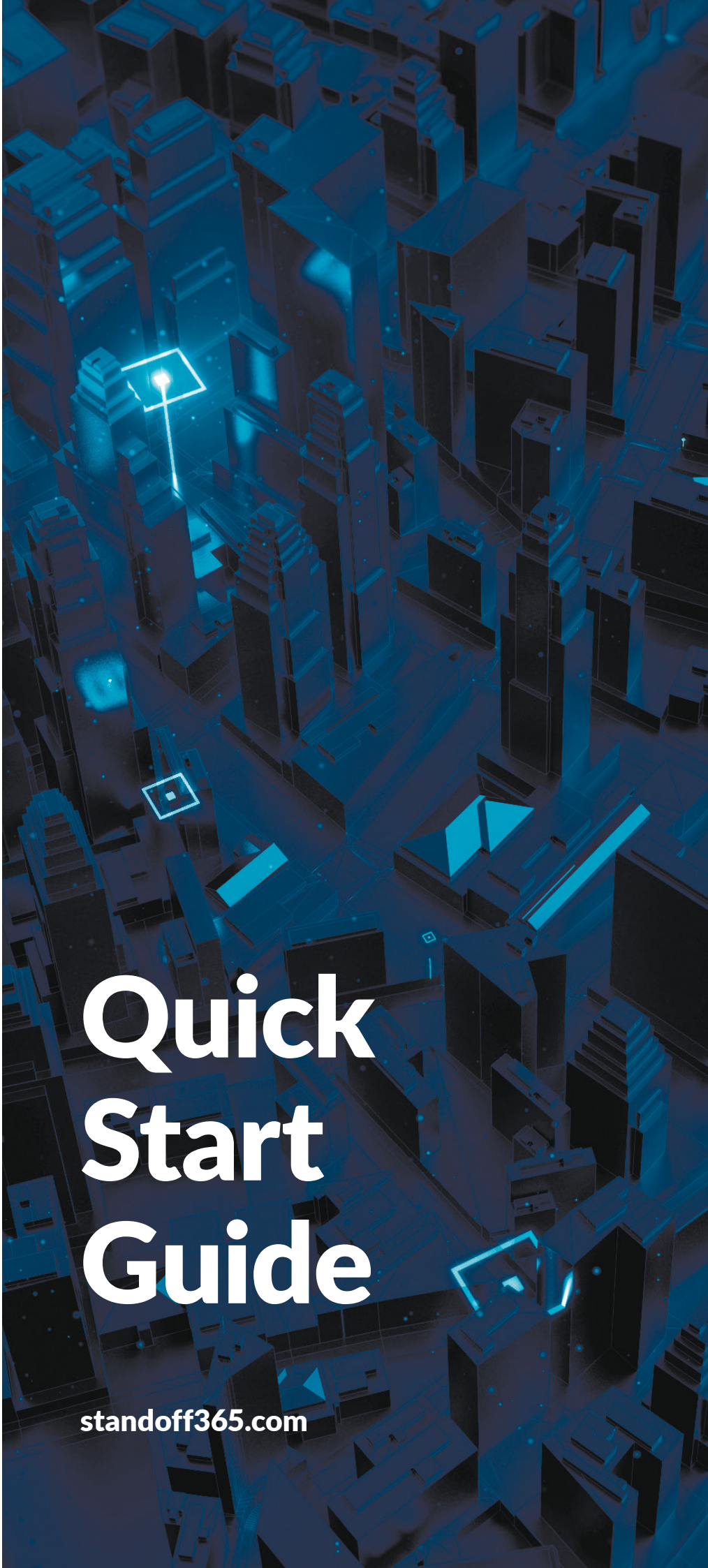
THE STANDOFF



Quick Start Guide

standoff365.com

THE STANDOFF

Meet The Standoff

The Standoff is a cyber-range platform created by IT and information security experts committed to advancing the development of a truly secure IT infrastructure.

At The Standoff, top-tier offensive and defensive security specialists battle each other in a mock digital city. The cyber-range contains full-fidelity replicas of the production chains, business scenarios, and technology landscape typical of different industries.

Companies and security professionals alike benefit from participating in The Standoff by empirically testing the feasibility of cyberattacks in a safe environment, gaining knowledge and hands-on skills to detect and counter threats, gaming out response scenarios, and seeing first-hand the close relationship between cybersecurity and business.

What Is Hapenning Here in Just 100 Words

- The cyberbattle unfolds in a city with lots of businesses that mimic real companies of various kinds
- Attackers try to damage those businesses by attacking the infrastructure and causing impacts which real companies might face in the real world
- Defenders try to stop or at least locate hackers until it's too late
- Real industrial control systems withstand wide variety of advanced attacks
- New attack vectors and techniques on ICS and SCADA are discovered
- The Standoff promotes new security paradigm that cybersecurity systems should have KPIs connected to business
- Besides pursuing key goals, both sides—attackers and defenders are enjoying a gaming atmosphere and frankly speaking.....just having fun!

Plot

City F is a digital twin of a modern agglomeration where people work and live. The city features business districts, amusement park with a big ferry, transportation (cargo and passenger), energy extraction and distribution, smart city systems, finance, telecom, and more. Every object in the city has its own IT systems which use the exactly the same web applications, software, hardware, PLCs and SCADA as their counterparts in the real life. Those systems are connected into a sophisticated ecosystem which is protected by the blue teams and, well, attacked by red.

The cyber battle itself is also much closer to what we see in the news every day. Unlike traditional red vs blue competitions where red teams are directed to bring exact predefined flags, 'hacker teams' at The Standoff need not only to break into IT systems but also to trigger some risks which put victims' business in danger or even provoke a catastrophe.

Various companies of the City F carry their own list of risks, every risk comes as its own complexity and price and the hackers are free to choose which company and which risks they are going for. Those changes give attackers more freedom but also requires to demonstrate much more effort and field expertise especially when they are dealing with SCADA systems.

Blue teams or Security Operation Centers monitor and protect most of the City F infrastructure with their goal set to timely identify and prevent attempts to trigger risks for the protected companies. Like in the real world they also need to ensure no business process is interrupted due to overreacting security measures.

Both attackers and defenders work non-stop from 8 am GMT November 12 until 11 am GMT November 17.

How IT Security Risks affect the business

Most of the adversaries today do not break into companies' networks out of pure interest and boredom. Whether they steal confidential information, mount a potent DDoS or encrypt internal systems with ransomware, their usual goal is money. Hacking groups purchase zero-days on special markets, pay analysts for crafting spearphishing emails and calculate the economic outcome of their "investments" before they start a campaign. They know exactly where they want to be, have a clear goal in mind and operate under a certain budget to achieve it.

On the contrary, their potential victims often choose different approach to defend. Given absence of any information on expertise of potential attackers or expected attack vectors, companies tend to invest intosecurity technologies perceived as the most usefuland then use all highly diversified portfolio to their best knowledge, aiming to block all attacks at a perimeter. However, such approach brings in a lot of questions from budget holders such as:

- We already invested a significant sum on cybersecurity. Is the business really safe now?
- We increased our security budget for another million last year, wasn`t that enough?
- What is the return on our investment in cybersecurity?

In order to answer these questions, an implemented cybersecurity approach should be changed taking into consideration below assumptions:

- Some of the risks to the business can be triggered by exploiting IT systems in various ways
- These risks can be triggered only when attackers gain control over some systems and keep it for a certain amount of time
- The goal of a cybersecurity system is to make a successful attempt to trigger risks intolerable by business more expensive than hackers will like to invest in it.

Practically, this means that a new paradigm of designing cybersecurity systems should come in place. This paradigm is built on these cornerstones:

1. Risks should be clearly identified and ranked by criticality
2. Ways to trigger these risks via IT should be thoroughly assessed and recorded for every system including how much time attackers need to trigger the risk
3. Security teams should spend an effort to build monitoring centers capable of timely detecting and containing incidents aimed at triggering security risks
4. Any preventive technology should be regarded as a cost multiplier for attackers, not as a silver bullet
5. Existing cybersecurity system should on a regular basis undergo a stress test mimicking adversaries' actions as close to real as possible

Cybersecurity system built on these principles simply made hackers' endeavor financially not feasible, which will turn them away for a search of an easier target.

Promoting risk-based approach to cybersecurity is a core belief behind The Standoff platform and the cyberbattle. Thus, The Standoff red teams are not just asked to bring a particular system down, they aim to trigger certain events and thus disrupt the business of a target company. This new paradigm of architecting cybersecurity will not only make cybersecurity more efficient from business standpoint but will also make security spending much more transparent and predictable.

Companies and Risks

"FA" Airport and the "F-ly" aviation company

Major Risks:

- Disruption of passenger boarding and deboarding via a jet bridge
- Malfunction of internal passenger registration systems and logistical management systems
- Disruption in automated conveyance of passenger baggage

HSL Sea Port

Located on the coast near the city. Headquarters of the Heavy Ship Logistics sea carrier.

Major Risks:

- Disruption of a gantry crane operation
- Exposing data on shipping container transportation and freight charges

Railway

City F is a major railway hub with long-distance passenger and cargo transportation established. Everything is controlled by a distributed smart information systems. All railway switches, traffic lights and barriers at crossings are fully automated.

Major Risks:

- Breach of railway control systems
- Halt of railway control systems

Bank of FF

The country's largest bank in assets and market capitalization also comes from city F. In 2020, Bank of FF is ranked 7th in the world by assets and 52nd most valuable brands.

Major Risks:

- Fraudulent card transactions
- Theft of funds from bank accounts
- Distribution or leak of client personal information

City

F has a large business district. All office buildings feature centralized automated heating and air conditioning system, which maintains comfortable conditions inside the building.

Major Risks:

Disruption of building HVAC systems

Traffic lights and street Lighting

Major Risks:

- Disruption of city traffic lights: all go green or all go red
- Disruption in operation of street lighting systems – city goes dark

Amusement Park

Major Risks:

- Deactivation of Ferris wheel control system
- Disruption of online ticket sales

Major risks to other businesses presented at The Standoff 2020:

Television and radio broadcasting system

- Broadcasting of unauthorized content on video billboards

Oil extraction

- Halt of oil extraction processes
- Halt of petroleum product transportation to oil terminals

Power plants

- Halt of power production processes via fire control system
- Suspension of power production by wind turbine converters

Electrical substation

- Disruption in delivery of electricity to consumers

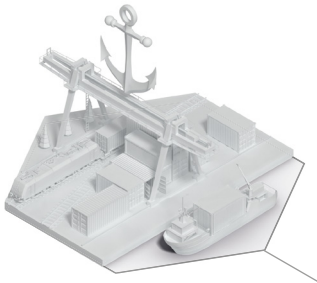
Gas distribution station

- Suspension of gas delivery to consumers
- Halt of gas transportation processes

Petrochemical plant

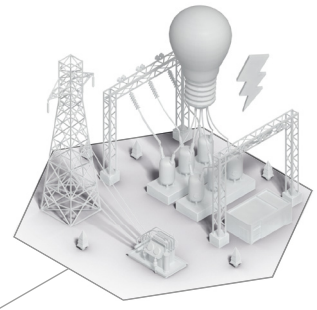
- Halt of petrochemical production processes
- Accident

How network works



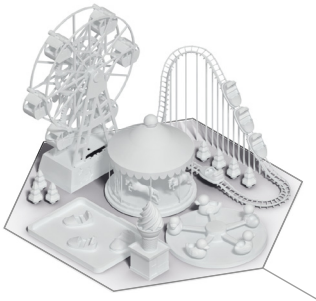
Blue Team 1

- FA Airport
- Heavy Ships Logistics SeaPort
- Railway
- Business center



Blue Team 5

- Power Plants
- Wind Power Turbine
- Business Center

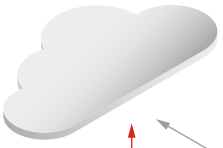


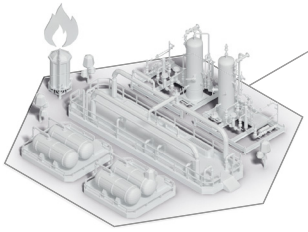
Blue Team 2

- City
- Traffic Lights
- Amusement Park
- Business Center

Blue Team 6

- Oil Extraction
- Petrochemical Plant
- Business Center



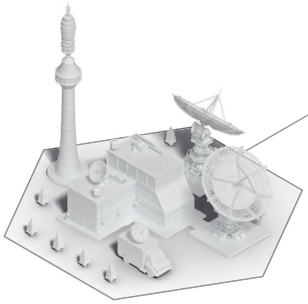


Blue Team 3

- Gas distribution station
- Electrical Substation
- City Lighting
- Business Center

Blue Team 7

- Bank



Blue Team 4

- TV Broadcasting

Hackers

Digital Map of the City F

Numbers and Facts

The Standoff 2020 will last for 123 hours, from 8 am GMT November 12 until 11 am GMT November 17.

The competition is held fully online, red and blue teams connect to the platform from various places across the globe.

29 red and 6 blue teams participate in The Standoff 2020.

13 companies of the City Fare facing security challenges this year: Airport, Seaport, Railway, Business District, Bank, Amusement Park, City Hall systems (traffic lights and street lighting), TV and radio broadcasting system, Oil extraction, Electrical sub-station, Natural Gas distribution station, Thermal power plant, Petrochemical plant.

Security Software from more than 10 worldwide known vendors is used by the blue teams. This includes IBM, Microsoft, Micro Focus, CheckPoint, Kaspersky, Positive Technologies and others.

Industrial IT systems are built on PLCs from Siemens, Schneider Electric, Yokogawa, Phoenix Contact, Allen-Bradley, Bachmann, Mitsubishi Electric, B&R, Emerson, Beckhoff.

Next Steps

Regardless of a role and job title of participants, the Standoff have united IT and cybersecurity enthusiasts around the world under one goal—gain and share unique knowledge on advancing cybersecurity approaches.

On November 17th 1:00pm GMT the grand finale and announcement of winners at The Standoff is rather a comma, not a stop.

All incidents happened during the cyberbattle will be meticulously analyzed and an essence will be presented publicly within several months in different formats.

Join us for upcoming follow-up virtual events!

THE STANDOFF