INDUSTRIAL CONTROL
VULNERABILITIES
2017 IN REVIEW

DRAGOS

"Industrial Control Vulnerabilities: 2017 in Review", Dragos, Inc., Hanover, MD, 1 March 2018

CONTENTS

DRAGOS

A YEAR IN VULNERABILITIES

2017

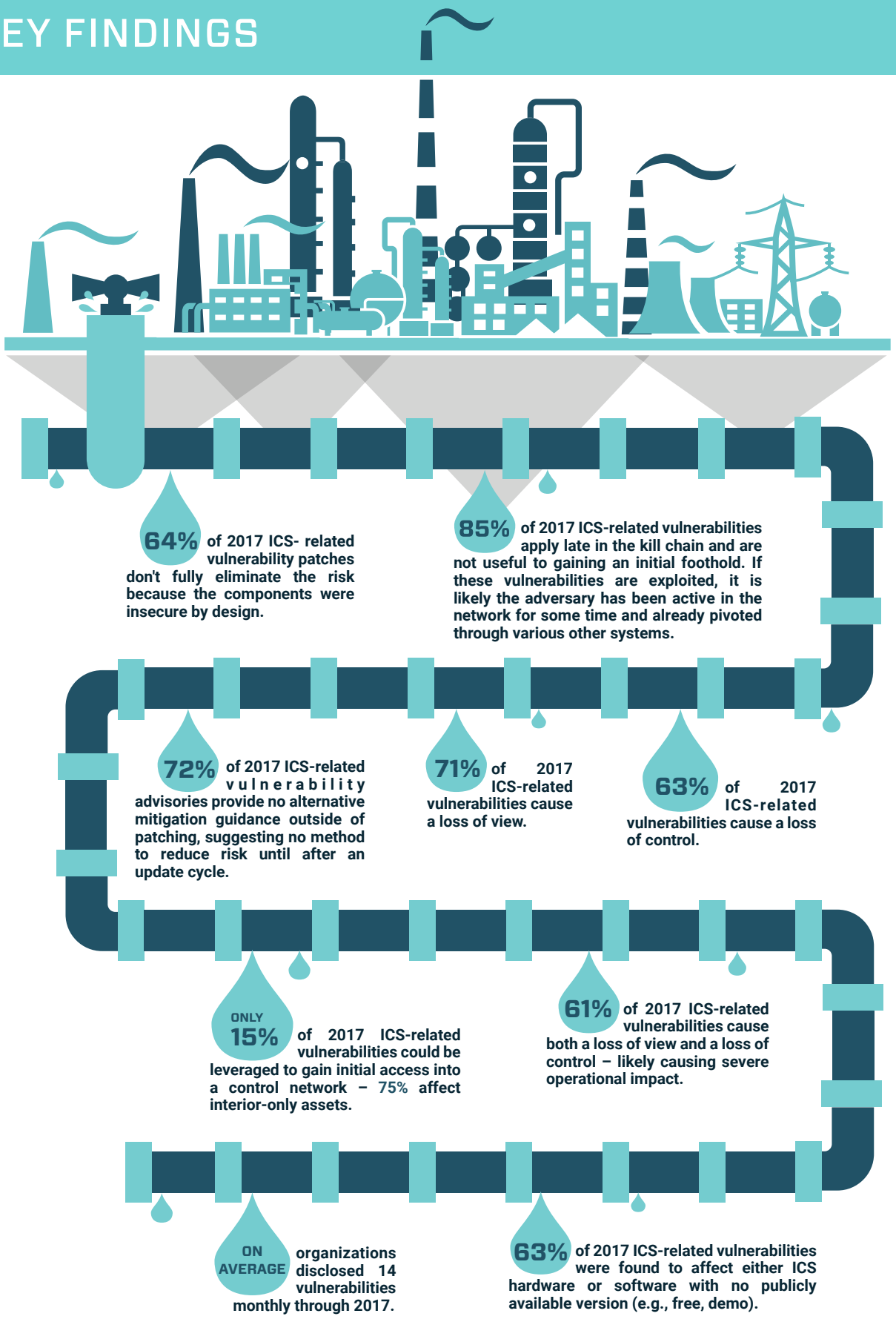
In 2017, Dragos tracked 163 vulnerability advisories with an industrial control system (ICS) impact. Of these, the majority were vulnerabilities in insecure-by-design products which are typically deep within an ICS network.

Dragos found that public reports failed to adequately define the industrial impact of vulnerabilities. Coupled with the fact that most public vulnerability disclosures provide no alternative guidance beyond, "patch," or "use secure networks," Dragos sees huge room for improvement in public disclosure reports – improvement that it strives to make in its own reporting.

Reid Wightman

Senior Vulnerability Analyst | Dragos, Inc.

KEY FINDINGS



64% of 2017 ICS- related vulnerability patches don't fully eliminate the risk because the components were insecure by design.

85% of 2017 ICS-related vulnerabilities apply late in the kill chain and are not useful to gaining an initial foothold. If these vulnerabilities are exploited, it is likely the adversary has been active in the network for some time and already pivoted through various other systems.

72% of 2017 ICS-related vulnerability advisories provide no alternative mitigation guidance outside of patching, suggesting no method to reduce risk until after an update cycle.

71% of 2017 ICS-related vulnerabilities cause a loss of view.

63% of 2017 ICS-related vulnerabilities cause a loss of control.

ONLY 15% of 2017 ICS-related vulnerabilities could be leveraged to gain initial access into a control network – 75% affect interior-only assets.

61% of 2017 ICS-related vulnerabilities cause both a loss of view and a loss of control – likely causing severe operational impact.

ON AVERAGE organizations disclosed 14 vulnerabilities monthly through 2017.

63% of 2017 ICS-related vulnerabilities were found to affect either ICS hardware or software with no publicly available version (e.g., free, demo).

RECOMMENDATION

BETTER ICS VULNERABILITY

ICS vulnerability assessments as published are frightfully inadequate to providing asset owners and operators with meaningful guidance.

"Deploy firewalls and use only trusted networks" is not a meaningful suggestion yet is the only alternative guidance provided by most advisories aside from "patch."

RECOMMENDATION

Vulnerability advisories must provide reasonable effective alternative options. Offer several alternatives which may not be applicable to all users but help some. This advice should include specific ports and services to restrict or monitor to reduce risk and impact from an attack, or specific system hardening recommendations to better defend systems from local exploitation.

ICS vulnerability impact analysis is woefully uninformed leading to poor risk assessment by asset owner/operators. For example, a "denial of service" against field devices doesn't determine if such an attack results in a communications disruption or impact physical function which are radically different risks.

RECOMMENDATION

Traditional IT impact assessments are insufficient for ICS/OT environmental risk analysis. Advisories should adopt ICS-specific metrics to better inform users of operational risks.

RESEARCH WITH STRONGER COMMUNITY

Researchers tend to over-focus on hardware and field devices, and focus little on the network perimeter and entry points to ICS networks. Research thus ignores helping to detect and prevent the critical early stages of an attack.

Industrial-focused advisories ignore common firewalls and VPNs used for both separating ICS networks from the corporate network, and for providing remote access. These firewalls tend to be enterprise IT firewalls, and not ICS-specific, however they are an important protection component of ICS networks.

RECOMMENDATION

Advisories should provide broader coverage and include common enterprise devices and applications commonly used in ICS network separation.

Nearly 66% of advisories cover human-machine interface (HMI), engineering workstations (EWS), and Field Device components; historians, OPC servers, and analytics services all provide cross-domain access between Corporate and ICS networks. Mitigating vulnerabilities in these components does little to reduce overall risk, because the components themselves are insecure by design.

RECOMMENDATION

The research community should increase scrutiny on cross-domain devices and applications where research outcomes will lead to a stronger first layer of defense.

END USER PATCH APPLICATIONS

The beginning of 2018 has shown some massive flops in patch production. Major vendors have released patch-sets that triggered failures in end user systems.

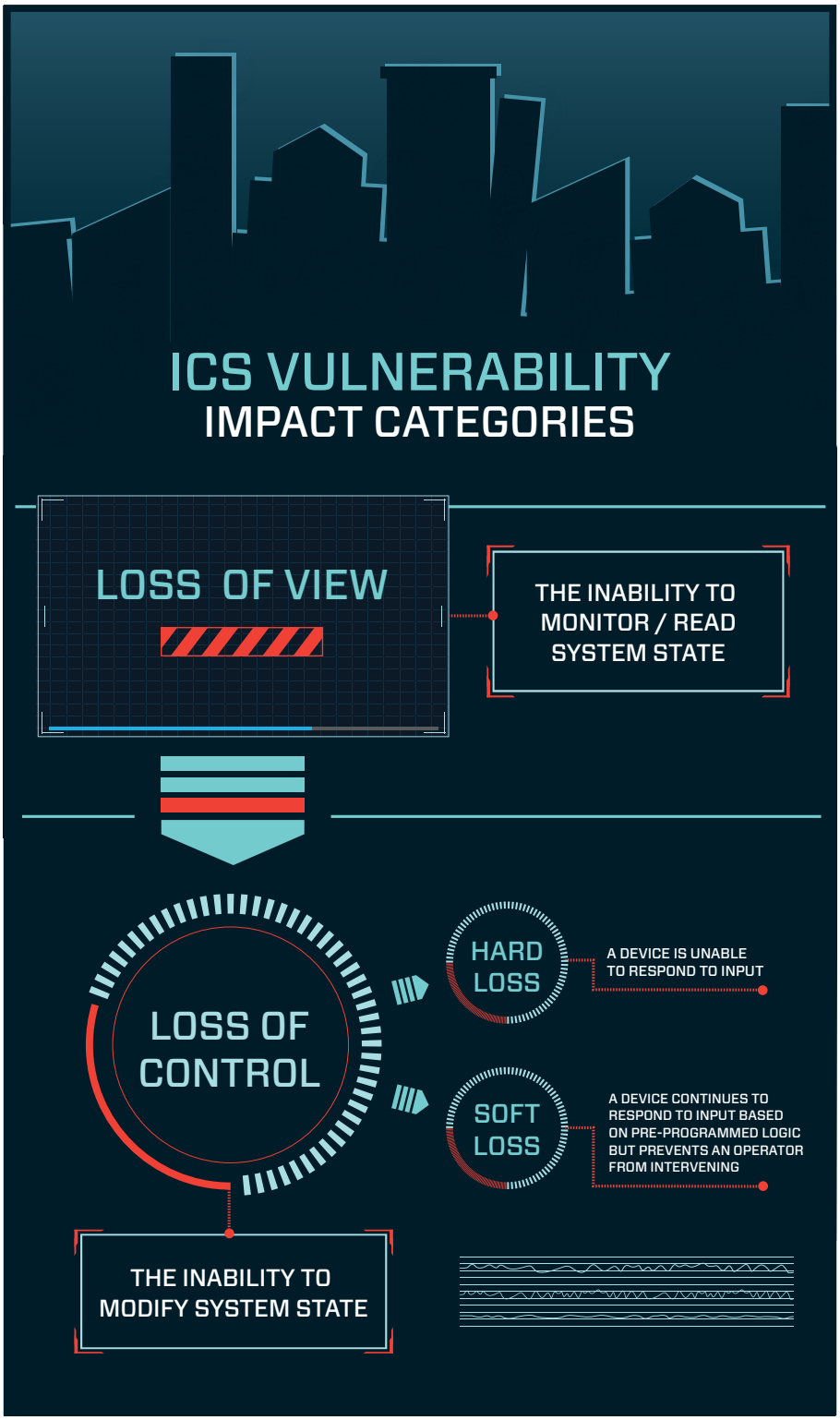
Patches are rarely applied quickly in ICS environments due to concern that the patch may cause an operations outage. Recent patch failures are reinforcing this argument.

RECOMMENDATION

The first step to starting a patch management program must be developing a 'test' or 'development' control systems network which contains samples of the actual plant's critical systems. This allows for proper testing of patches, and minimizes the risk of outage of any critical plant systems.

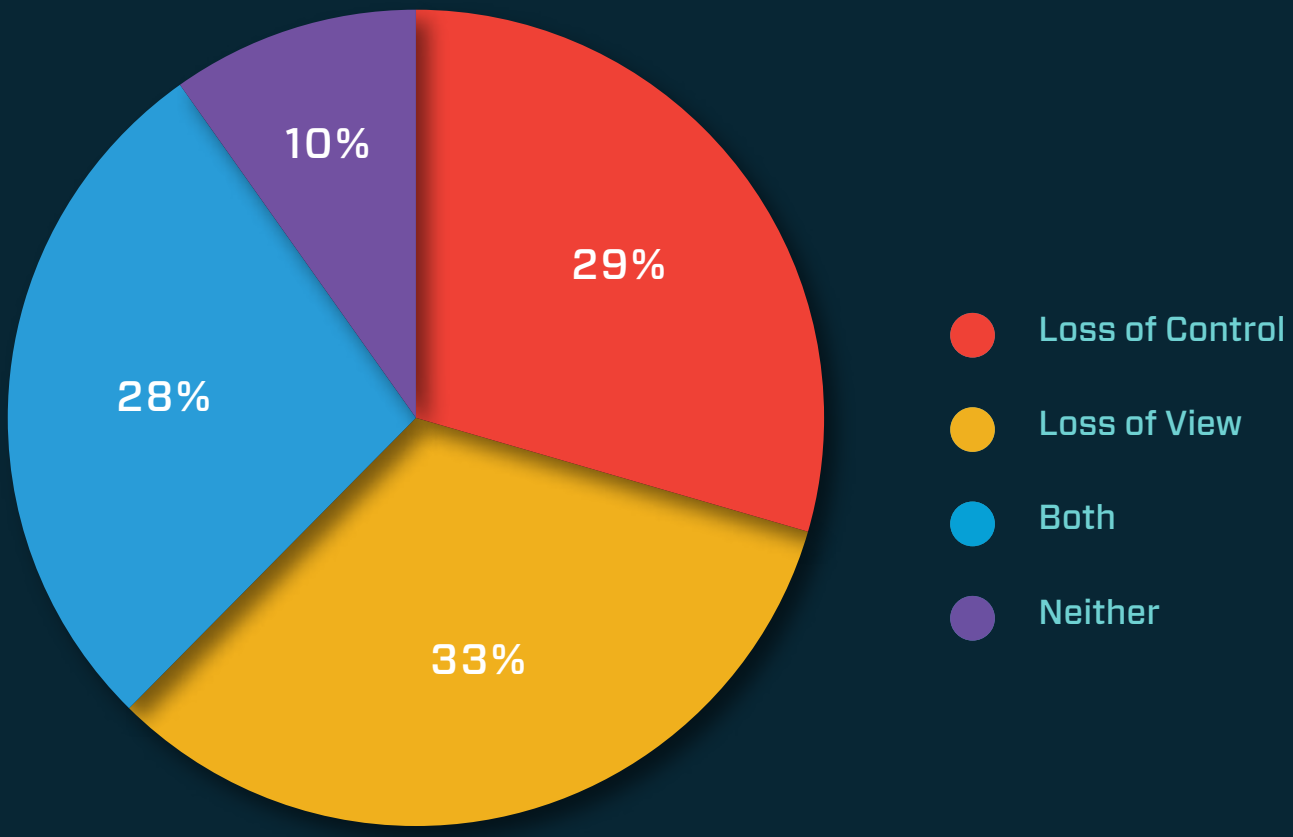
OPERATIONS IMPACT

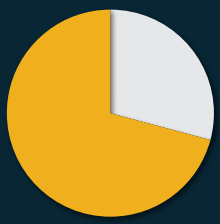
Dragos assesses each vulnerability's operational impact on industrial control processes. Specifically, threats against industrial processes result in three impact categories: Loss of View, Loss of Control, or both.



2017 ADVISORIES

OPERATIONAL IMPACT





71% of all 2017 ICS-related vulnerabilities could result in a loss of view.

63% of all 2017 ICS-related vulnerabilities which could result in a loss of control.

61% of all 2017 ICS-related vulnerabilities potentially causing both a loss of view and a loss of control, a high degree of overlap.

Vulnerabilities which lead to both a loss of view and control occur in the core of traditional control networks affecting both field devices (PLCs, RTUs, etc.) as well as management such as human-machine interface (HMI) systems and engineering workstation (EWS) software. This means that a large percentage (61%) of ICS-related vulnerabilities will cause severe operational impact if exploited.

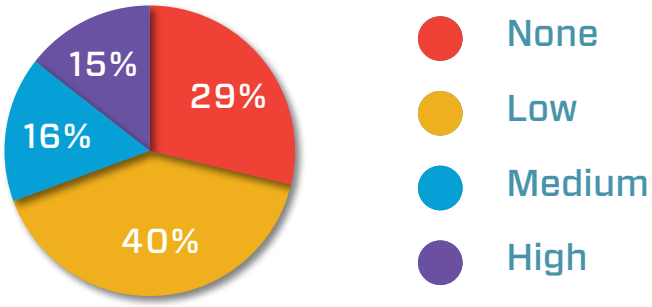
Dragos categorizes both hard and soft loss of control into "Loss of Control." Where possible, Dragos further clarifies which whether a loss of control is hard or soft in vulnerability descriptions.

PERIMETER IMPACTING VULNERABILITIES

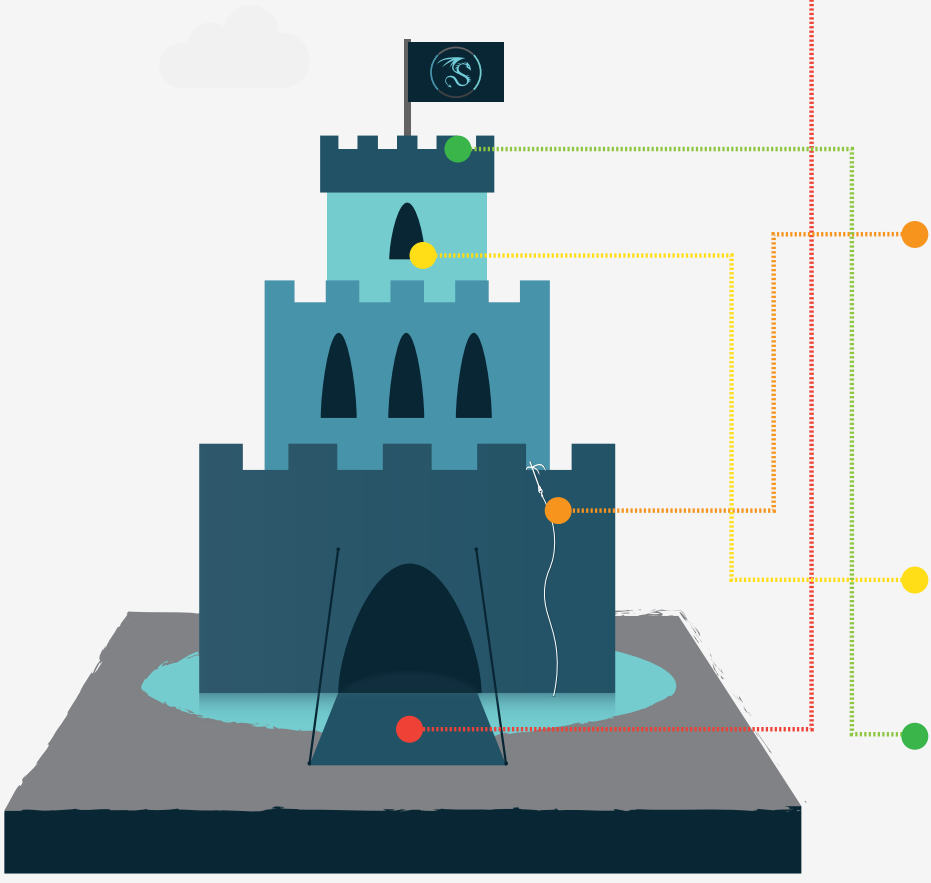
Most industrial control networks exist as separate entities separated from the Internet by the business or corporate network. Even within an industrial control network, devices are layered – with some close or even in the business network while others are deep and more inaccessible. Dragos assesses each vulnerability based on the exposed product's usual proximity to the ICS network perimeter: high (close), medium, low, and none (far).

2017 ADVISORIES

LIKELIHOOD OF ADVISORY IMPACTING NETWORK BORDER



PERIMETER IMPACT



HIGH

Perimeter-connected or even internet-connected. Directly accessible by a non- ICS network. Examples: historians, OPC servers, firewalls and VPN products, as well as cellular and other external network gateways. These systems are often connected to Level 3.5, Level 3 on the Purdue Model.

MEDIUM

Network devices which will cross-connect multiple networks accessible and managed from a network. Most often management will occur from the Purdue Level 3 network, however in some insecure schemes may be managed from DMZ or even Corporate networks. Reconfiguration or poor configuration of these systems may expose ICS networks to Business/ Corporate or Internet networks.

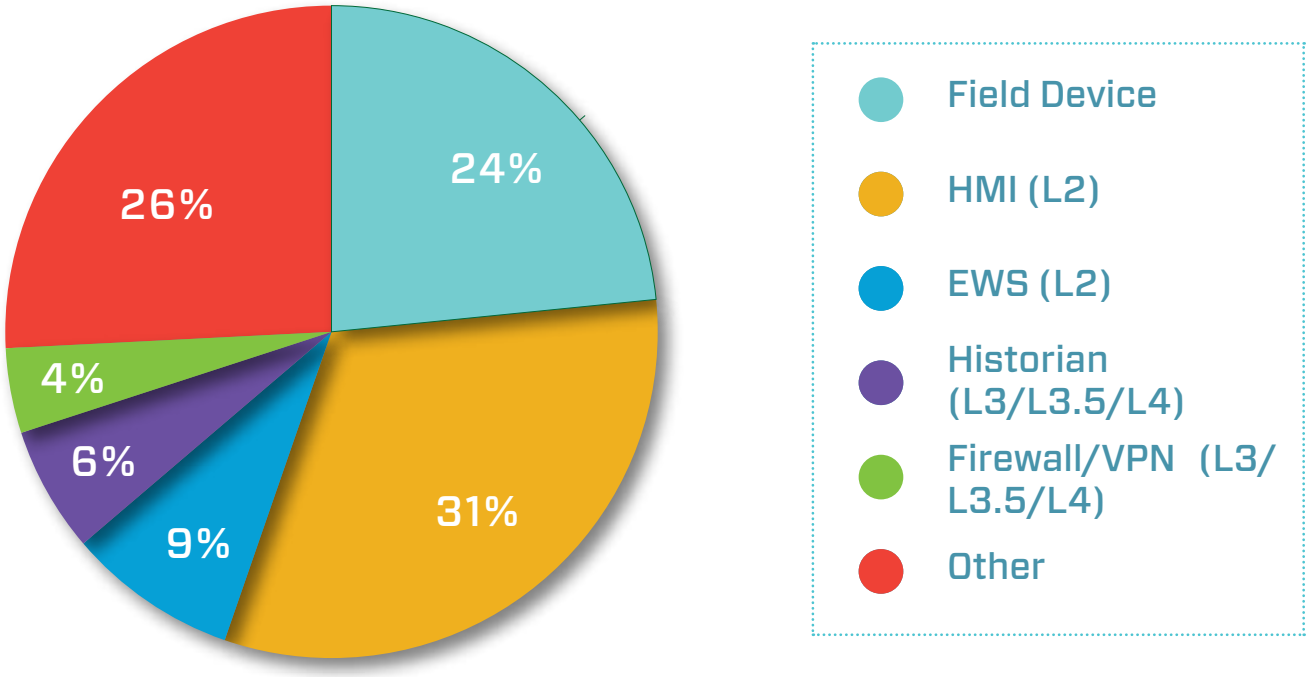
LOW

Central assets on control networks (e.g., HMI, engineering workstations). These map to Purdue Level 2 network.

NONE

Products and assets generally several steps from another network such as field controllers (e.g., PLCs, RTUs). These map to Purdue Level 1 networks.

2017 ADVISORIES
COMPONENT TYPE



The vast majority of vulnerabilities (85%) expose systems unlikely to be used to pivot into an ICS network (proximity: none through medium).

64% of the 2017 ICS-related vulnerabilities impact interior control systems components (HMI, EWS, or controllers).

Only 15% of 2017 ICS-related vulnerabilities would be used to gain initial access to a control network (proximity: high).

26% of all vulnerabilities were reported in field devices (PLCs, RTUs, and other networked controllers which directly read and operate the physical process).

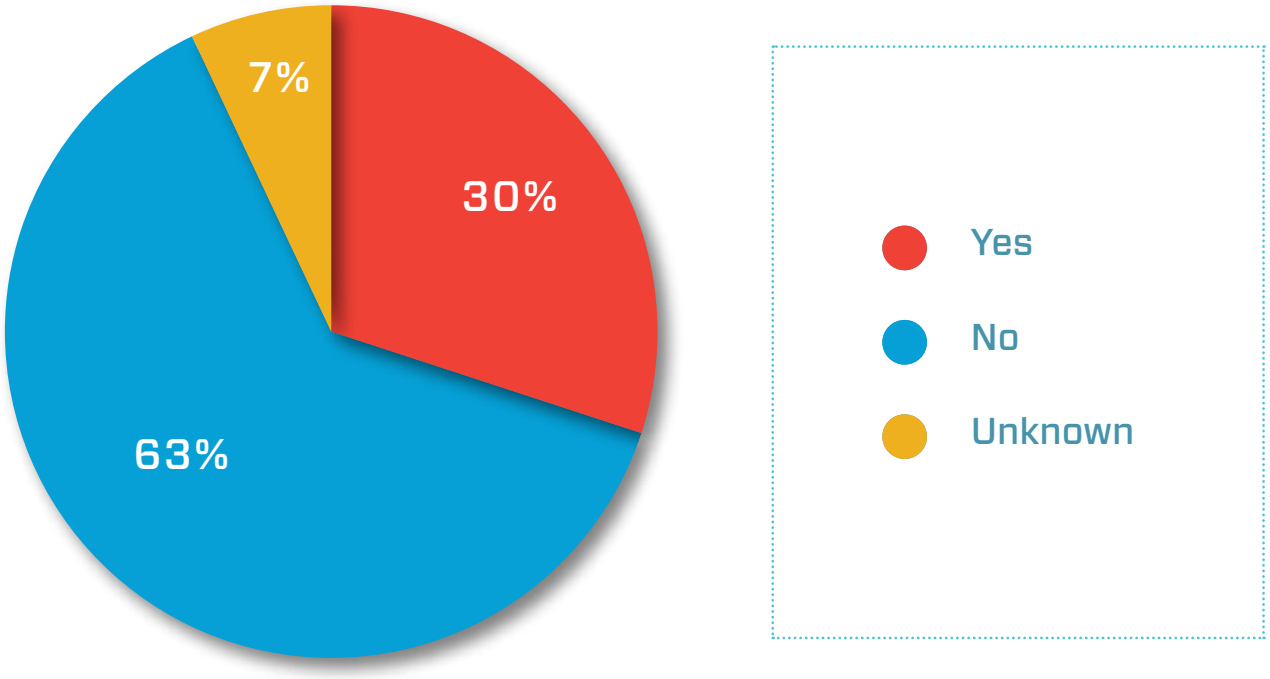
Most of the control system vulnerability patching focus should be placed on the 30% of vulnerabilities which impact exterior-facing systems. Since so many assets and interior control elements are nowhere near a network border, applying patches in the 85% of interior and none-to-medium proximity cases would likely have little to no reduction in risk for impact against attack. However, we caution that this analysis only applies to ICS-related vulnerabilities not underlying traditional operating system patching whose vulnerabilities can lead to worm- like threats and ransomware inside of a control network.

While patching vulnerable field and Purdue layer devices will be rare in practice, and provides little direct benefit due to the insecure-by-design nature of the devices, the sheer percentage of vulnerabilities identified in these devices indicates a decent likelihood of attack should an attacker find its way onto the ICS network. While applying patches to field devices can generally only be performed during a plant outage, providing segmentation such that only valid HMI, EWS, or OPC systems can access the field devices directly, provides a terrific mitigation strategy for defending the interior of the network, should the perimeter be breached. Since accessing the physical process requires sending commands to these controllers, taking a defensive posture can force an attacker to access the HMI or EWS as a step in achieve a process disruption goal. In this way, an end user closes off potential attack vectors to important field devices.

This also highlights the importance of network monitoring at this low level of the network. Since a large amount of security research is performed on these low-level components, it presents a potential source of attack detection via analytics on control protocols – not only in detecting the use of true vulnerabilities in products, but also in the detection of abnormal behavior from the insecure-by-design protocols for manipulating the process.

VULNERABILITIES IN FREE/ACCESSIBLE ICS

2017 ADVISORIES
FREE/DEMO VERSION AVAILABLE



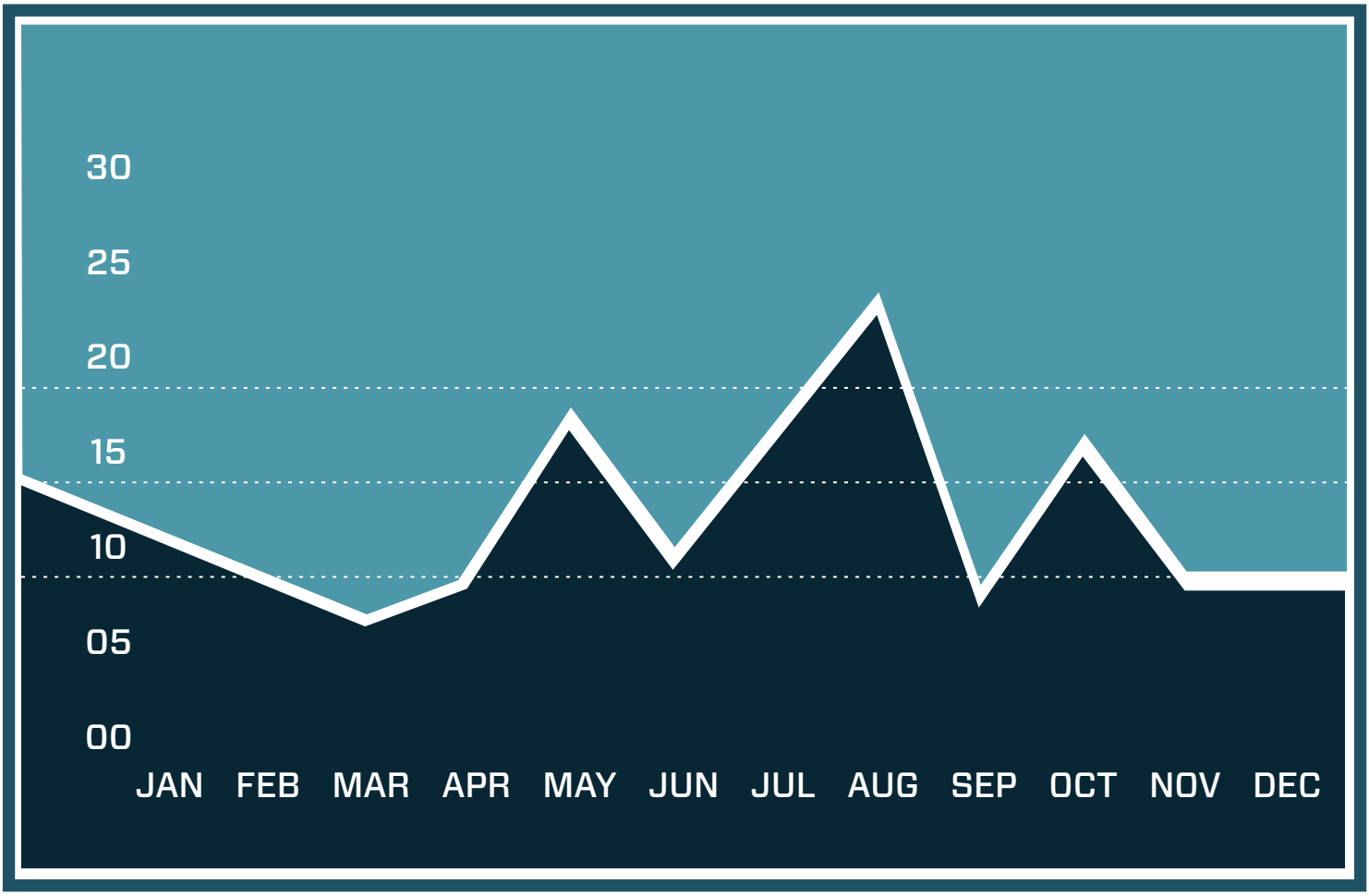
63% of all 2017 ICS-related vulnerabilities were found to affect either ICS hardware or software with no publicly available version (free, demo, etc.)

COMMON MYTH
Most ICS vulnerabilities are uncovered in 'Free' and 'Demo' software that is seldom-used in actual control systems.

DETERMINATION: FALSE
This means that the majority of 2017 ICS-related vulnerabilities are sourced from hardware or software which had to be procured at cost.

VULNERABIITY DISCLOSURES OVER TIME

VULNERABILITIES BY MONTH
OVER 2017



On average, organizations disclosed 14 vulnerabilities monthly through 2017.

Accounting for known conferences and other variables, the disclosure rate remained reasonably flat through 2017.

An increase in ICS-related vulnerability disclosures in July and August most likely coincides with 'conference season' – the BlackHat and DefCon security conferences. This also coincides with the disclosure of MS17-010 impacting Microsoft Windows. Spikes in the Fall season of 2017 coincide with the KRACK vulnerability, when many ICS vendors updated wireless systems.

ALTERNATE MITIGATIONS

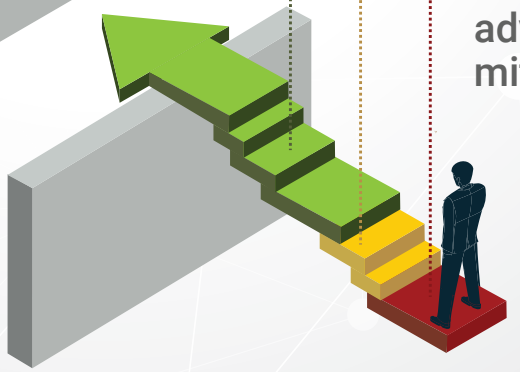
2017 ADVISORIES

ALTERNATE MITIGATION PROVIDED

72%
of advisories provided no alternate mitigation

28%
of all vulnerability advisories did provide an alternate mitigation

12%
of all vulnerability advisories had no mitigation at all



When an advisory only included language such as 'use VPNs and trusted networks', Dragos does not count the advisory as containing an alternate mitigation. To count as including an alternate mitigation, a vulnerability advisory must include specific and reasonable guidance. For instance, a simple description of which network port is impacted by a vulnerability (for network-accessible exploits) or local system configuration changes that can be made by an owner (for local or privilege escalation exploits).

These simple additions arm administrators with the means to limit access to the vulnerable service, and provide the breathing room needed for patch testing and subsequent application.

A sizable percentage of advisories contained neither a patch nor an alternate mitigation for the vulnerabilities mentioned in the advisory. These advisories are effectively useless, providing owners with no actionable data.

DRAGOS

Dragos, Inc. | www.Dragos.com | version 01

1745 Dorsey Road | Hanover, MD 21076 USA | email: info@dragos.com