RSAC Sandbox

RSAConference2020

HUMAN ELEMENT

SESSION ID: **SBX1-W6**

ICS OSINT: An Attacker's Perspective

Selena Larson

Intelligence Analyst
Dragos | Threat Intelligence
@selenalarson

Amy Bejtlich

Director of Intelligence Analysis
Dragos | Threat Intelligence
@_Silent_J

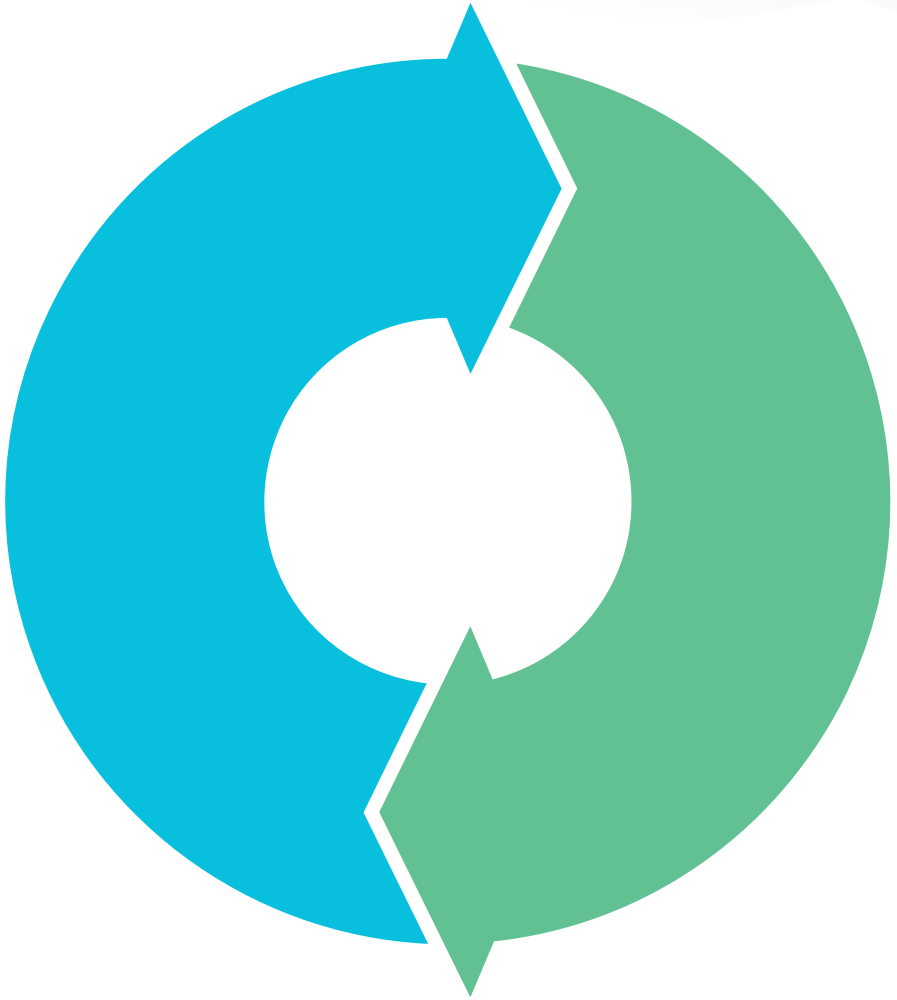
Goals

1. Provide an OSINT primer
2. Raise awareness
3. Understand the adversary
4. Recommend mitigations

What is OSINT?

OSINT

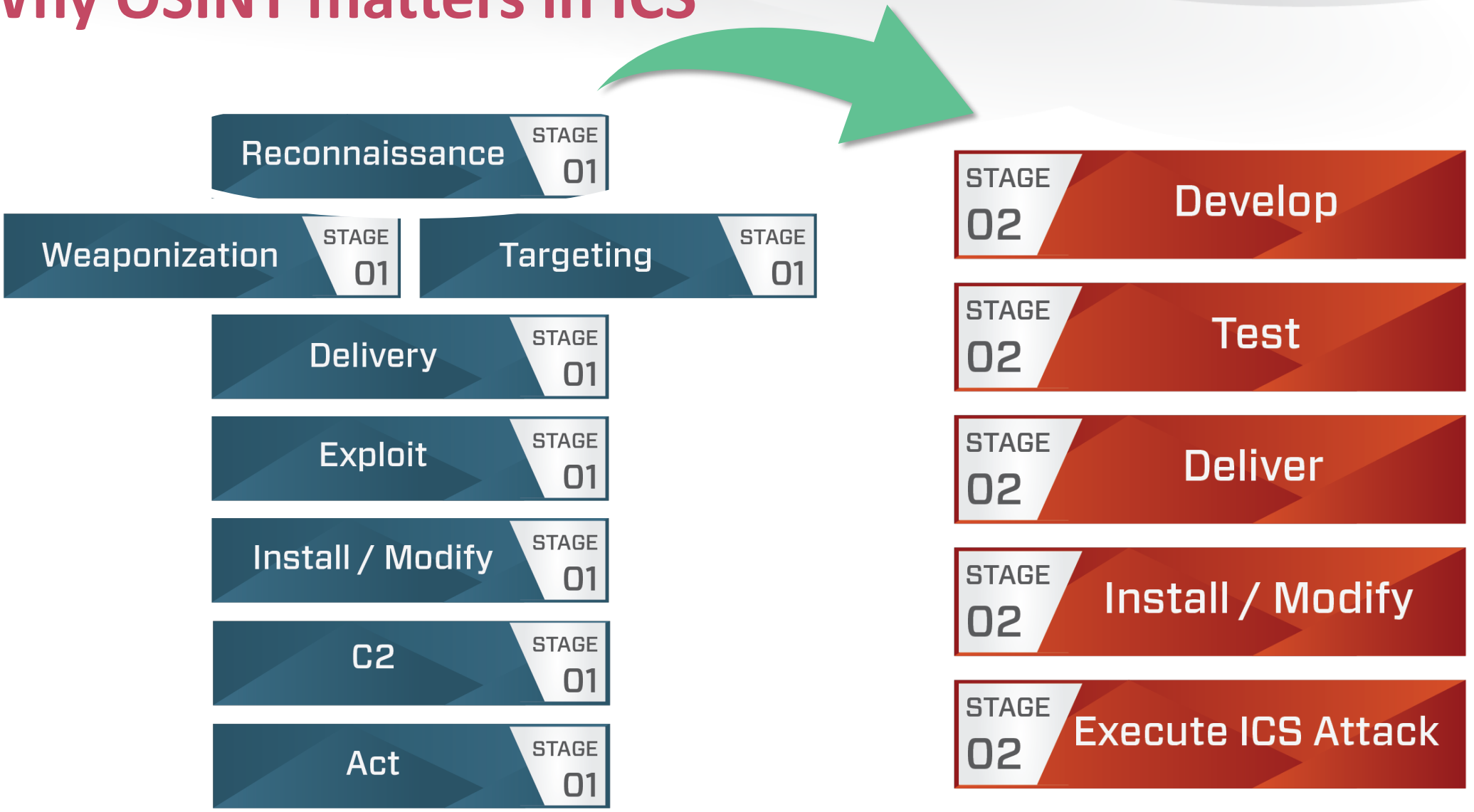
- Legally collected
- Publicly available
- Informs investigations, reporting, attacks, or defense



OPSEC

- Means & methods to deny adversary info
- Discover could lead to failure or compromise

Why OSINT matters in ICS

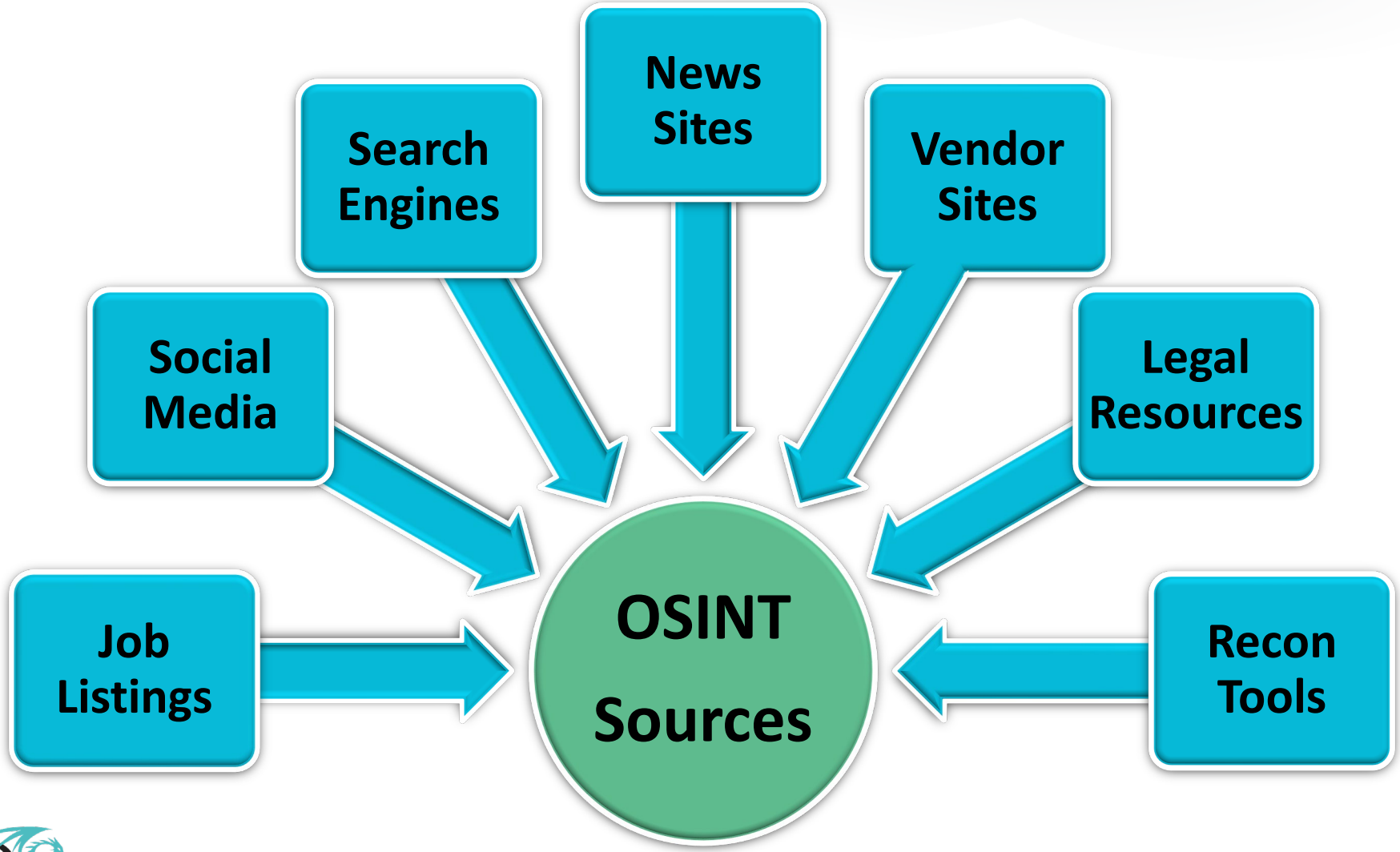


OSINT characteristics

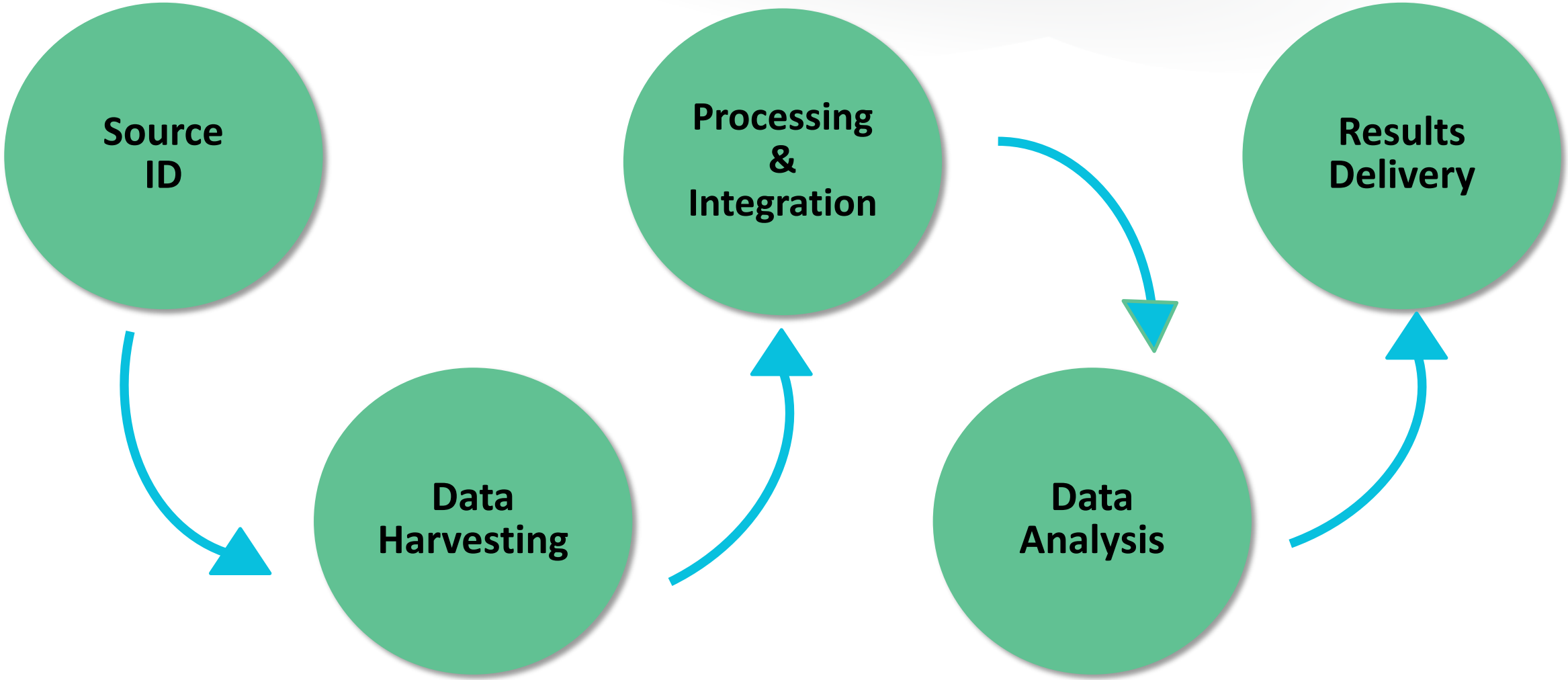
Applications
Offense vs. Defense

Methods
Active vs. Passive

OSINT sources



The OSINT process



Key Terms

- Personal/Personnel Information
  - Allows for identification of critical personnel, general personnel, or outside source personnel (e.g. contractors, third party operators)
- Criticality Information
  - Informs an adversary of the impact of an attack for a target's continued operations. A target's criticality is determined if its compromise or destruction has a highly significant impact in the overall organization and it's ability to conduct business or operations.
- Accessibility Information
  - Informs the adversary of the ability or method to remotely/physically access or egress from a target.

Key Terms

- Recoverability Information
  - Gives an adversary insight into the ability for a target's process, system, or network infrastructure to recover from an attack or compromise.
- Vulnerability Information
  - Informs an adversary of a vulnerability that exists in target's infrastructure, processes, or response actions.
- Effect Information
  - Information about the amount of direct or indirect loss a target would have from an attack or compromise. Also information on the effects losses would have on the target, it's organization, processes, or operations.
- Recognizability Information
  - Assists adversaries in the ease of identifying targets for operational gain and the level of obscurity that the target has from both internal and external sources.

Why target ICS?

RSAC Sandbox

- Value
  - Strategic: Attacks on ICS entities like oil and gas or electric utilities can be used to further political, economic, and national security goals. Understanding critical infrastructure can put an adversary at a tactical advantage.
  - Monetary: Companies willing to pay ransoms to limit downtime.
- Ease
  - Legacy operating systems in use across various environments.
  - Limitations on patch management and insufficient external mitigations.
  - Default passwords
    - Example: During a pentest, a colleague identified a default password on a device that the operator did not know about following an outage + replacement.

Dragos case study

How a Dragos sales rep socially engineered a vendor

Example: SEC 10-K

RSAC Sandbox

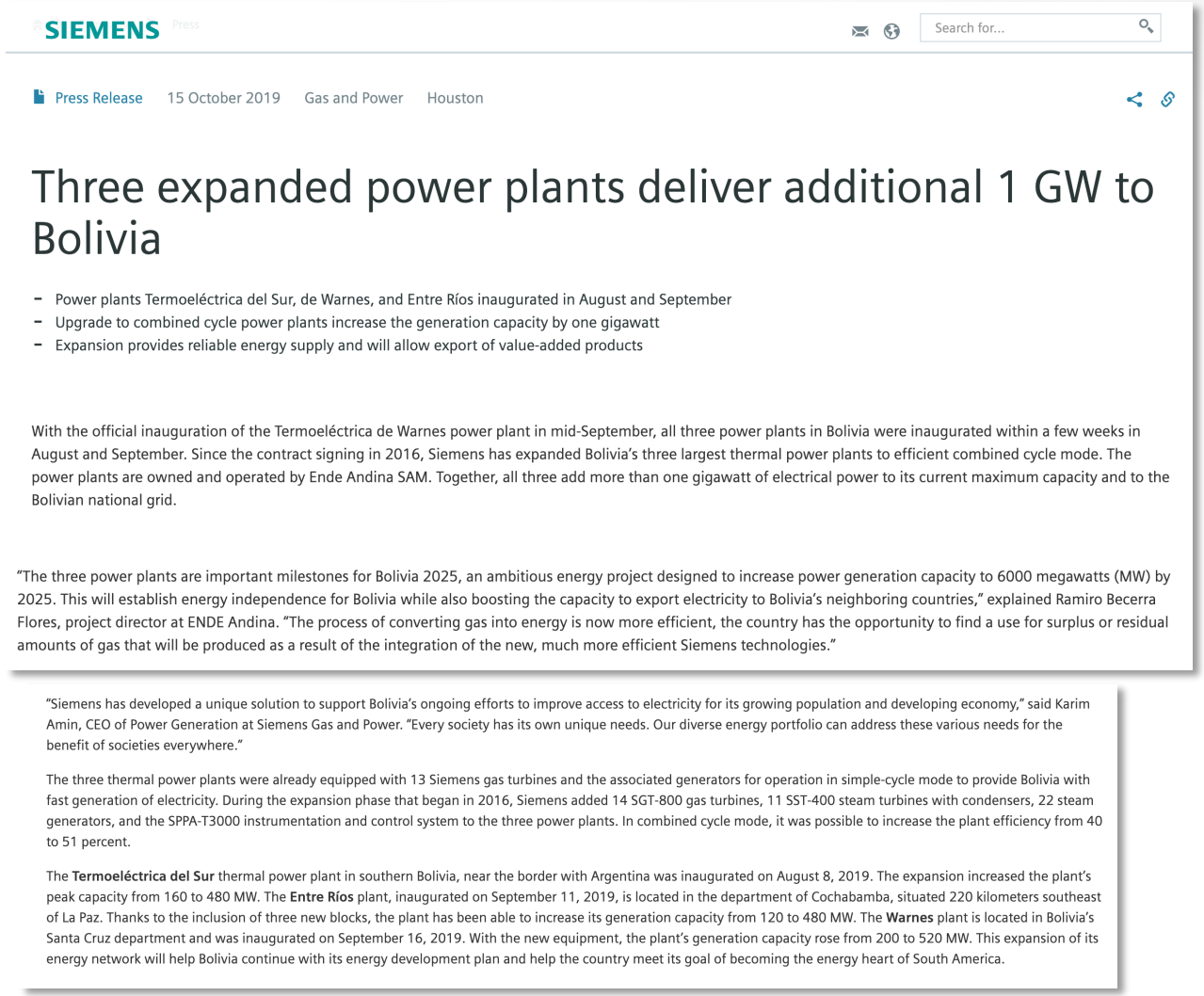
- EDGAR: US SEC information repository for publicly traded companies (e.g. 10-K)
  - Financial information, key personnel, names/addresses of major common stock holders, summary of legal proceedings, etc.
- Manufacturer of health and security devices
  - Legal proceedings, M&A, updates to enterprise resource planning system, governments/agencies, name of accounting company that submitted filing
  - Define appropriate controls for the database
- Possible use: phishing campaigns or supply chain attacks

Example: Documents

RSAC Sandbox

- June 2019 NYC blackout
  - ~6 hours; 72,000 affected; caused by primary/backup system malfunction
- Publicly available documents
  - 2014-2020 upgrades to specific, decades old RTUs across sites (including affected substation)
  - Protection relay connection to Energy Control Center (new and old configurations) is serial
    - Modifying protection relay setting requires engineers onsite
- ***Not cyber***, but useful to understand the lay of the land

Vendor websites



SIEMENS

Search for...

Press Release 15 October 2019 Gas and Power Houston

Three expanded power plants deliver additional 1 GW to Bolivia

- Power plants Termoeléctrica del Sur, de Warnes, and Entre Ríos inaugurated in August and September
- Upgrade to combined cycle power plants increase the generation capacity by one gigawatt
- Expansion provides reliable energy supply and will allow export of value-added products

With the official inauguration of the Termoeléctrica de Warnes power plant in mid-September, all three power plants in Bolivia were inaugurated within a few weeks in August and September. Since the contract signing in 2016, Siemens has expanded Bolivia's three largest thermal power plants to efficient combined cycle mode. The power plants are owned and operated by Ende Andina SAM. Together, all three add more than one gigawatt of electrical power to its current maximum capacity and to the Bolivian national grid.

"The three power plants are important milestones for Bolivia 2025, an ambitious energy project designed to increase power generation capacity to 6000 megawatts (MW) by 2025. This will establish energy independence for Bolivia while also boosting the capacity to export electricity to Bolivia's neighboring countries," explained Ramiro Becerra Flores, project director at ENDE Andina. "The process of converting gas into energy is now more efficient, the country has the opportunity to find a use for surplus or residual amounts of gas that will be produced as a result of the integration of the new, much more efficient Siemens technologies."

"Siemens has developed a unique solution to support Bolivia's ongoing efforts to improve access to electricity for its growing population and developing economy," said Karim Amin, CEO of Power Generation at Siemens Gas and Power. "Every society has its own unique needs. Our diverse energy portfolio can address these various needs for the benefit of societies everywhere."

The three thermal power plants were already equipped with 13 Siemens gas turbines and the associated generators for operation in simple-cycle mode to provide Bolivia with fast generation of electricity. During the expansion phase that began in 2016, Siemens added 14 SGT-800 gas turbines, 11 SST-400 steam turbines with condensers, 22 steam generators, and the SPPA-T3000 instrumentation and control system to the three power plants. In combined cycle mode, it was possible to increase the plant efficiency from 40 to 51 percent.

The **Termoeléctrica del Sur** thermal power plant in southern Bolivia, near the border with Argentina was inaugurated on August 8, 2019. The expansion increased the plant's peak capacity from 160 to 480 MW. The **Entre Ríos** plant, inaugurated on September 11, 2019, is located in the department of Cochabamba, situated 220 kilometers southeast of La Paz. Thanks to the inclusion of three new blocks, the plant has been able to increase its generation capacity from 120 to 480 MW. The **Warnes** plant is located in Bolivia's Santa Cruz department and was inaugurated on September 16, 2019. With the new equipment, the plant's generation capacity rose from 200 to 520 MW. This expansion of its energy network will help Bolivia continue with its energy development plan and help the country meet its goal of becoming the energy heart of South America.

- "Power plants Termoeléctrica del Sur, de Warnes and Entre Rios inaugurated in August and September"
- "Siemens added 14 SGT-800 gas turbines, 11 SST-400 steam turbines with condensers, 22 steam generators, and the SPPA-T3000 instrumentation and control system to the three power plants. In combined cycle mode, it was possible to increase the plant efficiency from 40 to 51 percent."
- Exact names and locations of Bolivian plants.

Vendor websites

Rockwell Automation

Industries Capabilities Products News Events

Investor Relations Overview Press Releases Financials Events & Presentations Corporate Governance Shareowne

Lonza Selects Rockwell Automation for Digital Transformation of Pharmaceutical Operations

July 16, 2019

Lonza to use PharmaSuite MES software, along with FactoryTalk InnovationSuite to accelerate paperless, 24/7 production of cutting-edge capsules

MILWAUKEE--(BUSINESS WIRE)-- Lonza has selected Rockwell Automation for the turnkey implementation of the Lonza strategic vision of bringing the digital factory to nine former Capsugel facilities that manufacture drug capsules. The Switzerland-based company, founded in 1897 with approximately 15,500 employees, chose Rockwell Automation's PharmaSuite Manufacturing Execution System (MES) software to digitize the operations in their manufacturing environments. Specifically, the solution is designed to help avoid disruptions during high volume periods of just-in-time orders for on-demand production, ushering in a new era of operational efficiency.

Rockwell Automation services all of the top 10 global life sciences firms, offering expertise in scalable digital transformation, industrial analytics, and IoT solutions for fully automated, high-speed manufacturing environments. This deployment to nine sites will also provide 1,500 employees across the globe new, operational technology-centric tools for reaching the next level of efficiency and quality.

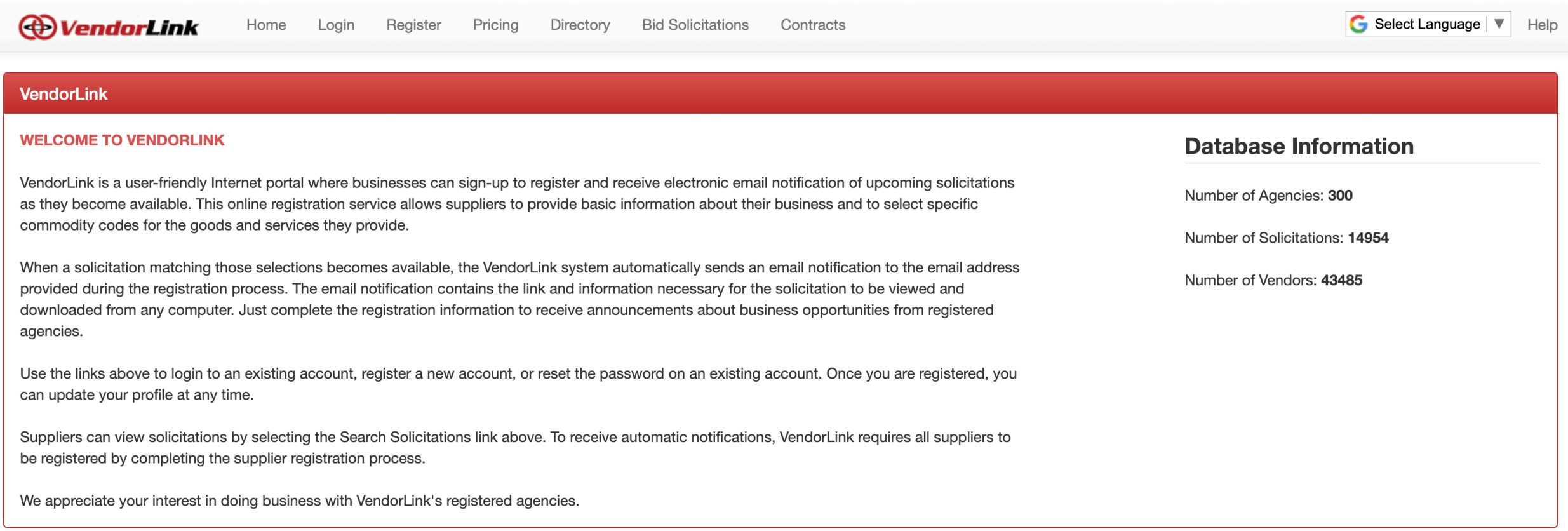
"Digital transformation is bringing new levels of operational efficiency, quality, process automation, and employee productivity to pharmaceutical companies globally," said John Genovesi, senior vice president, Enterprise Accounts and Software, Rockwell Automation. "We're proud to be working with Lonza as they evolve their products, operations, and workforce towards their maximum potential through the use of Rockwell Automation's software solutions."

Lonza will use PharmaSuite MES software, along with FactoryTalk InnovationSuite software to better trace product down to the individual capsule carton and gain insights into performance and production. A segregation of SAP and PharmaSuite MES will also help avoid the disruption of in case of a global enterprise resource planning ERP shutdown or required maintenance by enforcing workflows and collecting necessary information.

- Pharmaceutical company details Rockwell integration/use:
  - "Lonza will use PharmaSuite MES software, along with FactoryTalk InnovationSuite software to better trace product down to the individual capsule carton and gain insights into performance and production. A segregation of SAP and PharmaSuite MES will also help avoid the disruption of in case of a global enterprise resource planning ERP shutdown…"

Third-party software and services

RSAC Sandbox



Shodan

RSAC Sandbox

207.171.203.219 ip-207-171-203-219.wrecwireless.coop View Raw Data

Industrial Control System

City	Wells
Country	United States
Organization	Wells Rural Electric Company
ISP	NRTC
Last Update	2019-10-17T14:14:13.008774
Hostnames	ip-207-171-203-219.wrecwireless.coop
ASN	AS36788

Ports

80 161 502 9999 30718

Services

80
tcp
http

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic
```

161
udp
snmp

```
Modbus/TCP to RTU Bridge
```

502
tcp
modbus

```
Unit ID: 1
-- Slave ID Data: Gateway Target Device Failed To Respond (Error)
-- Device Identification: Gateway Target Device Failed To Respond (Error)

Unit ID: 2
-- Slave ID Data: Gateway Target Device Failed To Respond (Error)
-- Device Identification: Gateway Target Device Failed To Respond (Error)

Unit ID: 3
-- Slave ID Data: Gateway Target Device Failed To Respond (Error)
-- Device Identification: Gateway Target Device Failed To Respond (Error)

Unit ID: 4
-- Slave ID Data: Gateway Target Device Failed To Respond (Error)
-- Device Identification: Gateway Target Device Failed To Respond (Error)

Unit ID: 5
-- Slave ID Data: Gateway Target Device Failed To Respond (Error)
-- Device Identification: Gateway Target Device Failed To Respond (Error)
```

Job postings

RSAC Sandbox

NORTHROP GRUMMAN

Senior Principal Industrial Controls Engineer -Manufacturing Operations

APPLY NOW →

NORTHROP GRUMMAN

A leading global security company, Northrop Grumman provides innovative products and solutions in autonomous systems, cyber security, and complex logistics to government and commercial clients.

ABOUT THIS JOB

- LOCATION
  Baltimore, MD

Northrop Grumman's Mission Systems is seeking an **Industrial Controls Engineer for Operations Manufacturing**. This position focuses on automated control systems used in electronics and mechanical manufacturing, assembly, and packagi

The Industrial Controls Engineer responsibilities includ tasks outlined below:

Process Development

Developing new and maintaining or improving existing manufactu machine autonomy

Creating and managing to project plans (tasks, resources, schedul activities

Designing, specifying, and procuring custom manufacturing equip production readiness and preparing equipment for production

Developing and optimizing industrial control systems

Developing/revising control logic, wiring, and human-machine in troubleshooting

Assisting with design of custom equipment, conveyors, robots, an

Documenting state-of-the-art automation capabilities and guideli

Basic Qualifications for a Senior Principal Engineer:

Bachelor of Science degree or higher in Engineering or related STEM area plus 9 years of relevant professional experience (or 7 years with an MS). Candidates with a High School diploma and 13 years of experience and those with an Associate's degree and 11 years of experience will be considered.

Industrial Controls Engineering experience

Familiarity with programmable logic controllers (PLC's) (for example Siemens, Allen Bradley, Omron and Beckhoff)

Experience programming PLC's per IEC 61131-3 (for example -ladder logic, function block diagram and structured text)

Familiarity with some of these -RSLogix, Step 7, CX-One, TwinCAT, Labview and/or Wonderware software

Experience sending PLC data to servers (for example Open Platform Communications (OPC), OPC Unified Architecture (OPC-UA) and Structured Query Language (SQL) servers)

Familiarity with motion controllers, solenoids, conveyors, servos, actuators and other pneumatic/electromechanical systems

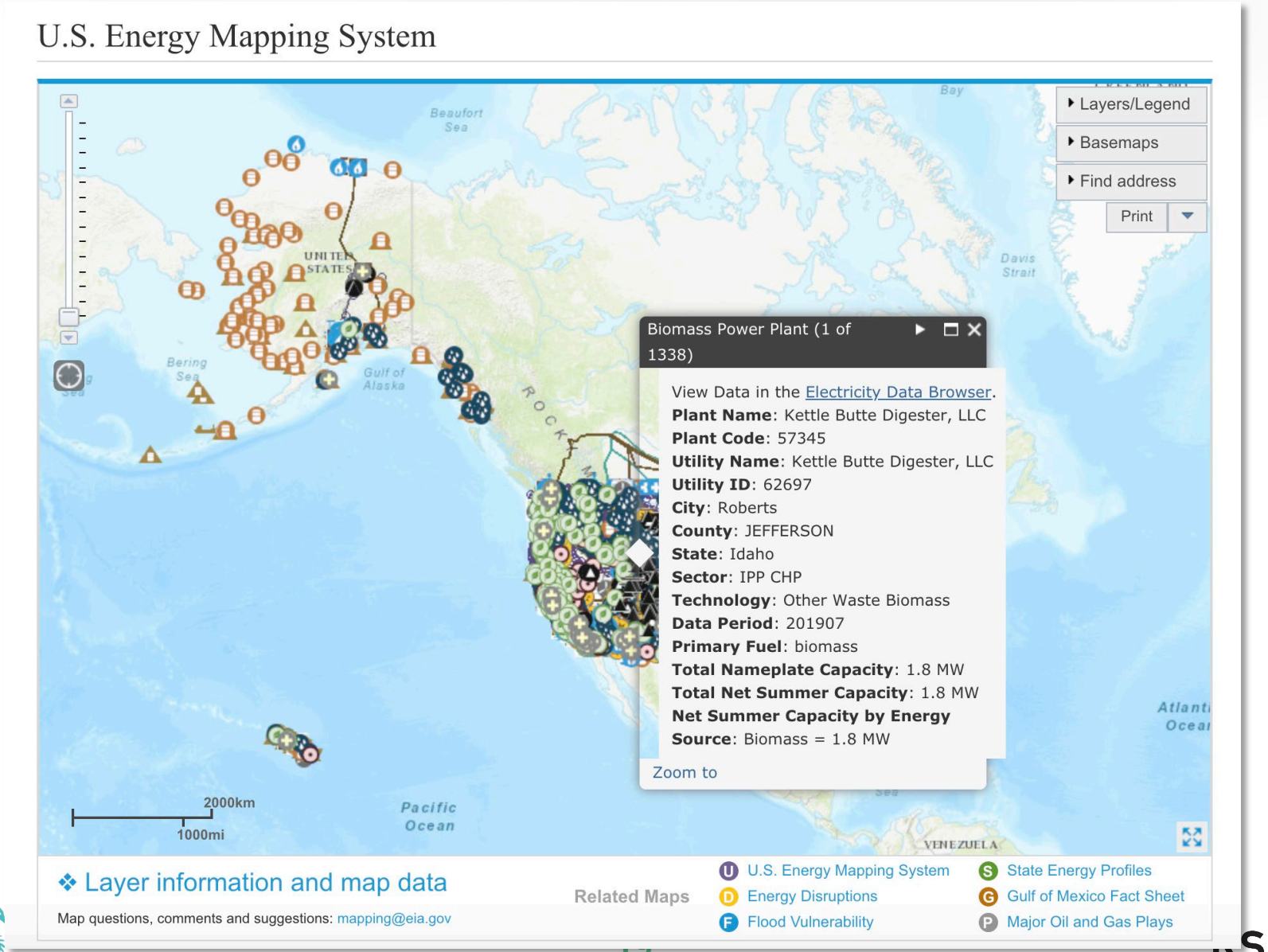
Experience with machine vision systems and barcode readers (for example Cognex, Keyence, and Fanuc)

Familiarity with varying process sensors for environment, motion, measurement and presence (for example Banner, Sick, Allen-Bradley, Keyence, Omron)

Fluency in MS Office software applications

Ability to obtain and maintain a US Secret Security Clearance (US Citizenship is required.)

Government data



Dragos case study

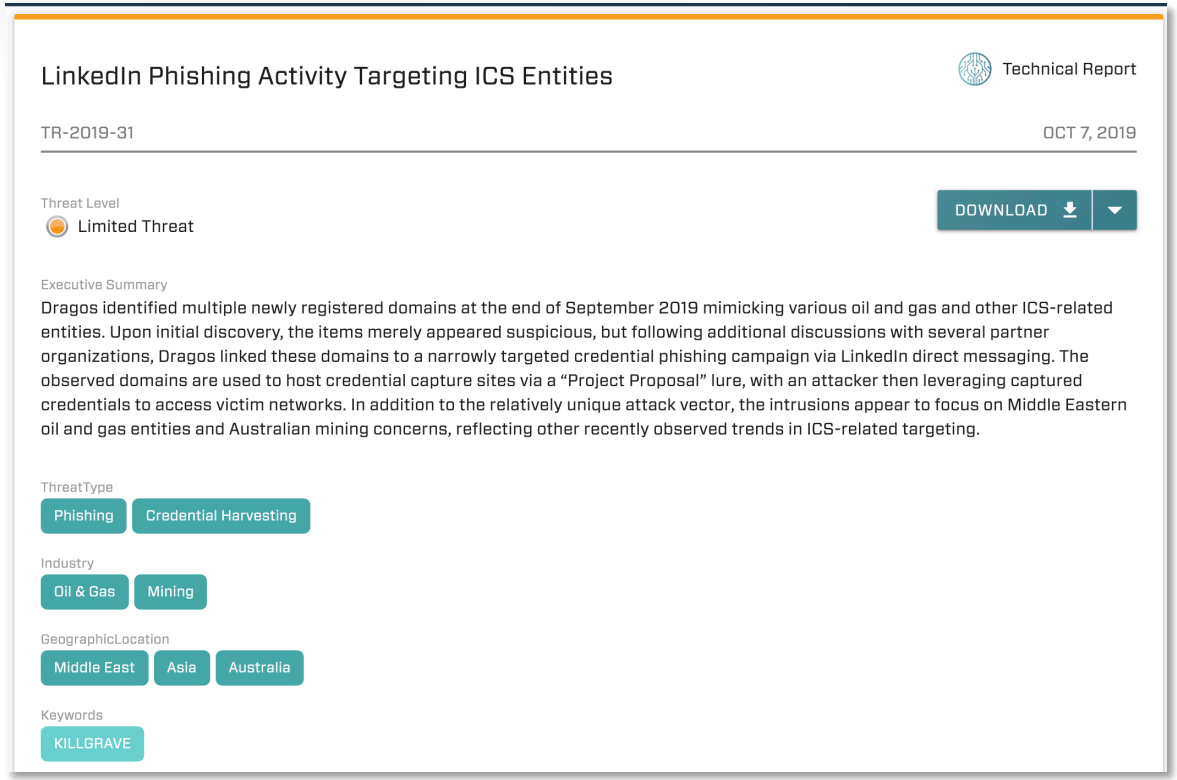
RSAC Sandbox

- Activity group targeting western energy company
  - Early attack planning; heavy reconnaissance on outward infrastructure
  - Goal: develop targeting, inform operational planning, predict defender response
- Adversary obtained specialized knowledge required for successful attack
  - List of generation stations
  - Engineering diagrams
  - Information relating to islanding events and responses to grid instability
  - Outage and services maps

DRAGOS

Dragos case study

- Newly registered domains mimicking Middle Eastern ONG & Australian mining entities
- Sent links to corporate leadership via LinkedIn DM with “project proposal” lure
  - Credential capture webpages; spoofed logins used for remote credential replay across victims network for initial access
- Key takeaway: unique attack vector; reflects ICS-targeting trend



LinkedIn Phishing Activity Targeting ICS Entities

Technical Report

TR-2019-31

OCT 7, 2019

Threat Level

Limited Threat

DOWNLOAD

Executive Summary

Dragos identified multiple newly registered domains at the end of September 2019 mimicking various oil and gas and other ICS-related entities. Upon initial discovery, the items merely appeared suspicious, but following additional discussions with several partner organizations, Dragos linked these domains to a narrowly targeted credential phishing campaign via LinkedIn direct messaging. The observed domains are used to host credential capture sites via a “Project Proposal” lure, with an attacker then leveraging captured credentials to access victim networks. In addition to the relatively unique attack vector, the intrusions appear to focus on Middle Eastern oil and gas entities and Australian mining concerns, reflecting other recently observed trends in ICS-related targeting.

ThreatType

Phishing | Credential Harvesting

Industry

Oil & Gas | Mining

GeographicLocation

Middle East | Asia | Australia

Keywords

KILLGRAVE

DRAGOS

Defense & mitigations

RSAC Sandbox

- Conduct regular OSINT assessments
  - Identify and limit information available about vendors and partners; documents, schematics, data sheets; job advertisements; credentials in public dumps; identify gaps in security architecture
- Implement compensating controls
  - Implement authentication gateways to sensitive documents; mandate multifactor authentication and user awareness; document and assess OSINT value to an adversary

OSINT Collection Risk and Vulnerability Matrix

RSAC Sandbox

	Information is of Low relevance/importance for intelligence collection	Information is of Medium relevance/importance for intelligence collection	Information is of High relevance/importance for intelligence collection
Adversary utilization requires little to no analytical effort for operational integration	2	3	3
Adversary utilization requires moderate to specialized analytical effort for operational integration	1	2	3
Adversary utilization requires highly technical analytical effort for operational integration	1	2	3

DRAGOS

References

- https://www.nytimes.com/2019/07/15/nyregion/nyc-blackout-con-edison.html
- https://www.sec.gov/Archives/edgar/data/1039065/000104746919004853/0001047469-19-004853-index.htm
- https://press.siemens.com/global/en/pressrelease/three-expanded-power-plants-deliver-additional-1-gw-bolivia
- https://ir.rockwellautomation.com/press-releases/press-releases-details/2019/Lonza-Selects-Rockwell-Automation-for-Digital-Transformation-of-Pharmaceutical-Operations/default.aspx
- https://download.schneider-electric.com/files?p_enDocType=Customer+success+story&p_File_Name=998-20020509_GMA-US_Thu+Thiem+Power_X1A.pdf&p_Doc_Ref=998-1284-02-04-15AR0_EN
- https://www.themuse.com/jobs/northropgrumman/senior-principal-industrial-controls-engineer-manufacturing-operations?utm_campaign=google_jobs_apply&utm_source=google_jobs_apply&utm_medium=organic
- Shodan.io
- Casey Brooks, Senior Adversary Hunter, Dragos (OSINT Collection Risk Framework)


THANK YOU
https://dragos.com
Twitter: @DragosInc
LinkedIn: DragosInc
25
DRAGOS