DRAGOS

WHITEPAPER

Phosphorus Intelligent Active Discovery

An accurate, fast, and safe solution for high-fidelity **x**IoT asset visibility.

Phosphorus
A DRAGOS COMPANY

Intelligent Active Discovery Whitepaper

INTRODUCTION

A New Generation of xIoT Asset Discovery & Risk Assessment

The Phosphorus **x**IoT Security and Management Platform, now part of the Dragos portfolio, is powered by the industry's first and only scalable Intelligent Active Discovery engine that is fast, accurate, and safe across a wide variety of extended Operational Technology (xOT) asset classes, including enterprise IoT devices, OT and ICS devices, IoMT devices, IIoT devices, and other embedded devices. The patented Phosphorus approach intelligently calibrates the platform's device interactions, dynamically adjusting discovery parameters such as probe sequencing, packet rates, ports in scope, and more – while ensuring that assets are fully classified with speed, safety, and minimal network impact.

Note: Phosphorus does not use MAC addresses for any aspect of our asset classification process.

Three Foundations of The Phosphorus Approach

01 **Complete Visibility**

All **x**IoT devices discovered through active polling, not traffic monitoring. Deterministic discovery means first-time and accurate classification.

02 **Deep Discovery**

Unmatched high-resolution device detail with granular risk assessment and deep device metadata, all without hardware, agents, or complexity.

03 **Zero Disruption**

Safety is the foundation of our platform. Devices are discovered and classified without operational impact on mission-critical, life-critical, and other sensitive cyber-physical devices.

THE CHALLENGE

Legacy Passive Solutions Can't Keep Up

Legacy passive solutions in the market depend on network monitoring to perform discovery. The Phosphorus approach does not depend on SPAN port traffic analysis for asset discovery. As a result, it doesn't suffer from the many limitations of legacy passive solutions — including limited visibility, incomplete or inaccurate inventory (e.g., OUI lookup-based solutions), slow discovery with long mean-time-to-inventory, network performance impact with strain on network resources, and the deployment complexity associated with configuring and maintaining SPAN ports.

Legacy Approach	Phosphorus Approach
✕ **Dangerous, Brute Force Scanning** Overwhelms devices, often causing harm and interruption.	✓ **Safe, native communication** No reckless scanning. Only safe and intelligent active xIoT discovery using native device protocols.
✕ **Assumption-Based Analysis** Often results in lower confidence & speculation. Not sufficient for device remediation.	✓ **Evidence-Based Analysis** No guesswork here. 99% = 0%. 100% device certainty the first time.
✕ **Infrastructure Dependencies** SPANs & TAPs — requiring big network switching investments.	✓ **No Infrastructure or Agents** Software-based and agentless. Can be deployed on-prem or in the cloud in minutes.
✕ **Unscalable Manual Effort** Slow, complex, error-prone, costly, and manual.	✓ **Automated and Scalable** Discovers faster, uses fewer resources, & collects more granular data.
✕ **No remediation** No built-in remediation. Can only isolate using VLANs, which is complex & expensive.	✓ **Full Remediation** Goes beyond discovery to full risk remediation for passwords, firmware, certs, insecure configurations.

REAL-WORLD EXAMPLES

The Fastest xIoT Discovery, With Immediate Results

In multiple large critical-infrastructure environments, Phosphorus safely provided a full inventory of IoT, OT, IoMT, and IIoT footprints in minutes or hours, while legacy passive solutions only returned a partial (and inaccurate) inventory in several days or weeks. Phosphorus has become the solution of choice for enterprises with large, multi-homed, highly segmented, and global networks — especially given the ease with which we accommodate physically segmented or air-gapped sites into our centralized management console.

~4 min

Global 500 machinery & robotics conglomerate

xIoT Discovery across a select customer network.

~11 min

Leading managed healthcare consortium

xIoT Discovery across a select customer network.

~8 min

Leading agricultural machinery manufacturer

xIoT Discovery across a select customer network.

~12 min

Large energy & exploration company

xIoT Discovery across a select customer network.

MAJOR DIFFERENTIATORS

The Phosphorus Difference

The platform's foundational device-interaction layer is the major differentiator. The layer facilitates direct communication with embedded devices in both authenticated and unauthenticated mechanisms, utilizing their native protocols in a scalable, extensible manner. The patented Phosphorus approach provides active discovery technology that is inherently attuned to the nuances of the deployment environment.

Intelligent Active Discovery dynamically adjusts probe sequencing, packet rates, and ports in scope while ensuring assets are fully classified with speed, safety, and minimal network impact. Asset-discovery jobs use dynamic, self-calibrating "Agendas" that ensure safety regardless of whether the **x**IoT assets are in Healthcare, Manufacturing, Data Centers, Retail and Hospitality, critical infrastructure, or other mission-critical environments. This proprietary and patented Agenda system underpins the technology's built-in safety mechanism.

COVERAGE & SCALE

Built For Device Diversity. And Ultra-Fast.

1200+

Optimized for Device Diversity

Phosphorus covers more than **1,200** different IoT, OT, IoMT, and IIoT device vendors and manufacturers. The patented Phosphorus "Genus-Species" approach means that more than 1 million unique device models are covered.

Hours

Built for Rapid Expansion

Net-new **x**IoT device coverage can be added in a matter of hours, regardless of the device type or vendor. As the need arises, the extensible **x**IoT Security and Management platform can seamlessly add net-new capabilities.

MINIMAL IMPACT. MAXIMUM RESULTS.

Far More Efficient Than Hardware-Based Legacy Solutions

Phosphorus Intelligent Active Discovery is far more efficient than hardware-based legacy solutions that strain network resources. Our software-based solution has no network performance impact and sends a fraction of the traffic compared to legacy passive solutions.

SAFETY FIRST

Finally — xIoT Discovery That's Safe

Safety is the foundation of our platform. Devices are fully classified without operational impact on more sensitive, mission-critical, and life-critical devices. With full control over Intelligent Active Discovery, you set the Agenda so you can safely find every connected device.

✓ **ZERO Disruption**
Devices are discovered and fully classified with ZERO disruption.

✓ **Customized Discovery Agendas**
Customized Discovery Agendas enable tiered probe sequences to ensure safety.

✓ **Safely discover all xIoT devices**
Safely discover even the most sensitive, legacy, & critical OT, ICS, & IoMT devices.

High-Resolution xIoT Asset Discovery

Get more device metadata and context than ever before — including the make, model, firmware version, and whether the device is end-of-life or even banned. Phosphorus provides the following high-fidelity asset attributes:

- Device Type
- Manufacturer
- Model/Series
- IP
- MAC
- Device Identifier
- Serial Number
- Model Number
- Firmware Version
- Active Protocols
- Open Ports
- Active Services
- Device Family-Specific Detail
- Device Manufacturer-Specific Detail
- Password Configuration

RISK ASSESSMENT

In-Depth xIoT Risk Assessment & Alerts

Beyond device detail, you'll see the state of things with in-depth Risk Assessment information generated as part of the device-interrogation process.

- **Default Passwords**
  Device is still running default passwords.
- **Insecure Configuration**
  Device is running with an insecure configuration.
- **Vulnerable Firmware**
  The active firmware version has known vulnerabilities.
- **Out-of-Date Firmware**
  A newer firmware version is available.
- **Expired Certificate**
  Device certificate needs renewal or replacement.
- **Discontinued Device**
  Device has been marked End-of-Life by the manufacturer.
- **Firmware Changed**
  Suspected tampering: firmware changed out of band.
- **Password Reset**
  Suspected tampering: password reset to default.
- **Prohibited Device**
  A U.S. Government-prohibited device was discovered.

Metadata That Adapts To Every Device Family

The unique Phosphorus approach means the set of "Device Metadata" changes across device families, with a large set of details that can only be determined by direct interaction with the **x**IoT asset. For reference, note the differences between the metadata generated for an IP camera and a programmable logic controller (PLC):

IP Camera

Axis M3104-LVE

Workplace IoT / surveillance class — camera-specific metadata such as streaming protocols, codecs, and firmware posture surfaced through native interrogation.

PLC

Allen-Bradley 1756-L83E/B

OT / ICS controller class — controller-specific metadata such as backplane modules, firmware revision, and protocol services unique to the PLC family.

CONTEXT IS KING

Focus On The Vulnerabilities That Matter Most

Managing vulnerabilities without full context can be a daunting task. The Phosphorus Platform enriches device data with CISA's Known Exploited Vulnerabilities (KEV) catalog and FIRST's Exploit Prediction Scoring System (EPSS). This combination delivers real-world context and predictive insight to help CISOs, CIOs, and device owners focus on the vulnerabilities that matter most.

CISA KEV

Known Exploited Vulnerabilities

Real-world evidence of vulnerabilities actively being exploited in the wild — grounding prioritization in confirmed adversary behavior rather than theoretical severity.

FIRST EPSS

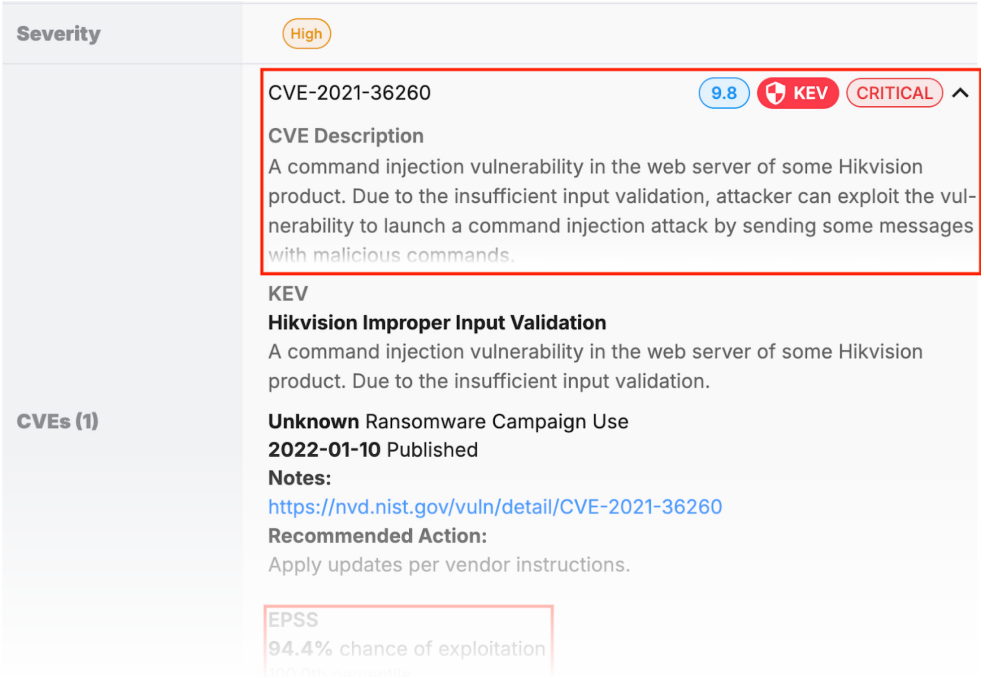
Exploit Prediction Scoring System

Predictive scoring of the likelihood that a vulnerability will be exploited — adding forward-looking insight that complements confirmed exploitation data.

KEV+EPSS

Combined, KEV and EPSS deliver real-world context and predictive insight — turning an overwhelming vulnerability backlog into a focused, defensible remediation plan.

Source: phosphorus.io/context-is-king-understanding-and-reducing-xiot-risk-with-kev-and-epss



OUR PLATFORM

Don't Just See Risks. Eliminate Them.

Phosphorus Intelligent Active Discovery is just one part of the industry's only **x**IoT Security and Management Platform that takes you from complete visibility to complete remediation. Most IoT and OT security tools stop at visibility, leaving remediation as a manual and overwhelming burden for already-stretched teams.

Phosphorus was built to close this gap. By unifying discovery, risk assessment, automated remediation, and continuous monitoring, the platform enables organizations to not only identify device risks but also fix them at scale — safely, efficiently, and without disrupting operations.

Discover & Assess

Safely discover, classify, and assess all **x**IoT devices in minutes, with no expensive hardware, SPANs, TAPs, or packet brokers.

Harden & Remediate

Automatically remediate **x**IoT device vulnerabilities, including credentials, firmware, certificates, & risky configurations.

Monitor & Manage

Continuously monitor and manage all **x**IoT devices, while detecting and responding to device drift.

Full-Lifecycle Remediation

The Phosphorus Platform automates discovery and risk assessment, device hardening and remediation, and continuous monitoring and management for every connected device. It provides capabilities such as:

- ✓ Rotating Passwords and Credentials
- ✓ Patching Firmware
- ✓ Managing Certificates
- ✓ Managing Configurations
- ✓ Removing Banned or Risky Devices

With flexible scheduling, remediation can be automated across thousands of devices or applied individually within defined maintenance windows — keeping organizations in control.

OUR PLATFORM

Continuous Device State Monitoring & Management

Continuously monitoring for device drift is central to maintaining the security and stability of IoT, OT, IoMT, and IIoT environments. As cyber-physical systems evolve, even small configuration changes, expired certificates, outdated firmware, or unauthorized adjustments can create critical security gaps.

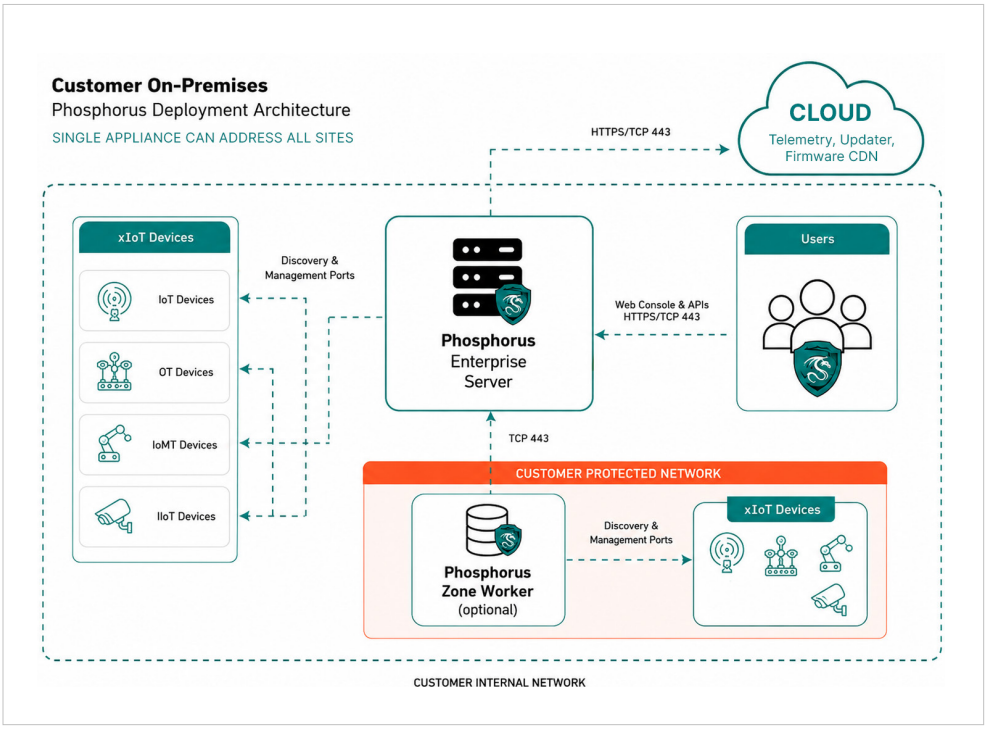
The Phosphorus platform continuously tracks these changes to detect drift. By automatically identifying and allowing remediation directly in the platform — whether through credential rotation, firmware patching, or configuration enforcement — Phosphorus ensures devices remain compliant, resilient, and secure at scale. This proactive approach helps organizations prevent vulnerabilities from creeping back in, while reducing operational overhead and minimizing disruption to essential systems.

Flexible Deployment

Phosphorus can be deployed on-premises, in the cloud, or in a hybrid deployment. A lightweight Zone Worker extends discovery and monitoring into segmented and air-gapped sites, all managed from a centralized console.

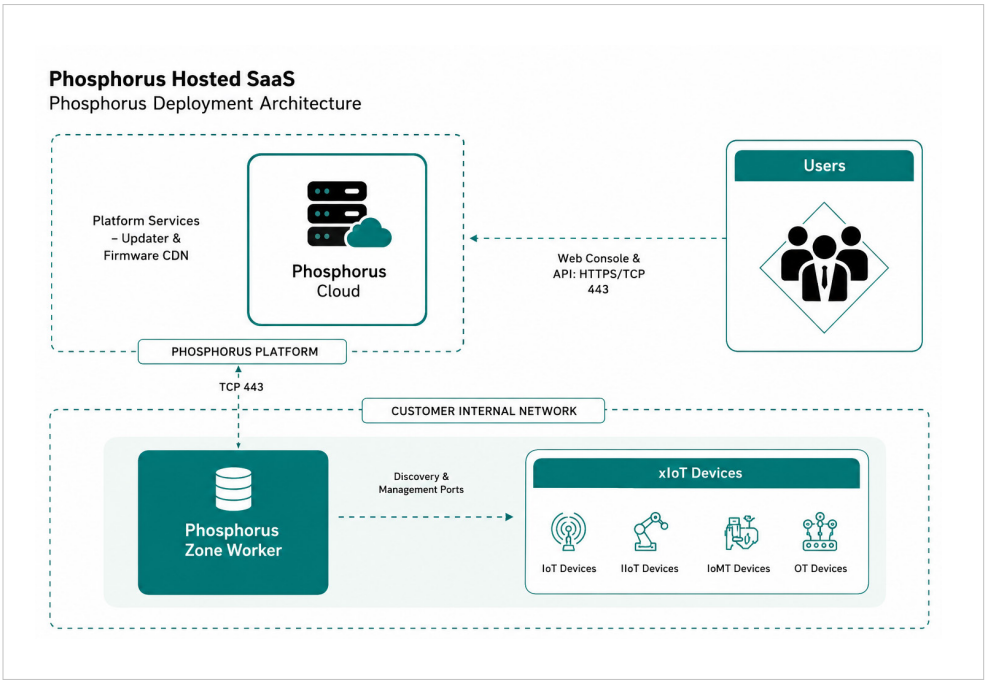
ARCHITECTURE

Customer On-Premises Deployment



ARCHITECTURE

Hosted SaaS Deployment



AGENDA OVERVIEW · APPENDIX

Standard xIoT Enterprise Discovery

Phosphorus Agendas intelligently calibrate the platform's device interactions — dynamically adjusting probe sequencing, packet rates, ports in scope, and more — while ensuring assets are fully classified with speed, safety, and minimal network impact. These customizable Agendas ensure asset safety regardless of whether targets are in Financial Services, Transportation, Healthcare, Manufacturing, Data Centers, or other critical-infrastructure environments, by factoring in the presence of sensitive devices early in the tiered approach.

The standard **x**IoT enterprise discovery is the default Phosphorus Active **x**IoT Discovery Agenda, employing a tiered approach to progressively discover **x**IoT devices in your environment. This Agenda stops sending traffic to a device once it is deemed fully classified, and is intended for use with specific IP ranges. The following details the protocols in scope at each Tier.

AGENDA OVERVIEW

Tier 0

PROTOCOL / PROBE	PORTS
ARP	--
ICMP	--

AGENDA OVERVIEW

Tier 1

PROTOCOL / PROBE	PORTS
BACnet	47808
TCP SYN	102, 502, 5094, 9999, 44818

AGENDA OVERVIEW

Tier 2

PROTOCOL / PROBE	PORTS
SNMP v2	--
S7	--
SIP	--
ENIP	--
HART IP	--
Modbus	--
NETBIOS	--
Telnet	9999
TCP SYN	21, 22, 23, 80, 443, 8443

AGENDA OVERVIEW

Tier 3

PROTOCOL / PROBE	PORTS
SNMP v1	--
SNMP v3	--
FTP	--
SSH	--
TCP	80
TLS	443, 8443
Telnet	23

PROTOCOL / PROBE	PORTS
TCP SYN	1200, 2455, 18245, 18519, 1911, 2222, 3500, 4545, 4911, 5007, 5015, 8080, 8081, 9600, 65535
IEC61850MMS	102

AGENDA OVERVIEW

Tier 4

PROTOCOL / PROBE	PORTS
Bachmann	3500
BACnet	47809, 47810
BAEWR	--
Crestron	--
CODESYS 2	--
DeltaV	--
FINS	--
FOX	--
GE SRTP	18245, 18519
GOT2000	--
MDNS	--
MELSECQ	--
OpenProtocol	--
Profinet	--

PROTOCOL / PROBE	PORTS
RDNS	--
SLMP	--
TCP	80, 102, 8080, 8081, 44818, 65535
TLS	443, 8443
TCP SYN	280, 554, 593, 789, 832, 981, 1311, 1443, 1947, 1962, 2443, 3443, 4443, 5000, 5001, 5060, 5061, 5443, 5985, 5986, 6443, 7002, 7443, 8000, 8008, 8088, 8333, 8403, 8888, 9080, 9443, 16080, 20547
Totalflow	--
UPnP	--
WSD	--

AGENDA OVERVIEW

Tier 5

PROTOCOL / PROBE	PORTS
HTTP	80, 8080, 8081
TLS	443, 8443
iLO	--
Redfish	--
RTSP	--
DHIP	--
TCP	280, 593, 1947, 1962, 5000, 5060, 5061, 5985, 8000, 8008, 8088, 8403, 8888, 9080, 16080

PROTOCOL / PROBE	PORTS
TLS	832, 981, 1311, 1443, 2443, 3443, 4443, 5001, 5443, 5986, 6443, 7002, 7443, 8333, 8403, 9443
KNX	--

AGENDA OVERVIEW

Tier 6

PROTOCOL / PROBE	PORTS
PCWorx	--
ProConOS	--
Crimson3	--
HTTP	280, 593, 1947, 5985, 8000, 8008, 8088, 8403, 8888, 9080, 16080
TLS	832, 981, 1311, 1443, 2443, 3443, 4443, 5000, 5001, 5443, 5986, 6443, 7002, 7443, 8333, 8403, 9443
TCP SYN	25, 53, 69, 79, 81, 85, 88, 111, 113, 123, 135, 137, 139, 161, 179, 389, 445, 500, 513, 515, 623, 631, 783, 902, 1090, 1300, 1494, 1720, 1900, 2049, 2082, 2100, 2103, 2199, 2380, 2598, 3389, 3702, 4000, 5250, 5353, 5355, 5555, 5560, 5900, 5901, 6000, 6060, 6542, 7474, 7700, 7787, 7801, 8009, 8012, 8089, 8090, 8197, 8300, 8545, 8834, 9002, 9100, 9197, 9200, 10000, 10001, 10009, 10050, 11000, 12000, 14330, 20000, 20111, 23472, 28222, 30000, 30718, 41794, 47001, 49152, 50000
SIP	--

AGENDA OVERVIEW

Tier 7

PROTOCOL / PROBE	PORTS
ATG	--
Cognex	--
DNS	--
IPP	--
H323	--
SMB	--
LANE POS	--
PAX POS	--
ADDP	--
ROC	--
TCP	25, 53, 69, 79, 81, 85, 88, 111, 113, 123, 135, 137, 139, 161, 179, 389, 445, 500, 513, 515, 623, 631, 783, 902, 1090, 1300, 1494, 1720, 1900, 2049, 2082, 2100, 2103, 2199, 2380, 2598, 3389, 3702, 4000, 5000, 5250, 5353, 5355, 5555, 5560, 5900, 5901, 5985, 6000, 6060, 6542, 7474, 7700, 7787, 7801, 8009, 8012, 8089, 8090, 8197, 8300, 8545, 8834, 9002, 9100, 9197, 9200, 10000, 10050, 11000, 14330, 20000, 20111, 23472, 28222, 30000, 30718, 41794, 47001, 49152, 50000

PROTOCOL / PROBE	PORTS
TCP SYN	7, 9, 13, 17, 19, 37, 49, 82, 83, 84, 107, 110, 143, 264, 465, 512, 548, 587, 617, 636, 705, 771, 873, 888, 910, 912, 921, 993, 995, 1000, 1024, 1030, 1035, 1080, 1089, 1098, 1099, 1100, 1101, 1102, 1103, 1128, 1158, 1199, 1211, 1220, 1234, 1241, 1352, 1433, 1440, 1521, 1533, 1581, 1582, 1604, 1723, 1755, 1811, 1883, 2000, 2083, 2121, 2181, 2200, 2207, 2323, 2332, 2362, 2375, 2379, 2381, 2525, 2533, 2601, 2604, 2638, 2809, 2947, 2967, 3000, 3037, 3050, 3057, 3128, 3200, 3217, 3273, 3299, 3306, 3311, 3312, 3351, 3460, 3500, 3628, 3632, 3690, 3780, 3790, 4322, 4433, 4444, 4445, 4567, 4659, 4679, 4730, 4840, 4848, 5038, 5040, 5051, 5222, 5247, 5400, 5432, 5433, 5554, 5580, 5601, 5631, 5632, 5666, 5672, 5800, 5938, 5984, 6001, 6002, 6050, 6080, 6101, 6112, 6262, 6379, 6502, 6503, 6660, 6667, 6905, 7001, 7071, 7077, 7080, 7144, 7210, 7580, 7680, 7777, 7778, 7800, 7879, 8014, 8023, 8028, 8087, 8095, 8161, 8180, 8205, 8222, 8400, 8686, 8800, 8880, 8883, 8899, 8901, 8902, 8903, 9000, 9042, 9060, 9081, 9084, 9090, 9092, 9111, 9160, 9300, 9527, 9530, 9595, 9809, 10008, 10023, 10051, 10080, 10098, 10443, 11099, 11211, 12345, 12397, 15672, 18264, 19810, 20010, 20171, 20222, 22222, 23791, 23943, 25000, 25025, 26000, 27000, 27017, 27019, 27888, 28784, 31001, 32764, 32913, 34443, 34964, 37777, 38080, 40007, 41025, 41080, 44334, 45230, 46823, 46824, 50013, 50070, 50090, 55553, 57772, 61616, 62078

AGENDA OVERVIEW

Tier 8

PROTOCOL / PROBE	PORTS
Lockdownd	--
Telnet	107, 2332, 10023
AMQP	--
MQTT	--
MYSQL	--
OPCUA	--

PROTOCOL / PROBE	PORTS
WUDO	--
Redis	--
TLS	4433, 7879, 10443, 34443, 44334
Memcached	--
TCP	7, 9, 13, 17, 19, 37, 49, 82, 83, 84, 110, 143, 264, 465, 512, 548, 587, 617, 636, 705, 771, 873, 888, 910, 912, 921, 993, 995, 1000, 1024, 1030, 1035, 1080, 1089, 1098, 1099, 1100, 1101, 1102, 1103, 1128, 1158, 1199, 1211, 1220, 1234, 1241, 1311, 1352, 1433, 1440, 1521, 1533, 1581, 1582, 1604, 1723, 1755, 1811, 1883, 2000, 2083, 2121, 2181, 2200, 2207, 2323, 2362, 2375, 2379, 2381, 2525, 2533, 2601, 2604, 2638, 2809, 2947, 2967, 3000, 3037, 3050, 3057, 3128, 3200, 3217, 3273, 3299, 3306, 3311, 3312, 3351, 3460, 3500, 3628, 3632, 3690, 3780, 3790, 4322, 4433, 4444, 4445, 4567, 4659, 4679, 4730, 4840, 4848, 5038, 5040, 5051, 5222, 5247, 5400, 5432, 5433, 5554, 5580, 5601, 5631, 5632, 5666, 5672, 5800, 5938, 5984, 6001, 6002, 6050, 6080, 6101, 6112, 6262, 6502, 6503, 6660, 6667, 6905, 7001, 7071, 7077, 7080, 7144, 7210, 7580, 7777, 7778, 7800, 7879, 8014, 8023, 8028, 8087, 8095, 8161, 8180, 8205, 8222, 8400, 8686, 8800, 8880, 8883, 8899, 8901, 8902, 8903, 9000, 9042, 9060, 9081, 9084, 9090, 9092, 9111, 9160, 9300, 9527, 9530, 9595, 9809, 10001, 10008, 10051, 10080, 10098, 10443, 11099, 11211, 12345, 12397, 15672, 18264, 19810, 20010, 20171, 20222, 22222, 23791, 23943, 25000, 25025, 26000, 27000, 27017, 27019, 27888, 28784, 31001, 32764, 32913, 34964, 37777, 38080, 40007, 41025, 41080, 45230, 46823, 46824, 50013, 50070, 50090, 55553, 57772, 61616, 62078
TCP SYN	104, 11112

AGENDA OVERVIEW

Tier 9

PROTOCOL / PROBE	PORTS
HTTP	--
RDPNTLM	--
RPCBind	--
Intellivue	--
DICOM	--
NTP	--
BACnet	47809, 47810

AGENDA OVERVIEW

Tier 10

PROTOCOL / PROBE	PORTS
wwwcrawler	--
SNMP GetNext	--

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com