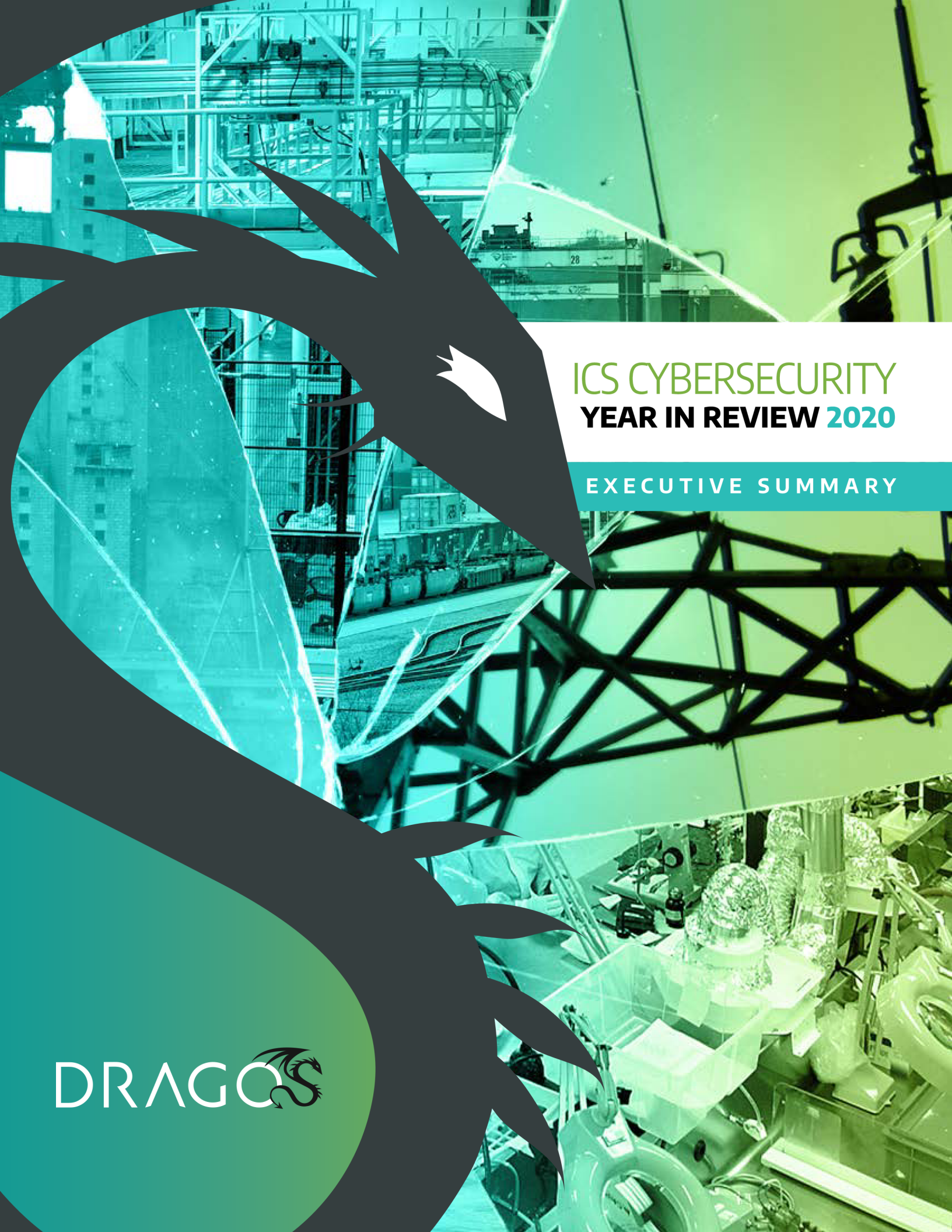


ICS CYBERSECURITY
YEAR IN REVIEW 2020

EXECUTIVE SUMMARY

DRAGOS

Executive Summary

The Dragos Year in Review report is an annual analysis of Industrial Control System (ICS)/Operational Technology (OT) focused cyber threats, vulnerabilities, assessments, and incident response insights.[1] In this executive summary, Dragos experts share highlights from the report.

In 2020, the industrial community performed amazing feats to keep civilization running under extremely challenging circumstances with the global pandemic. Infrastructure providers kept key services and goods available including electric power, manufactured goods, water, oil and gas, mining, chemical, rail, and transport while many faced hardships globally. As a result of these efforts, organizations shifted in how they conducted business to include an increasingly connected industrial environment. This is a trend that has existed for many years, even while many organizations still believed they had highly segmented or even air-gapped ICS networks.

The Year in Review report captures how some of the community is performing and progressing, and areas of improvement that will be needed to continue to provide safe and reliable operations.

[1] The terms "ICS" and "OT" will be used interchangeably for the purpose of this report. These terms are used differently in different communities.

ICS Threat Landscape Highlights

Cyber risk to industrial sectors has grown and accelerated dramatically, led by ransomware impacting industrial processes, intrusions enabling information gathering and process information theft, and new activity from adversaries targeting ICS. Adversaries often build programs and campaigns slowly over time, with later campaigns often being more successful and disruptive due to previous efforts. Throughout 2020, the 11 Activity Groups identified by Dragos prior to 2020 remained active against industrial organizations. Four new Activity Groups with the assessed motivation of targeting ICS/OT were discovered.

Four new threat groups with the assessed motivation of targeting ICS/OT were discovered, accounting for a **36 percent increase** in known groups.

- STIBNITE
- TALONITE
- KAMACITE
- VANADINITE

The abuse of valid accounts was the **number one technique** used by named threats.

MAJOR ICS THREAT TRENDS IN 2020

- ICS THREAT ACTIVITY GROUPS INCREASE SIGNIFICANTLY
- PHISHING CONTINUES TO ENABLE ICS INTRUSIONS
- REMOTE ACCESS DIRECTLY TO ICS LEVERAGED OFTEN BY THREATS
- THE BEGINNING OF RANSOMWARE SPECIFICALLY TARGETING ICS
- SUPPLY CHAIN CONCERNS AMPLIFIED BY LIMITED VISIBILITY IN ICS

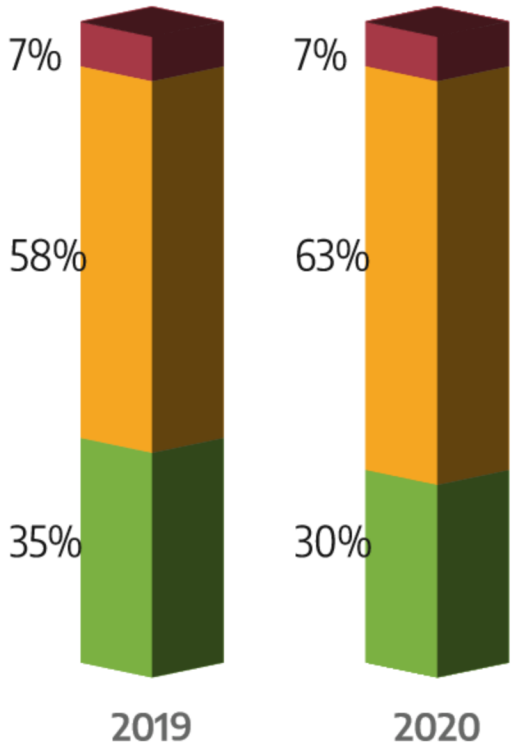
ICS Vulnerabilities Highlights

Dragos researchers analyzed 703 ICS/OT vulnerabilities in 2020, a 29 percent increase over 2019, demonstrating a rise in publicly known flaws in systems supporting industrial operations. Analysis of these vulnerabilities and related advisories found that a slim minority could be classified as flaws that require immediate actions, such as critical vulnerabilities with perimeter-facing and network exploitable vulnerabilities. The difficulty is that practitioners struggle to prioritize these due to errors and a lack of actionable guidance in advisories.

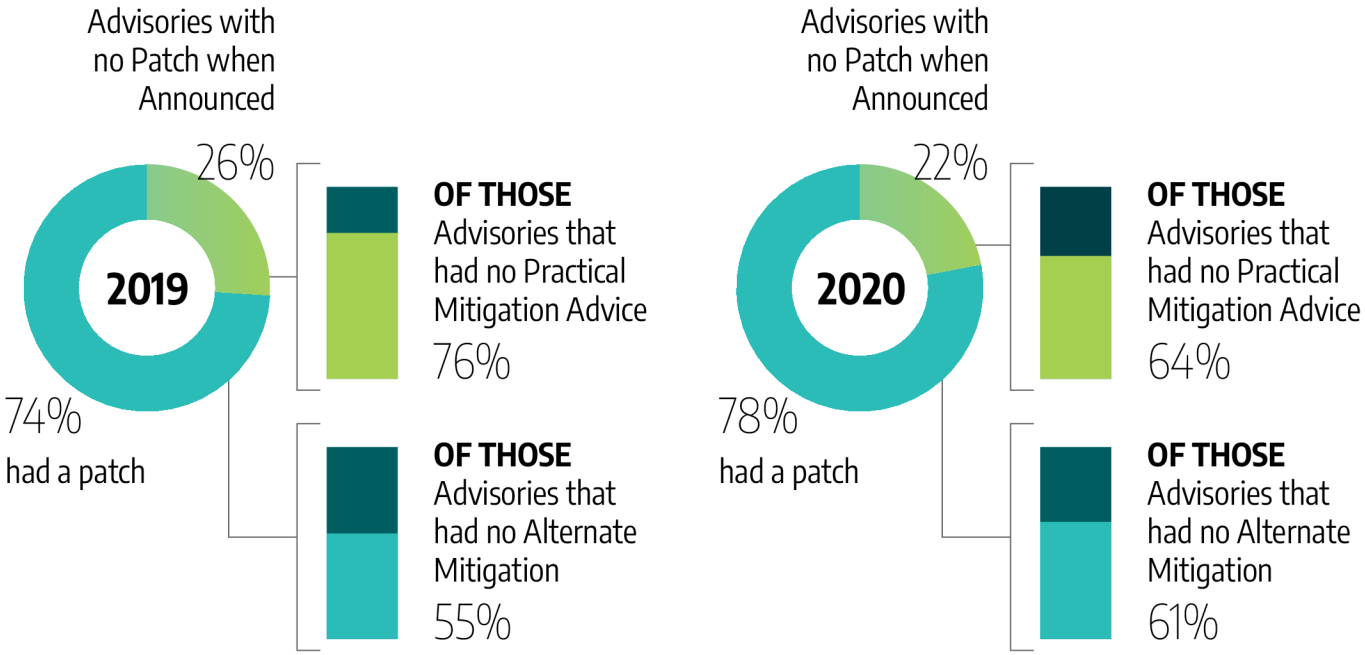
NOW – IMMEDIATE ACTION
The **"Now"** flaws require immediate action. These flaws include critical vulnerabilities such as perimeter-facing and network exploitable vulnerabilities, and other vulnerabilities that should be addressed as soon as practicable.

NEXT – LIMITED THREAT
Limited Threat vulnerabilities fall into the **"Next"** category. These might be network exploitable but are present deeper in the network and require more work, access, and knowledge for an adversary to exploit or impact OT processes.

NEVER – POSSIBLE THREAT/NO ACTION
Low vulnerabilities pose a possible threat but rarely require action in vulnerability prioritization. They can be considered **"Never"** vulnerabilities. It is more beneficial for an organization to monitor its environment for signs of exploitation rather than to take devices and services offline to take appropriate mitigation measures.

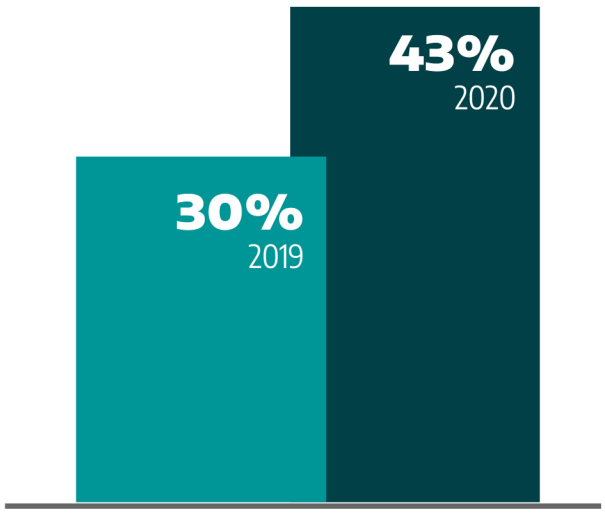


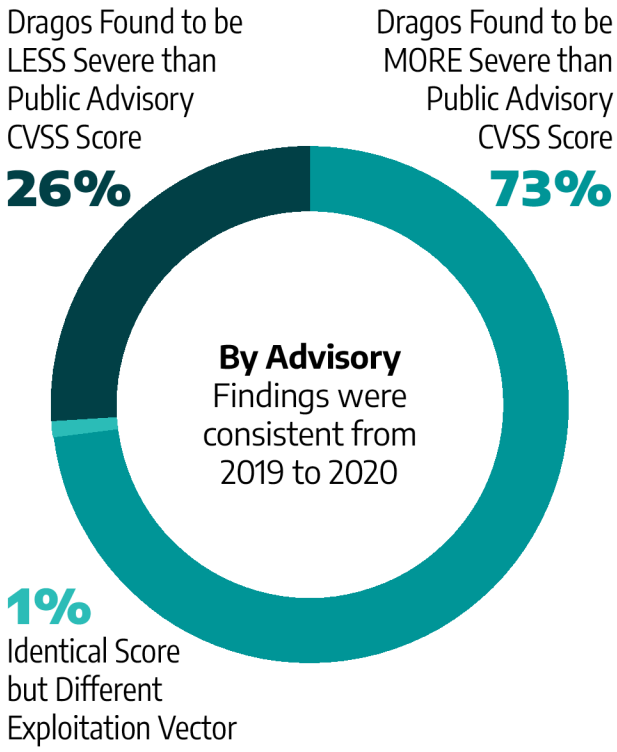
Actionable Guidance Missing in Most 2020 Advisories



Vulnerability Error Rates

By Advisory
Advisories with Incorrect Data

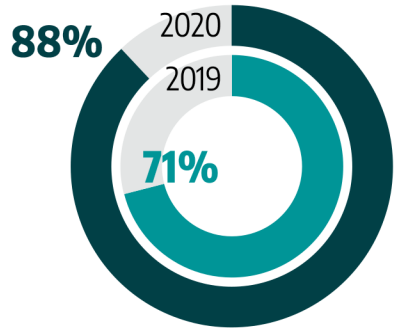




Lessons Learned from the Front Lines Highlights

Based on a growing set of data gathered from annual service engagements conducted by the Dragos team of ICS cybersecurity experts on several service types, Dragos found that the vast majority of its services clients had no visibility into their ICS environments. While most clients demonstrated a focus on an enhanced asset inventory, this effort is only the foundation for asset visibility. Many customers only monitored the IT to OT boundary without monitoring activity inside the ICS network. Although asset owners and operators follow many of the best practices and their applicable regulation, Dragos continues to observe instances of poor segmentation with unexpected or unknown connections from the ICS network. While Dragos threat data shows the abuse of valid accounts is a favorite method employed by Threat Activity Groups, Dragos found organizations continue to frequently share credentials between IT and OT networks.

Environments Exhibiting Poor Security Perimeters



Extremely Limited / No Visibility into OT Environment

Organizations that Lacked Separate IT and OT User Management

Recommendations

As organizations strategize a path forward, Dragos recommends five key OT cybersecurity initiatives to improve on in 2021 based on the empirical evidence demonstrated in the report.

The top five recommendations to enhance the security of an ICS environment are:

1 – INCREASE OT NETWORK VISIBILITY

90 percent of service engagements included a finding about lack of visibility. Visibility includes network monitoring, host logging, and maintaining a Collection Management Framework (CMF).

2 – IDENTIFY AND PRIORITIZE CROWN JEWELS

100 percent of external routable network connections to ICS environments were believed to be air-gapped. Crown Jewel Analysis identified a digital attack path to impact a critical physical process.

3 – BOOST INCIDENT RESPONSE CAPABILITIES

42 percent of Incident Response Services Engagements discovered organizations did not have a suitable Incident Response Plan (IRP) and **75 percent had difficulty with declaring a cyber incident.**

4 – VALIDATE NETWORK SEGMENTATION

88 percent of Services engagements included a finding about improper network segmentation. This includes issues like weak or segmentation between IT and OT networks, permissive firewall rulesets, and externally routable network connections.

5 – SEPARATE IT AND OT CREDENTIAL MANAGEMENT

54 percent of service engagements included a finding about shared credentials. This includes accounts shared between IT and OT, default accounts, and vendor accounts. Shared credentials enables adversaries to use Valid Accounts, which is the top TTP used by the ICS Activity Groups we track.

The risk to ICS is not born from an IT and OT convergence, but instead from a convergence of an increasingly ICS aware and capable threat landscape with the digital transformation and hyperconnectivity of the industrial community. As the community progresses, areas of improvement emerge to continue safe and reliable operations. Dragos is committed to providing actionable information to the industrial community to enable the safety and security of the environment and the protection of human life.

For more details, read the full Dragos Year in Review report HERE.

Dragos is an industrial (OT/ICS/IIoT) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Dragos.com