. All confidential information provided by IndexData will be returned or destroyed upon conclusion of the engagement.

NCC Group anticipates having access to the following information:

- Documentation, descriptions, specifications, source code and questions/answers about architecture.

- Optional VPN credentials to access the test environment.

Where storage of sensitive electronic information is required, that information will be placed on a logically segmented partition, with:

- Cryptographic authentication required

- Access to that server provided only to team members authorized to work on the project

- No direct access will be provided from that server to the public Internet

- Protected information and information derived from protected information will be encrypted where requested

- Paper copies (including deliverables, meeting notes, or emails) will either be destroyed or stored in a safe

- PGP keys for each team member will be provided to the team for secure email communication

Background Information

Corporate overview

NCC Group will help IndexData to prepare the Folio platform for a global deployment.

NCC Group is a global information assurance specialist providing organizations worldwide with expert escrow, verification, security consulting, website performance, software testing and domain services.

Through an unrivalled range of services, we provide organizations across the world with freedom from doubt that their most important assets are protected and operating as they should be at all times.

As the cyber arms race and technology revolution continue to outpace the ability of organizations to cope with the plethora of security, performance and availability issues, we are best placed to help organizations to manage the risk and limit the threat.

With our knowledge, experience, capability and global footprint we are committed to ensuring that organizations have access to a total information assurance solution that works for them.

Our complementary service areas provide comprehensive end-to-end information assurance for over 15,000 organizations worldwide. We have 30 locations across the UK, Europe, North America and Australia.

We are passionate about changing the shape of the Internet and making it safer.

NCC Group's North American Security Consulting division was created by uniting many of the best security consultancies, including iSEC Partners, Intrepidus Group, Matasano, NCC Group and NGS.

A combination of our people, client base and resources across the Group's Security Consulting businesses has enabled the establishment of a large team of consultants distributed across offices all over the US in San Francisco, New York, Chicago, Austin, Seattle, Sunnyvale and Atlanta.

Utilizing our specialized application, mobile and network security teams we work with major retail, technology and financial services companies across the globe.

Our security assessments leverage our extensive knowledge of current security vulnerabilities, penetration techniques and software development best practices to enable customers to secure their applications against ever-present threats on the Internet.

Our global research team has a long track record of world-class success and our combined vulnerability advisories; whitepapers and tools help us to find solutions to the challenges you are facing right now.

The technical depth in our teams added to the scale of operation that we now have has made us the ideal security partner for clients across the world.

Our security consultants are published authors in the information security field and regular speakers at major industry events, including Black Hat USA and Europe, DEFCON, Hack in the Box, OWASP Appsec USA, Re:Invent, RECon, RSA, Shmoocon, SOURCE, Toorcon, Amazon's ZonCon and Microsoft's BlueHat Security Briefings.

Practice focus areas

- **Application & Infrastructure Security** – NCC Group Application Security Consultants are experts at understanding how things work, and breaking them. We have spent years building and refining processes for assessing solutions, including everything from high level as object-oriented web applications, to low-level assembly based microcontrollers, to complicated multi-tenant systems that span the full stack. For each assessment type, we have developed general methodology on how one would assess that technology vertical. Each vertical as different technology or framework focuses, in turn we have developed specific methodologies for each of these as well.

- **Forensics & Incident Response** - NCC Group's unique end-to-end Cyber Resilience and Incident Response services range from executive engagement and strategy development through to education, incident management, remediation and verification. Our team can provide the full lifecycle of services you will need to prevent and recover from attacks. These services can be delivered either as a program of work or as discrete projects; ranging from traditional host based forensics to investigate areas such as acceptable use breeches through to full incident response management utilizing facets from the NCC Group CDO product suite for Network Forensics, host investigation using certified products and advanced Malware Reverse Engineering

- **Cryptography Services** – We have built and refined a methodology for assessing and exploiting cryptographic weaknesses, including block ciphers, stream ciphers, key negotiation, number theoretic crypto, hashes, and message authentication. We've presented research on breaking cryptography at Black Hat and numerous other venues. We excel at breaking down and understanding complex crypto systems and can help guide intelligent choices to build resilient systems.

- **Risk Management &Governance** - Our experienced & fully qualified Information Risk Management and Governance team will assist you in reaching and maintaining compliance to standards & regulations such as ISO 27001, PCI-DSS, PA-DSS, PCI P2PE, HIPAA, and NIST 800-53 to ensure that you are in line with best practice frameworks. NCC Group is a PCI QSA company and ASV, and our consultants hold multiple industry certifications and have deep backgrounds in information assurance, audit, compliance, and governance. We deliver our services using a systematic and strategic approach, to cover the many facets of organizational risk and control (both internal and external); an essential process in the modern compliance landscape.

- **Managed Security Services** - We manage the external and internal security testing/scanning programs for many hundreds of clients. In order to provide the most comprehensive services possible we use the most advanced scanning tools available on the market to ensure that we provide a market leading technological approach for our customers. NCC Group's Managed Services team works closely with customers to tailor a combination of Internal and External scanning / testing options. Our goal is to provide continuous security testing/scanning throughout the year from a dedicated Managed Services team to provide an efficient, clear, unified view of your infrastructure and application security footprint. We take all of the results from the tools we use and also from NCC Pen tests and provide these through an easy to use Web Based Portal so that you and your team can review the results.

- **Research** – NCC Group has a long-standing heritage of performing independent research for both commercial and Government organizations. With a long track record of research success for clients in all sectors, our vulnerability advisories, white papers, tools and knowledge-share presentations help us respond to the challenges you face in a rapidly-changing, technologically-driven market. They also enable us to develop our existing suite of software products, and to make further innovations as your preferences change. Being fortunate to have world-class researchers has enabled us to discover more high-risk security vulnerabilities in enterprise software than any other security organization.

- **Bug Bounty Support Program** - In response to popular demand, NCC Group is pleased to present this program working in conjunction with leading bug bounty providers. Harnessing the power of the global security community, these programs allow you to locate critical vulnerabilities and fix them before criminals can exploit them. Our experience as technical leaders in the information security field, and with bug bounty programs in particular, positions NCC Group perfectly to handle all of your bug bounty needs.

Our Strengths

We have a reputation for professional expertise and conduct that is unparalleled anywhere in the world. Our team of expert penetration testers provide sound advice and practical assistance to multi-national corporations and strategic intelligence services to government agencies around the globe. Clients that partner with us undoubtedly experience the difference.

- **Accurate vulnerability identification, classification, and analysis** - leveraging thorough methodologies and using elite penetration testing teams enables us to provide our clients with accurate vulnerability identification and classification, allowing information security risk to be quantified, adequate expenditure assigned, and appropriate action taken. Our deep technical skills and solid business acumen allow us to analyze vulnerabilities with an eye to effective remediation of risk, reduction of risk, or acceptance of risk, based on a customer's needs. NCC Group truly consults with our customers, providing valued next steps, rather than cookie-cutter recommendations.

- **Mitigated security risk** - our penetration tests are delivered as hands-on assignments, not simply as automated scanning exercises. The techniques and methods we use are cutting-edge and best practice; they match and often exceed those employed by hackers or suggested

by industry respected groups, such as OWASP, NIST, etc. Our techniques and methodologies ensure a deep-dive, repeatable approach that protects against false positives, a common issue from scanning-only vendors.

- **Sound, impartial remediation advice** - as we are independent, if we make a recommendation, our clients can be assured that it is because it is appropriate, not because we profit by doing so.

- **Thorough accessible reporting** - we take great pride in understanding our clients and reporting in a manner that is appropriate to their different needs. Our reports are clearly communicated, in a manner that is readily accessible for management and technical levels.

- **Scalable and responsive delivery** - as the largest penetration testing supplier in the world, we have the capacity to deliver small- and large-scale projects and to respond to our clients' challenging timescales.

- **Knowledge share** - whether through our formal courses or one-to-one on-the-job training sessions, a successful engagement always involves knowledge share with our clients.

- **World centers of excellence** - our penetration testing teams have been drawn from the world's foremost information security organizations; all are dedicated, seasoned professionals with many years of sustained practice in their expert fields of knowledge. Many of our testers come from strong commercial development and academic backgrounds. Our experience ensures a level of professional service that constantly meets the exacting demands of our clients.

- **Long-term client partnerships** - we believe in building long-term relationships with our clients, and everything we do is to that end. Over the years we have developed long-term relationships with clients from some of the world's largest corporations and public sector organizations. Our clients are always confident in our ability to bring the experience, knowledge of appropriate technologies, and best practice methodologies to meet all their requirements.

- **Cyber protection against targeted attacks** - We can provide a full end-to-end service, from analyzing and reverse-engineering malware to end-user awareness training, from digitally sound evidence collection to strategy advice on preventing data loss. Our team can provide every service you need to prevent and recover from attacks.

Appendices supporting this proposal

Quality control

NCC Group is a global information assurance specialist providing organisations worldwide with expert escrow and verification, security consulting, web performance and domain services. We are committed to the profitable provision of services that anticipate and meet our customers' requirements and deliver excellent returns to our shareholders.

Achieving a high level of customer satisfaction is the target for all work. Profitability targets are set for each area of our business each month in an annual plan. Our overall effectiveness is measured by how well we perform against this plan.

This policy is supported by detailed measurable objectives in the form of Key Performance Indicators at all levels in the organisation structure. Performance targets are reviewed on a regular basis by management to ensure quality standards are constantly met and improved.

NCC Group operates a quality system of standards and procedures, which manages and controls all our projects, products and service activities. The quality management system is based on the requirements of ISO 9001:2008, and is subject to continual improvement through our management review process.

The implementation of this policy is mandatory and is to be observed by all those who contribute to NCC Group's products and services.

Adam Palser

Chief Executive Officer

December 2018