DRAGOS®

OT Cybersecurity

The 2023 Year In Review

LESSONS LEARNED FROM
FRONTLINE DEFENDERS

Marissa Costa
Jackson Evans-Davies
Hussain Virani
Eddy Wade

Agenda

1 Introductions

2 ICS Incident Response Plan

3 Defensible Architecture

4 ICS Network Visibility & Monitoring

5 Secure Remote Access

6 Risk-based Vulnerability Management

7 Case Studies from the Frontlines

SANS

5 THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

Meet Our Experts

Jackson Evans-Davies
Director of Professional Services

Hussain Virani
Senior Industrial Incident Responder

Eddy Wade
Principal Industrial Consultant

Marissa Costa
Senior Industrial Penetration Tester

Five ICS Cyber Security Critical Controls

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

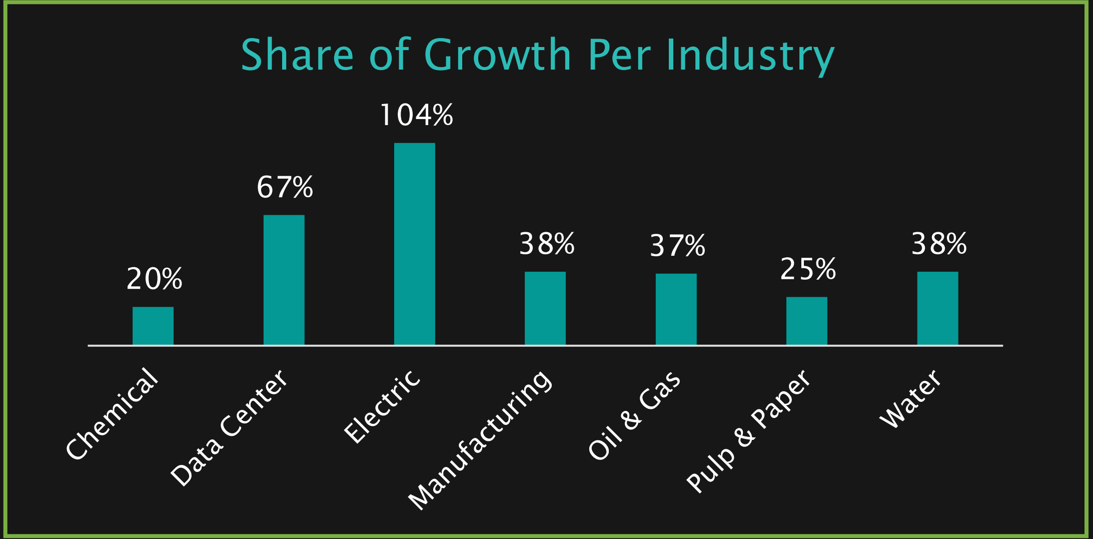
		Reports with findings
01	ICS Incident Response Plan	38%
02	Defensible Architecture	46%
03	ICS Network Visibility & Monitoring	61%
04	Secure Remote Access	29%
05	Risk-based Vulnerability Management	41%

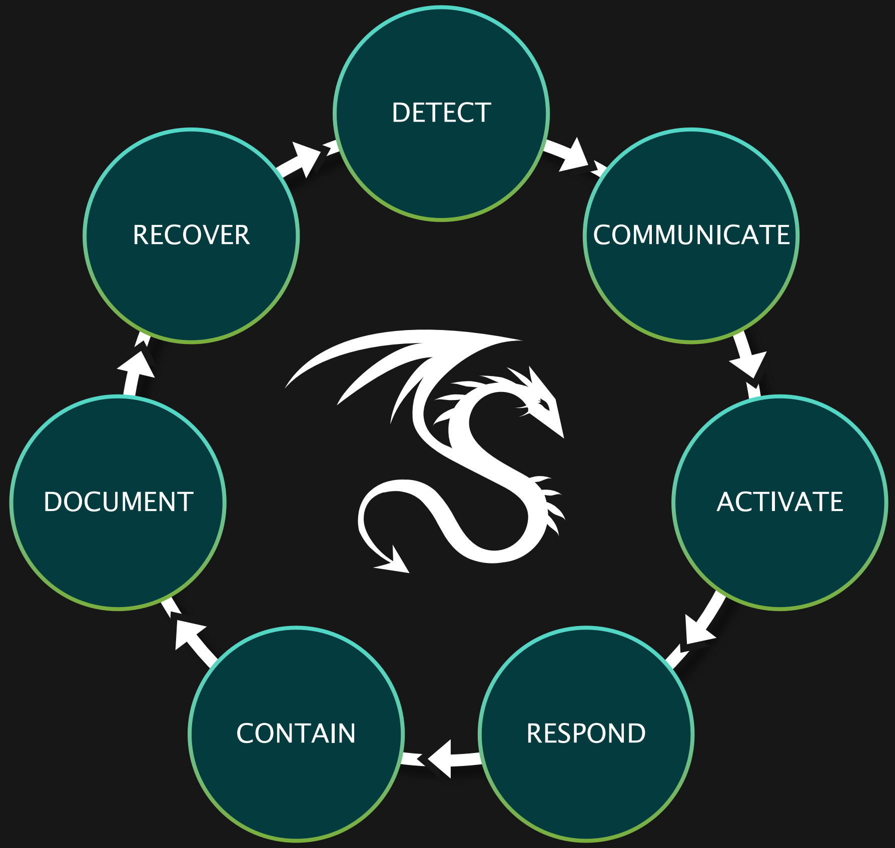
Incident Response (IR) Readiness

INDUSTRY-WIDE SHIFT TOWARD TABLETOP EXERCISE ENGAGEMENTS

Tabletop Exercises

- Best way to test & refine IR plan
- Demonstrate how a realistic attack may occur in your OT environment





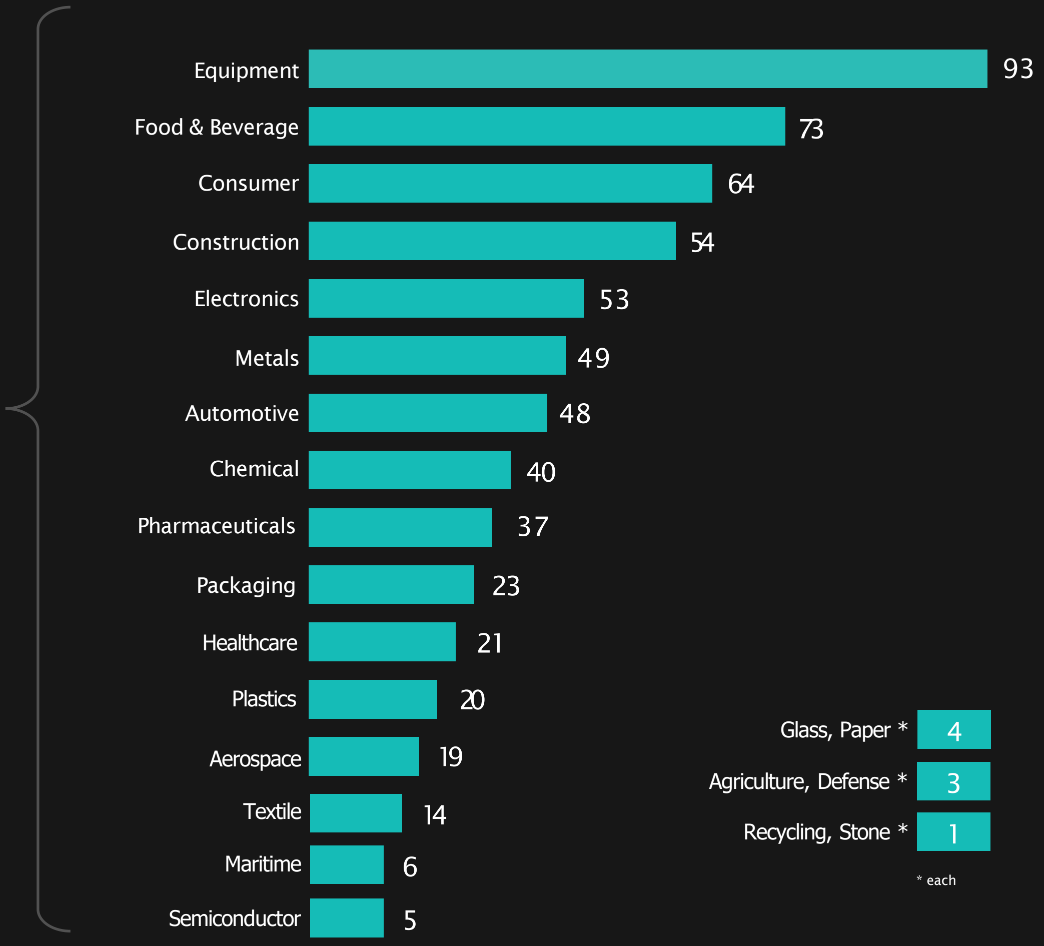
CORE CAPABILITES FOR INCIDENT RESPONSE READINESS

Ransomware Attacks Increased by 50%

LAST YEAR, THERE WERE 905 RANSOMWARE ATTACKS AGAINST INDUSTRIAL ORGANIZATIONS

RANSOMWARE BY ICS SECTOR

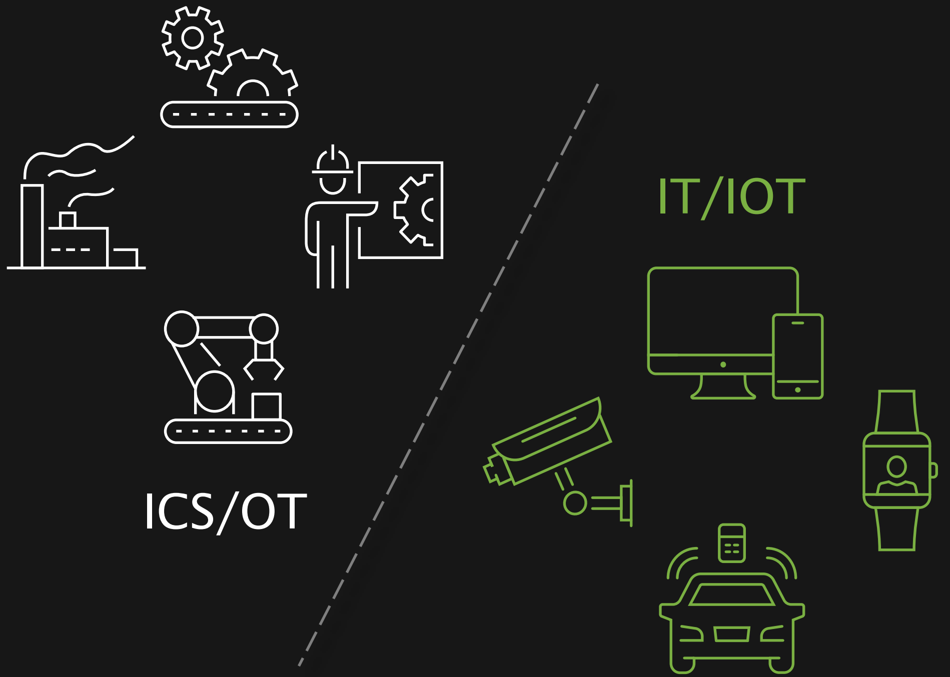
638	Manufacturing
115	Industrial Control Systems
65	Transportation
30	Oil & Gas
20	Electric
13	Mining
10	Water
10	Renewables
2	Government
2	Defense



RANSOMWARE SPREADS IN FLAT NETWORKS
28% of customer engagements had findings of segmentation issues or improperly configured firewalls

Lessons Learned From Customer Engagements

NETWORK SEGMENTATION



28% of Engagements in 2023 Identified Issues with Network Segmentation.

Notable Industries:
Mfg. (58% Engagements),
Transportation (36%)

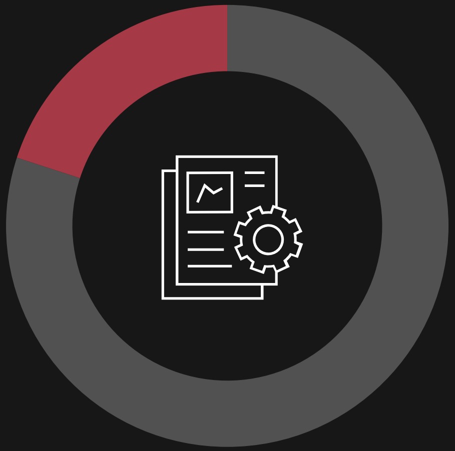
EXAMPLES INCLUDE:

- Lack of an OT DMZ
- Domain Authentication Spanning Zones
- Unsecured External Connectivity
- External DNS Resolvers
- Safety System Segmentation
- Unsafe Historian Architecture

Lessons Learned From Customer Engagements

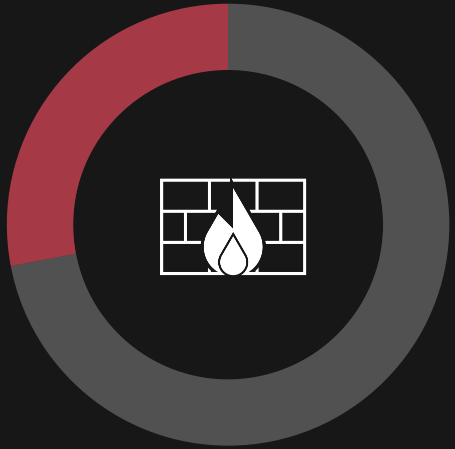
EXTERNAL CONNECTIONS TO OT ENVIRONMENTS

An External Connection is Any Internet Protocol (IP) and/or Asset That Communicated Beyond a Pre-defined Security Perimeter



Dragos issued findings related to external connections in 20% of assessment reports in 2023

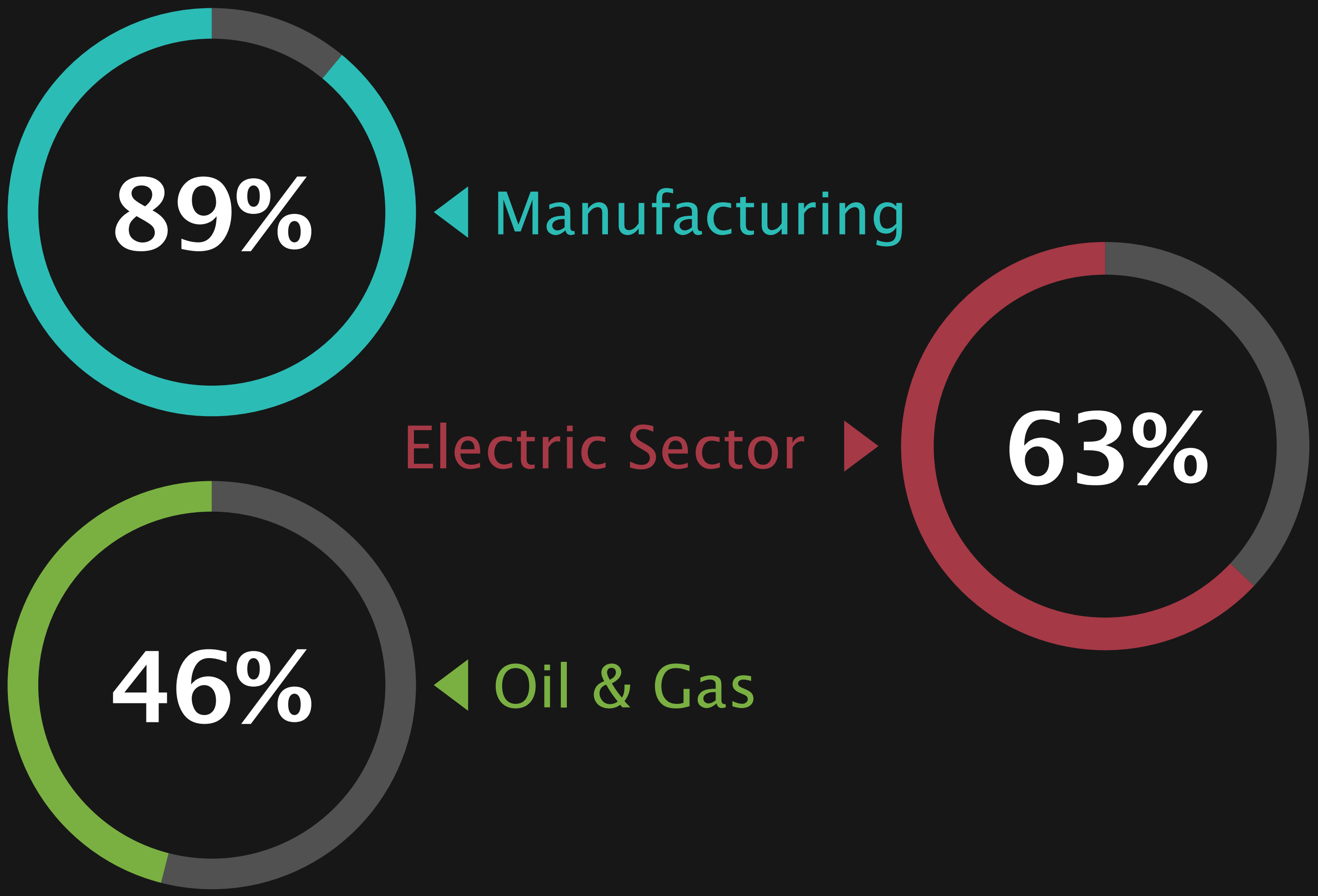
Dragos identified firewall weaknesses in 28% of assessment reports in 2023



Lessons Learned From Customer Engagements

LIMITED OR NO ASSET VISIBILITY

61% of Service Engagements in 2023 had Findings Related to Network or Asset Visibility

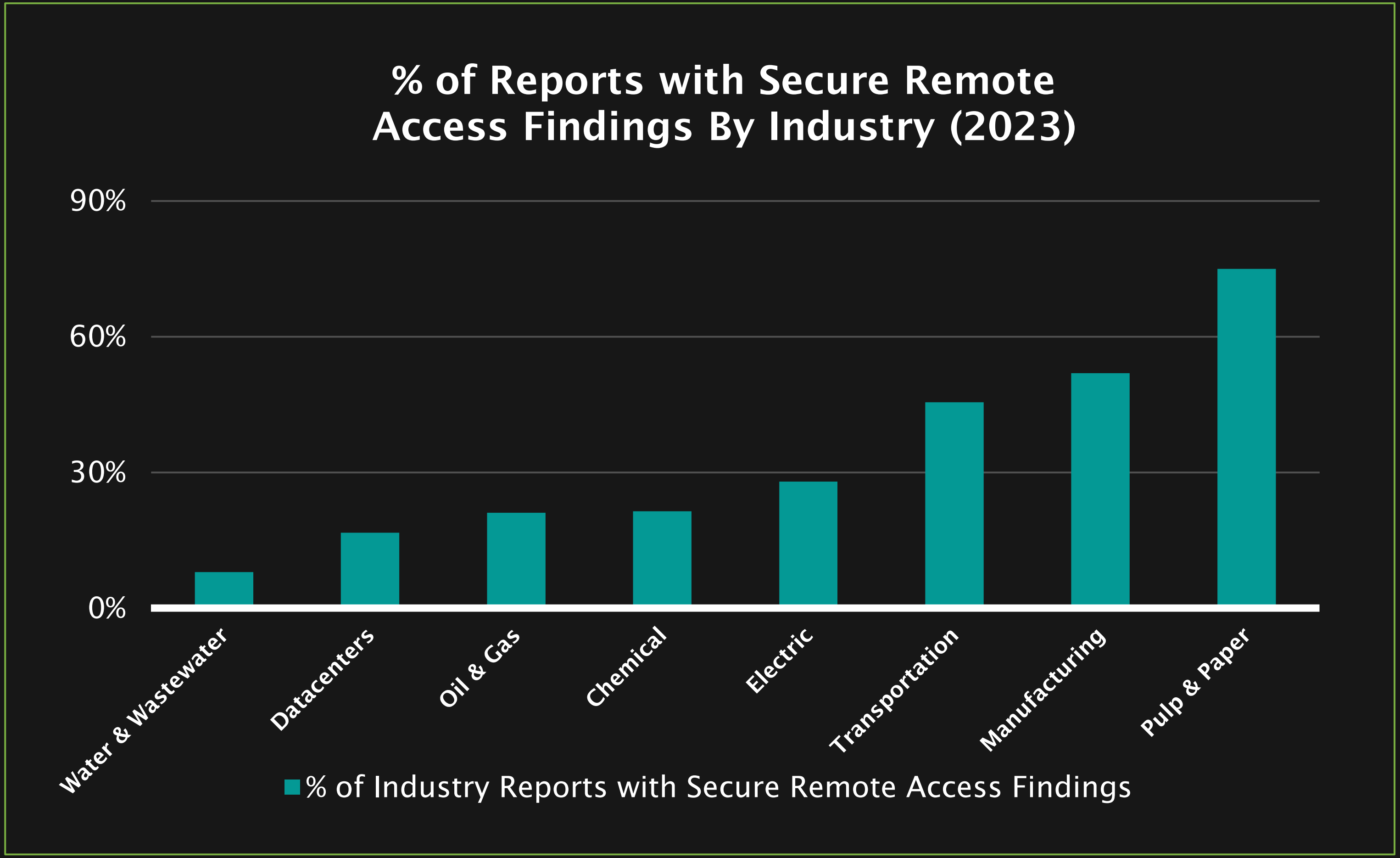


Lessons Learned From Customer Engagements

SECURE REMOTE ACCESS

Common SRA Findings:

- Lack of Multi-Factor Authentication
- Insecure Remote Access Configuration
- Remote Service Session Hijacking Vulnerabilities
- Insecure/Unrestricted File Transfer
- Unmonitored Permanent Vendor Connections



Lessons Learned From Customer Engagements

RISK-BASED VULNERABILITY MANAGEMENT

Almost half (41%) of Dragos 2023 assessment reports included vulnerability related findings.

Key Examples:

- No Vulnerability Mgmt. Program
- Unpatched Perimeter Devices (e.g. Firewalls)
- Industrial Control System Vulnerabilities
- Various *years old* vulnerabilities indicating a lack of maintenance
- Vulnerabilities exploited in penetration tests such as Windows *PrintNightmare*

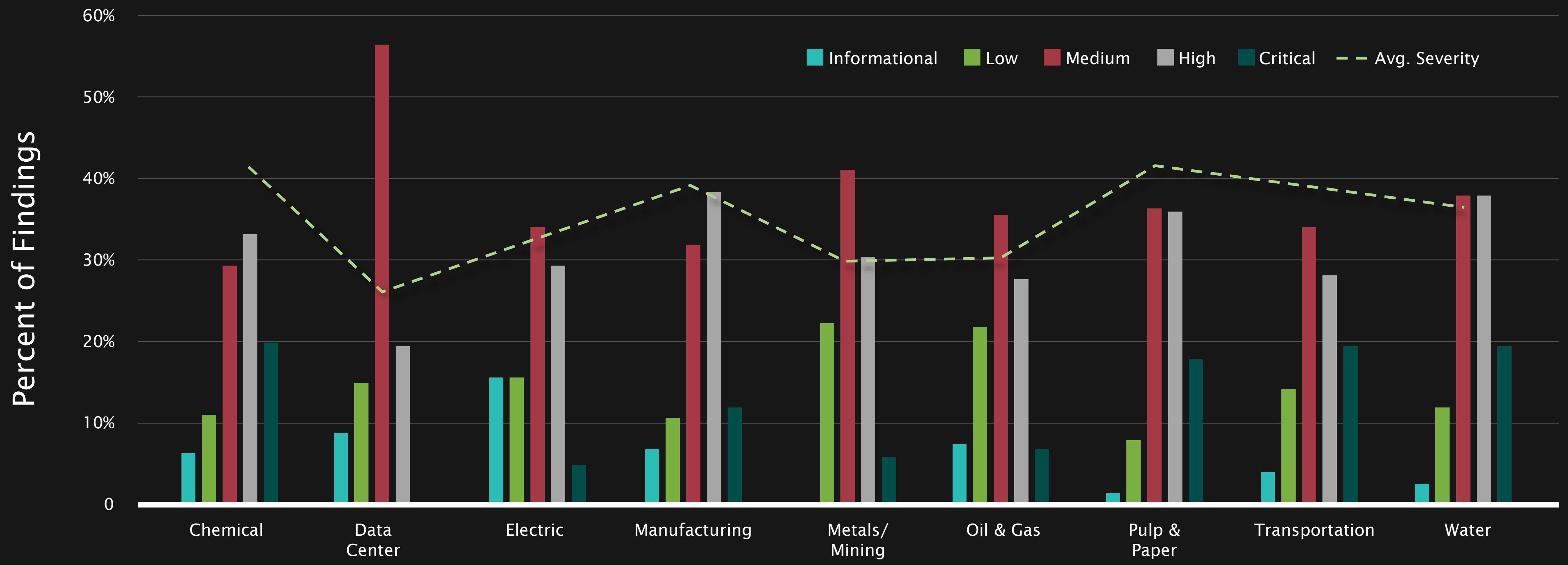
3% of ICS/OT Vulnerabilities Needed to be Addressed **NOW**

68% Need to be Addressed **NEXT**

29% Likely **NEVER** Need to be Addressed

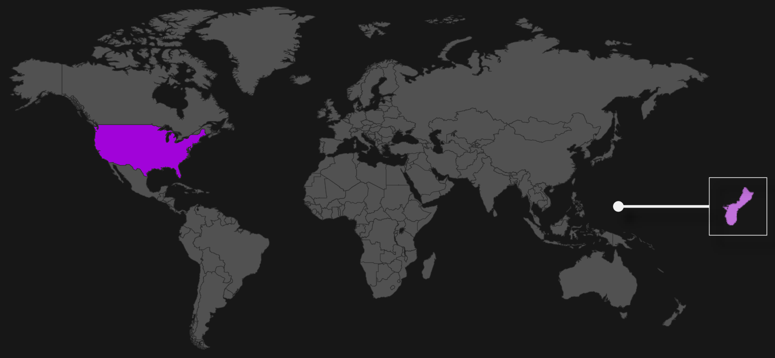
Lessons Learned From Customer Engagements

OVERALL REPORT SEVERITY BY INDUSTRY



Voltzite

VOLTZITE EXFILTRATION COULD FACILITATE FOLLOW-ON ACTIONS WITH PHYSICAL IMPACTS



Heavy use of living off the land (LOTL) techniques. Evades detection with slow, steady reconnaissance.

TARGETS:
Electric Power Generation, Transmission & Distribution, Emergency Services, Telecommunications, Defense Industrial Bases, Satellite Services

INTENT/MOTIVATION:
Espionage & exfiltration, long-term persistent access.

KILLCHAIN ANALYSIS		CAPABILITIES
Delivery	STAGE 01	Exploits internet accessible SOHO routers, uses them as intermediary hops back to ORB
Exploit	STAGE 01	Native Windows command line and PowerShell, Active Directory tools
Install/Modify	STAGE 01	Use of built-in proxy commands, open-source tools, & fast reverse proxy tool (frp)
C2	STAGE 01	Initial access by exploiting edge network devices from Cisco, Ivanti, PRTG Network Monitor, Fortinet amongst others
Act	STAGE 01	Stages and exfiltrates sensitive operational data related to OT networks and processes

Overlaps with Volt Typhoon (Microsoft), BRONZE SILHOUETTE (Secureworks), Vanguard Panda (Crowdstrike), UNC3236 (Mandiant)

Living Off the Land (LOTL) Attacks

THREAT GROUPS USING LOTL TECHNIQUES

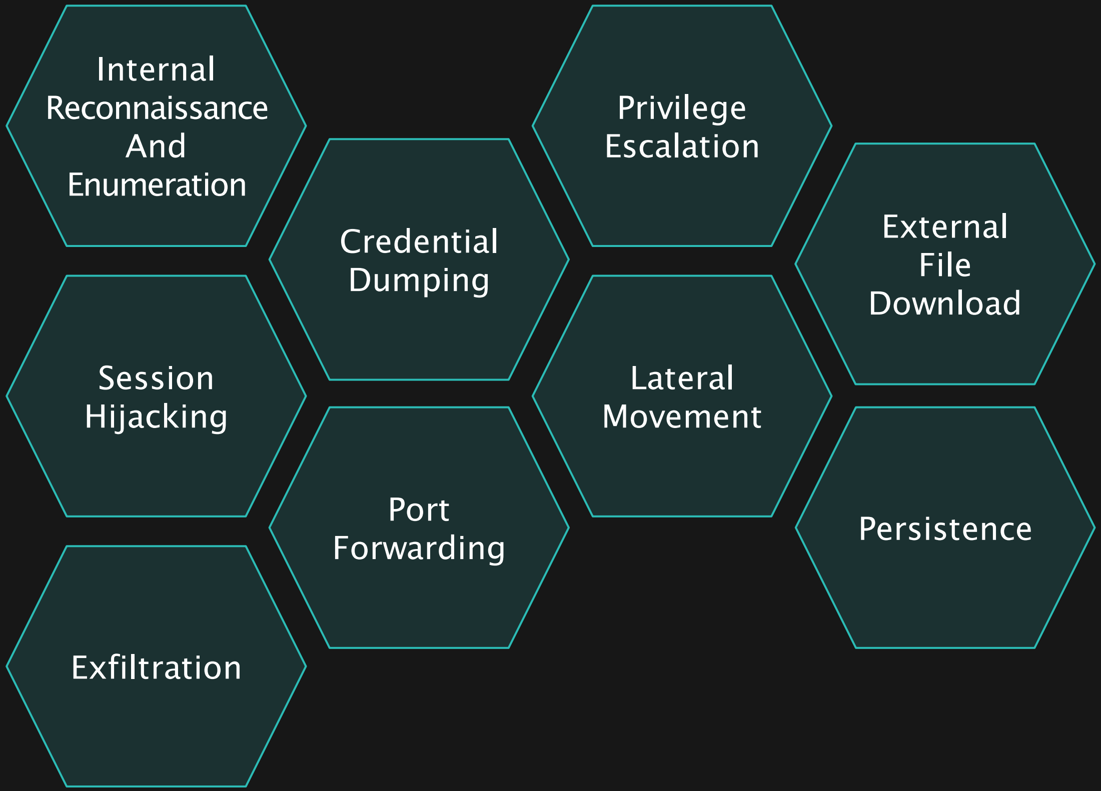
↓

Fileless Attacks Using Tools Native to Victim Environments

Evade Detection

Persist Longer

RANSOMWARE GROUPS USE LOTL TECHNIQUES TO ESCALATE PRIVILEGES, GAIN PERSISTENCE, & ESTABLISH C2 CHANNELS



Internal Reconnaissance And Enumeration

Credential Dumping

Privilege Escalation

External File Download

Session Hijacking

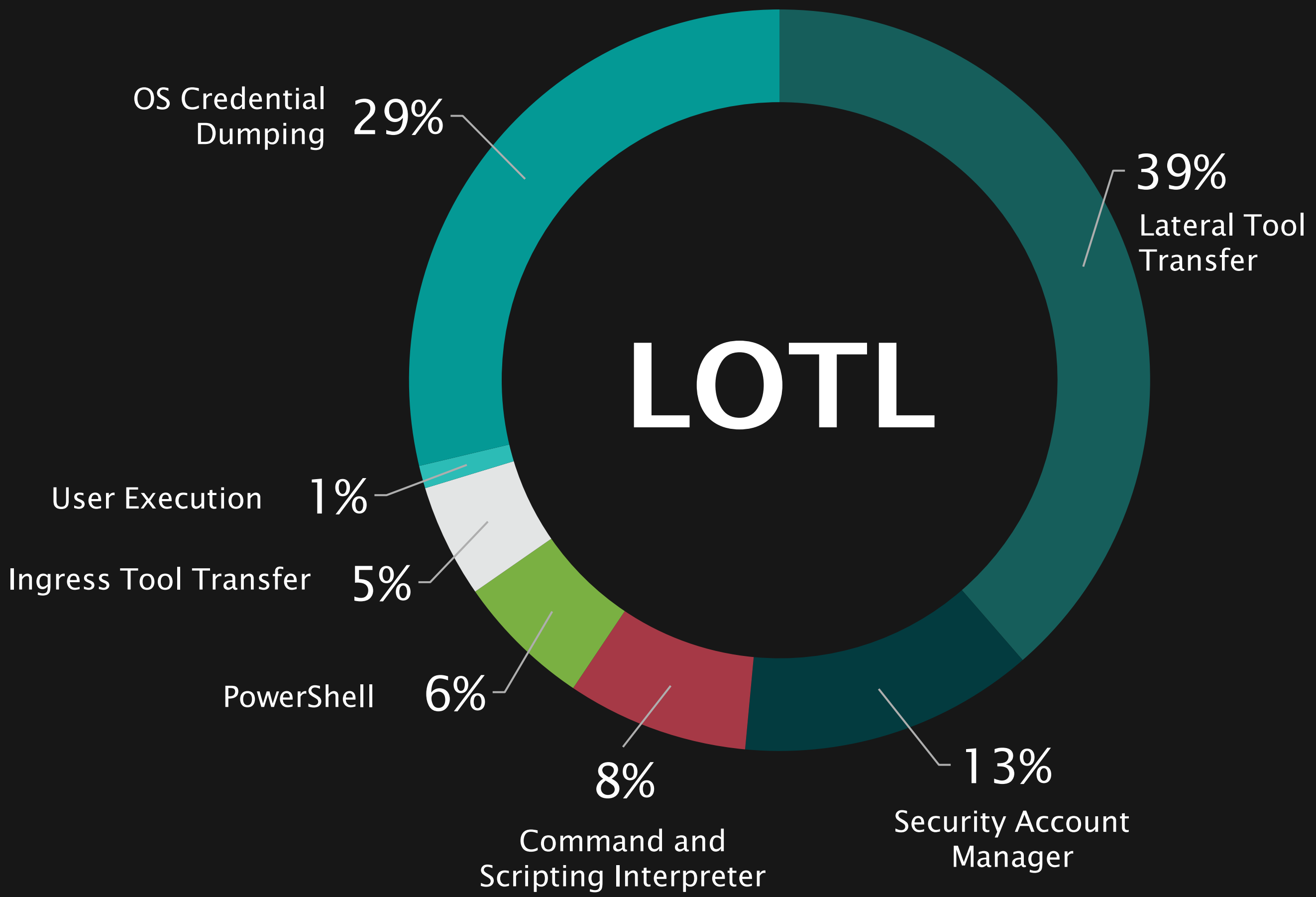
Lateral Movement

Port Forwarding

Persistence

Exfiltration

Living Off the Land (LOTL) Techniques



RESULTS FROM DRAGOS PROFESSIONAL SERVICES PENETRATION TESTING

Network Penetration Test – LOTL Case Study

IT to OT Perimeter Assessment

1. Collected IT Domain Hashes from previous Pentest (dump.txt)
2. Privilege Escalation & Persistence using NetExec
3. RDP Session Hijacking (tscon.exe & shadow support)

OT Assessment

1. Gain Persistence using Hijacked Access
2. Disable Workstation AV
3. Collect Local Hashes via Taskmgr.exe (lsass.dmp)
4. Upload Mimikatz.exe and Psexec.exe over RDP
5. Pass-the-Hash using Mimikatz.exe and Psexec.exe
   a) Lateral Movement (same network) via SMB
   b) Pivot (new networks and security zones) via SMB

Recommendations

SANS

5

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Visibility & Monitoring

04
Secure Remote Access

05
Risk-based Vulnerability Management

Q&A

QUESTIONS AND ANSWERS

ENHANCE YOUR OT THREAT PREPAREDNESS.

Download the Report:
dragos.com/year-in-review