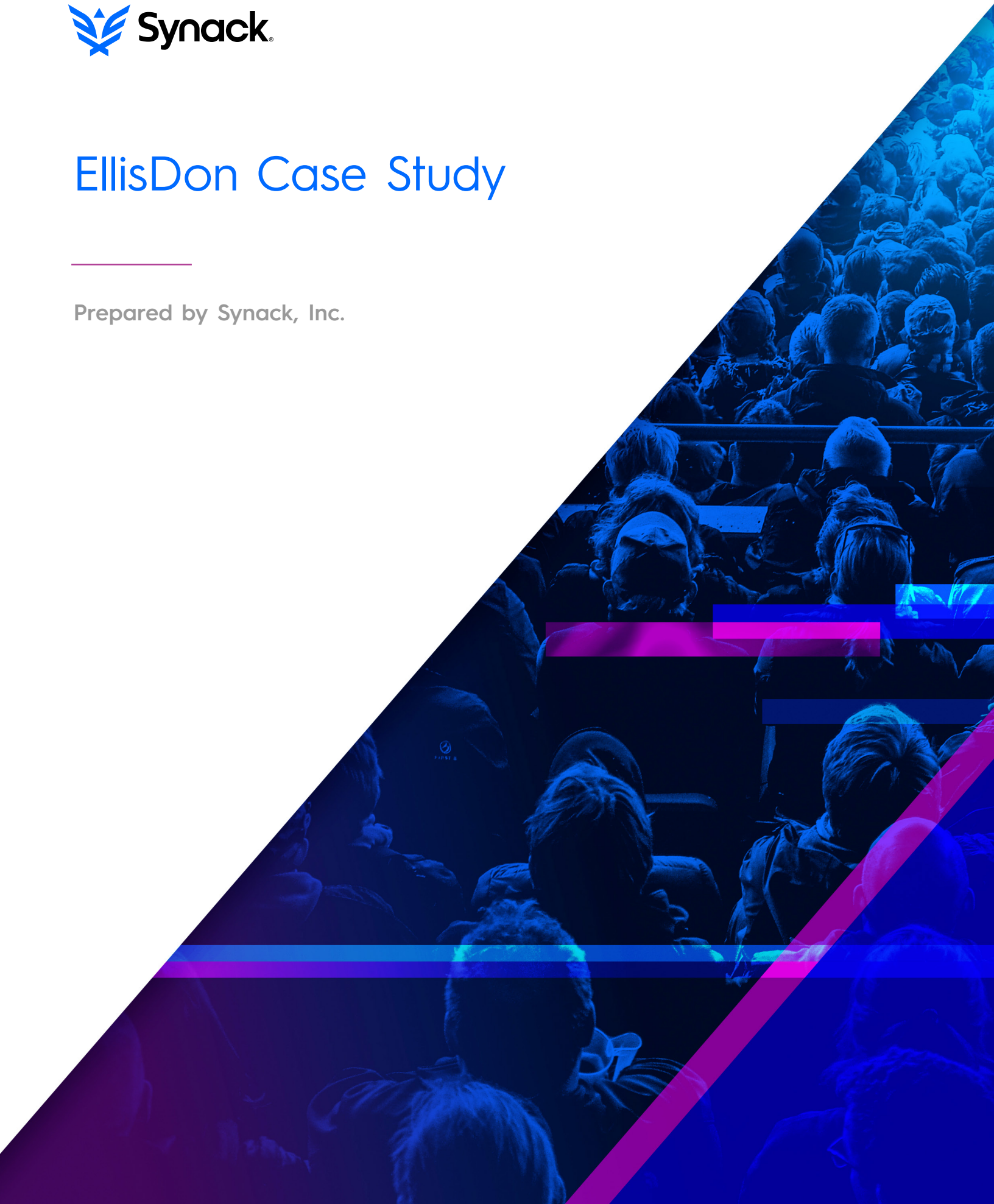
Synack

EllisDon Case Study

Prepared by Synack, Inc.



Synack EllisDon Case Study

> "EllisDon utilizes leading technology and leverages data to create a sustainable competitive advantage. That needs to be protected. Synack not only uncovers our unknown vulnerabilities, but they also provide us with valuable security data that tells us more about our security posture and how it changes over time."
>
> —Gary Smith, VP Enterprise Tech Relations

Canada's greatest hockey legend—Wayne Gretzky—said that he always skated to where the puck was going to be, not where it was. The same strategy describes Synack client EllisDon and its Gate Three construction ERP software.

Since 1951, EllisDon has grown into one of the largest general contractors in Canada. With thousands of projects delivered on four continents—80% from repeat customers—there was no doubt EllisDon could have been a successful builder for decades to come. However, long-time President and CEO saw a path to even greater rewards with a manageable risk.

That path to the puck's location was Gate Three.

The Target: Gate Three

First conceived in 2010, Gate Three is the culmination of decades of lessons learned from creating the most demanding construction projects in the world. First among those lessons was that construction was becoming a data-driven industry. Each party—from financiers to subcontractors—benefited from clear, consistent information around a building project. So EllisDon decided to build their end-to-end knowledge of construction processes into new software that would help streamline the entire construction process.

Gate Three is built on trust across every party in a building project. Starting with the site supervisor who transitioned from clipboards and verbal commands to logging key activities digitally, each party reports real-time on the status of everything from a concrete pour to a subcontractor calling in sick. This information is logged in Gate Three, and nothing but the most demanding security tests were needed to protect this data.

Gate Three was a hardened application before being tested by Synack. EllisDon's in-house software development team was sensitive to security issues during development and had over a dozen software tools used to help develop secure software, including static analysis, scanning tools, and WhiteSource (a common open source security manager to help root out known vulnerabilities).

Sample Vulnerabilities Discovered and Closed during Synack engagement:

- Sitewide Stored XSS affecting Rich Text Fields
- Bypassing file upload functionality... via .exe file
- Java object deserialization
- Unauthenticated root-privileged RCE*

Indicates third-party product

EllisDon, a world-leading Canadian Construction and Building Services company, is responsible for over 3.5 billion (CAD) of annual construction projects. EllisDon's corporate culture and approach to business is a reflection of its core values and principles: freedom, trust, complete openness, mutual accountability, entrepreneurial enthusiasm, integrity and mutual respect. These values provide their employees with the courage to express and apply their innovations and expertise, allowing their clients to work with EllisDon in an open, transparent way, as EllisDon expands beyond the boundary of what it means to be a construction company.

Their aim is to develop creative solutions for complex problems. From their first project in 1951—a modest home renovation—EllisDon has become Canada's premier construction services company offering "cradle to grave" services to deliver customers a full suite of construction and building services.

The Goal: Better Security Before an Incident, Not After

EllisDon wanted to be very proactive about finding potential security holes before attackers crossed mid-ice. They knew adversarial threats were present, so EllisDon turned to Synack to bring the latest attacker thinking to their security testing.

EllisDon uses leading technology and leverages its data to create a sustainable competitive advantage. Gate Three was symbolic of EllisDon's new growth into digital businesses, and much of EllisDon's digital aspirations rode upon Gate Three being successful and secure.

Working with Synack

EllisDon started with a Synack test engagement. Right out of the gate, they were impressed by Synack's adversarial approach through the use of a crowd of highly talented, trusted hackers, and the analytics available for review in the client portal. EllisDon decided to buy an additional Synack Crowdsourced Vulnerability Discovery subscription.

Example Vulnerability + Impact

> One vulnerability found by Synack alerted EllisDon's Security Team that the company was actively using a legacy version of a CRM application with several vulnerabilities present. The Security Team brought the Synack vulnerability report to the application's key stakeholders and raised concern for their current security risk. Ultimately, it helped EllisDon switch to a different platform and set a precedent to drive internal decisions with consideration for security risk.

Results

With Synack, all the action on the ice was visible at once. All of the rules of engagement, payments and security research prep was handled by Synack; EllisDon only spent a handful of person-hours between contract signing and the first recon from Synack's Hydra software. The Synack platform allowed EllisDon to keep track of their data and view their domains as an attacker would see it. At any moment, EllisDon could see the number of researchers engaged, testing coverage maps, attack attempts, etc on their assets in scope.

EllisDon fixed their vulnerabilities, but that was just one benefit.

With Synack, EllisDon was able to specify assets in scope, evaluate the severity of vulnerabilities found, and prioritize the implementation of remediation efforts. For later tests, EllisDon will be able to compare specific assets' resistance to attack over time and track their improvements using Synack Attacker Resistance Score. "Synack's data-driven and controlled approach to testing helped make our software and processes at EllisDon more secure," Smith added.

The Synack engagement gave EllisDon a better feel for their software development and security processes. For example, EllisDon strengthened the quality gate in their continuous integration (CI) process and added Sonar open source code quality platform to enhance developer security awareness. The Enterprise Intelligence group at EllisDon was open and communicative about vulnerabilities, greatly enhancing collaboration between software developers and security team members.

EllisDon truly feels that, with Synack on their team, they are skating towards where the puck is going to be, and are on the path to reducing security risks.

>600 researcher hours

~75 individual, vetted researchers

16 vulnerabilities discovered

6.6 average CVSS across valid vulnerabilities reported

6 high severity vulnerabilities found and remediated

2 third-party vendors with uncovered vulnerabilities

Synack, Inc.

855.796.2251 | www.synack.com | info@synack.com

v2018.1—INT US