DRAGOS

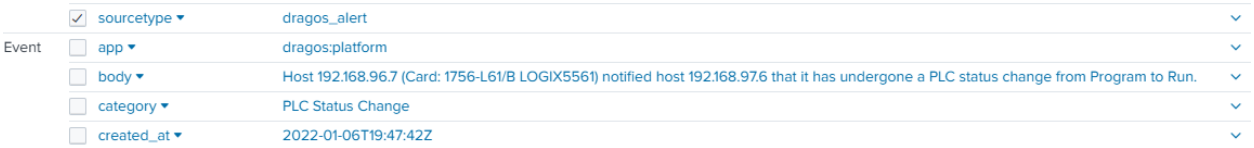
This project explores an industrial security investigation using data from Dragos' (BOTS) simulation. The environment mimics real-world ICS setups, including PLCs (Programmable Logic Controllers), sensors, and operator workstations. Using Splunk, I followed a series of scenario-based questions that guided me through analyzing alerts and logs. The questions pointed me in the right direction, I did investigation, asking what behavior looked unusual, what it might mean, and how it could impact the system. I focused on events like PLC status changes, SMB command shells, and CIP errors to understand how attackers might gain access, move through the environment, or manipulate physical processes. This gave me practical insight into how cyber threats can affect industrial systems and could shut down or damage critical operations.

Question:

Which host gets notified when the 1756-L61/B LOGIX5561 card undergoes a PLC status change?

🟢 Query 101 —→ index=* "status change" AND ("1756-L61" OR "LOGIX5561")

Expand date range to the whole month of January 2022



A PLC status change happens when the controller switches between modes like RUN (normal operation), PROGRAM (making changes), or FAULT (something went wrong). These changes can be part of normal work, like updates or restarts, but if they happen unexpectedly, they might be a sign of a problem or even an attack. The PLC talks to sensors and machines, so any change in its status is important. When this happens, it usually sends a message to another computer, for example an engineering workstation, that's set up to watch for these changes. Knowing

which computer gets this message helps us understand who is monitoring the system and whether anything suspicious is happening.

🟢 Query 102 As in many industries, there are multiple differently named manufactures and companies. Being able to identify what you have, including the make, model, and firmware can assist you in being proactive to hardware and/or firmware vulnerabilities.

Question: Based on the previous question, who is the manufacturer of the card?

Answer guidance: Provide the manufacturer for the PLC Processor Module

🔎 The makers of the PLC is Allen-Bradley

🟢 Query 103⟶

Knowing technical specifications of hardware can help with system designs and requirements. This can include software and hardware specs.

Question: Based on the answer in question 102, answering in MB, how large is the user memory on the previously identified controller?

The manufacturer is Allen-bradley and the user memory space is 2 MB.

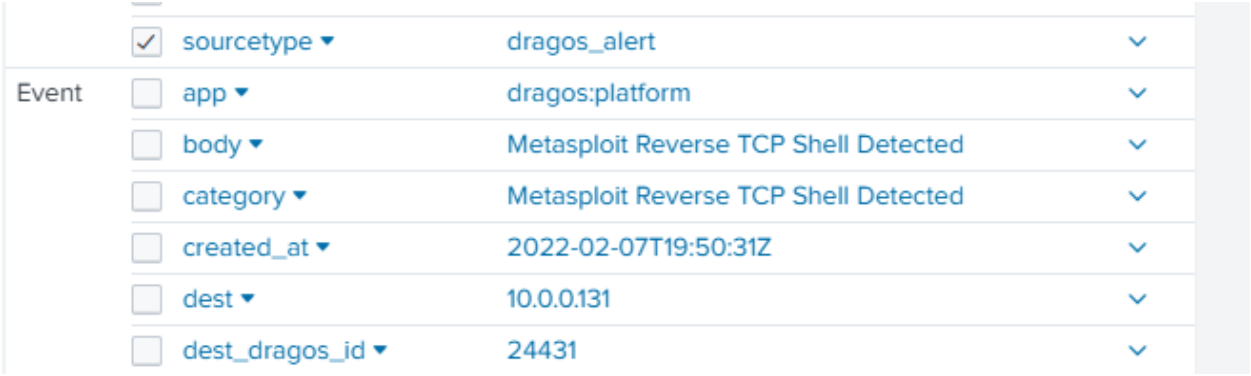
🟢 Query 104 ⟶ Along with knowing technical specifications of hardware, knowing built-in ports can help with upgrading systems and determining compatibility.

Question: What is the built-in COM (communication) port? RS-232

🟢 Query 105⟶ Many malicious actors may seek to establish C2, command and control to maintain a foothold or establish persistence within a target environment.

Question: What is the destination IP address of the TCP reverse shell that was detected?

🔎 index=* reverse



🟢 Query 106→ SMB is a common network protocol used to establish connections to remote systems and servers.

Question:What was the hostname that was connected to with a SMB command shell?

🔎 index=* "smb command shell”

🟢 Query 107→ Pylogix script as a lab simulation

Pylogix is a tool written in python that allows users to read/write tag values in different types of PLCs.

Question: If you were going to use the tool 'pylogix', what config file parameter needs to change in order to set the slot number?

Answer guidance: Provide the command to specify the slot number when using pylogix. You do not need to answer with the full syntax including Python. It's processorslot

🟢 Query 108 → Pylogix is a powerful tool that allows you to also route traffic through other devices.

Question:Using pylogix, what value is used to read a tag by routing through another device?

Answer guidance: Provide the command to read a tag by routing with pylogix. You do not need to answer with the full syntax including Python

🟢 Query 109—→ Pylogix is also useful for enumeration. With great power comes great responsibility and enumerating PLCs and ICS assets should be taken with extreme care due to sensitivity.

Question: Using pylogix, what value is used to enumerate and get all controller and program tags?

Answer guidance: Provide the command to enumerate all controllers and tags using pylogix.

GetTagList()

🔎 index=* "write tag"

sourcetype	dragos_alert
app	dragos:platform
body	Use of pycomm3 python library by host 192.168.212.229 to PLC 192.168.96.7. Pycomm3 is an open-source project that is used to read and write tag values from Rockwell Automatio n/Allen Bradley Logix PLCs over ENIP.
category	Pycomm3-generated CIP Traffic
created_at	2022-01-25T23:10:04Z
dest	192.168.96.7
dest_dragos_id	266
dest_host	
dest_ip	192.168.96.7
dest_mac	00:00:BC:3C:DB:0D

🟢 Query 110

Metasploit is a penetration testing tool suite that can help create payloads, establish C2 and contains multiple public exploits.

Question: On which hostname was the Metasploit alert for detected windows/speak_pwned run against? Answer guidance: Provide the hostname

🔎 index=* speak_pwned

choose create table view output


```
<11>Feb 05 01:47:51 dragos dragos_syslog: occurred_at="2022-02-05T01:46:52Z"
app="dragos:platform" body=" Metasploit Detected: windows/speak_pwned" category=" Metasploit
Detected: windows/speak_pwned" created_at="2022-02-05T01:47:51Z" dest="192.168.193.14"
dest_dragos_id="146" dest_host="srv-hq-nas01" dest_ip="192.168.193.14"
dest_mac="00:11:32:F7:22:DE" dest_name="range.local" dragos_detection_quad="Indicator"
dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name=""
id="85774" ids_type=network severity_id="2" signature="Network Traffic" src="192.168.193.12"
src_dragos_id="67" src_host="srv-hq-bkup01" src_ip="192.168.193.12" src_mac="00:50:56:86:53:6B"
src_name="range.local" subject="Indicator" type="alert" vendor_product="Dragos Platform"  Less
```


🟢 Query 111 → While PowerShell is a powerful tool for automation and system administration, there are additional capabilities in the form of PowerShell frameworks that are leveraged for offensive capabilities.

Question: What offensive PowerShell tool was used by the adversary?

🔎 index=* powershell


```
<12>Feb 07 20:17:55 dragos dragos_syslog: occurred_at="2022-02-07T20:17:09Z"
app="dragos:platform" body="ET TROJAN Possible PowerShell Empire Activity" category="ET TROJAN
Possible PowerShell Empire Activity" created_at="2022-02-07T20:17:55Z" dest="10.10.30.131"
dest_dragos_id="24433" dest_host="" dest_ip="10.10.30.131" dest_mac="" dest_name=""
dragos_detection_quad="Indicator" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host=""
dvc_ip="" dvc_mac="" dvc_name="" id="89437" ids_type=network severity_id="1" signature="Network
Traffic" src="10.10.30.129" src_dragos_id="24432" src_host="" src_ip="10.10.30.129" src_mac=""
src_name="" subject="Indicator" type="alert" vendor_product="Dragos Platform"  Less
```

🟢 Query 112 → The MS17-010 exploit is also famously known as EternalBlue. This exploit targets SMBv1 for all versions of Windows operating systems. In Windows 10, Windows Servers 2012 and newer, SMBv1 comes disabled by default.

Question: MS17-101 was run against a target. What was the target's MAC address?

Answer guidance: Provide the MAC address of the targeted system.

🔎 index=* "exploit" OR "smb" OR "MS17”

<10>Feb 07 20:18:00 dragos dragos_syslog: occurred_at="2022-02-07T20:17:13Z" app="dragos:platform" body="MS17-010 SMB1 Response STATUS_NOT_IMPLEMENTED - Possible NotPetya, EternalBlue, EternalRocks or WannaCry" category="MS17-010 SMB1 Response STATUS_NOT_IMPLEMENTED - Possible NotPetya, EternalBlue, EternalRocks or WannaCry" created_at="2022-02-07T20:18:00Z" dest="10.10.10.5" dest_dragos_id="24418" dest_host="" dest_ip="10.10.10.5" dest_mac="F8:DB:88:3E:83:A0" dest_name="" dragos_detection_quad="Indicator" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name="" id="89438" ids_type=network severity_id="3" signature="Network Traffic" src="192.168.48.3,10.10.10.10" src_dragos_id="24362" src_host="view-designer" src_ip="192.168.48.3,10.10.10.10" src_mac="00:09:91:02:2F:F2" src_name="" subject="Indicator" type="alert" vendor_product="Dragos Platform" Less

This exploit is notoriously known for wannacry ransomware.

🟢 Query 113→ Being able to identify which objects, fields or values are being changed can indicate possible malicious intent. Especially if those objects are not normally changed by different systems or devices.

Question:

Which host attempted to modify the Usermemory object on the host 192.168.1.6 more than once?

Answer guidance: Provide the IPv4 address.

#index=* dest_ip="192.168.1.6" "Usermemory"

2022-01-06T16:11:42.000Z	Host 192.168.1.100 attempted to modify the control logic on host 192.168.1.6 by writing to the Usermemory object. Less	dragos
2022-01-06T16:04:22.000Z	Host 192.168.1.100 attempted to modify the control logic on host 192.168.1.6 by writing to the Userm ...More	dragos
2022-01-06T15:56:18.000Z	Host 192.168.1.100 attempted to modify the control logic on host 192.168.1.6 by writing to the Userm ...More	dragos

In summary, modifying the stored logic changes how the plc or device operates.

🟢 Query 114 → A CIP connection is simply a connection between two devices, normally with a PLC. One type of error that can create an alert is of loss of connection. This is just one of many failures that can occur and be alerted upon.

Question: Host 192.168.1.200 received a CIP error indicating an unauthorized command from host 192.168.1.6. What type of request created the alert?

🔎 index=* src=192.168.1.6 ("cip" OR "unauthorized" OR "error")

to search for potential adversary activities.

<12>Jan 06 16:47:03 dragos dragos_syslog: occurred_at="2022-01-06T16:39:48Z" app="dragos:platform" body="Host 192.168.1.200 received CIP error code 8 extended error code N/A (Service Not Supported) from host 192.168.1.6 after issuing a Get Attribute List request to class Identity. This may indicate a device misconfiguration or an adversary attempting to interact with a controller." category="CIP Error (Service Not Supported) Indicating Unauthorized Command Message" created_at="2022-01-06T16:47:03Z" dest="192.168.1.200,192.168.96.200,192.168.1.100,192.168.97.6" dest_dragos_id="676" dest_host="ews-hq-siemens0,desktop-mln7j12,ews-hq-rslogix0" dest_ip="192.168.1.200,192.168.96.200,192.168.1.100,192.168.97.6" dest_mac="" dest_name="ews-hq-siemens01.local,desktop-mln7j12.local,ews-hq-rslogix01.local" dragos_detection_quad="Threat Behavior" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name="" id="31041" ids_type=network severity_id="1" signature="aa0820a3-2340-43c2-8082-d61cf18b4c98" src="192.168.1.6" src_dragos_id="266" src_host="" src_ip="192.168.1.6" src_mac="00:00:BC:3C:DB:0D" src_name="" subject="Communication" type="alert" vendor_product="Dragos Platform" Less

🟢 Query 115 → Port scans are useful for enumeration. Port scanning can show open ports and possible protocols and version numbers on different devices on the network. They can create visibility and help define your network footprint and what is being exposed across the network.

Question: There was a port scan initiated at 03:06. Providing the port number only, what was the highest port number scanned?

🔎 index=* "port scan"

> _raw

<12>Jan 13 03:07:48 dragos dragos_syslog: occurred_at="2022-01-13T03:06:24Z" app="dragos:platform" body="10.10.10.20 scanned at least 15 unique ports of host 10.10.20.10 in 0m0s. Ports: 1089/tcp, 1090/tcp, 1091/tcp, 1132/tcp, 1330/tcp, 1331/tcp, 135/tcp, 139/tcp, 21/tcp, 22/tcp, 23/tcp, 25/tcp, 443/tcp, 445/tcp, 502/tcp - local" category="Port Scan Detected" created_at="2022-01-13T03:07:48Z" dest="10.10.20.10" dest_dragos_id="15410" dest_host="" dest_ip="10.10.20.10" dest_mac="" dest_name="" dragos_detection_quad="Threat Behavior" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name="" id="41128" ids_type=network severity_id="1" signature="Network Traffic" src="10.10.10.20" src_dragos_id="15418" src_host="factory-talk-vi" src_ip="10.10.10.20" src_mac="F8:DB:88:3C:53:0A" src_name="" subject="Network Analytic" type="alert" vendor_product="Dragos Platform" Less

🟢 Query 116→ Being able to identify which systems are scanning others, along with being able to determine which systems can communicate with others are examples of good network visibility and hygiene. Firewall rules and additional considerations should be in place to reduce the amount of necessary communication across networks to reduce the attack surface or footprint.

Question: Based on the previous question, what is the hostname of where the scanner originated?

refer to the src_host value

🔎

🟢 Query 117→ There are multiple ways to detect access to systems, known as different access techniques. Being to detect, log and alert on the different types of access techniques will increases your overall cyber security posture.

Question: Host 192.168.193.12 sent a file from 192.168.2.2. What was the access technique used?

🔎 index=* src="192.168.193.12" dest="192.168.2.2"

```
<12>Jan 22 04:01:39 dragos dragos_syslog: occurred_at="2022-01-22T03:02:05Z"
app="dragos:platform" body="Within 1hr, host 192.168.2.2 (65) was logged into and received a
file from the same source host 192.168.193.12 (67). Access technique: None Logon. File Transfer
technique: Remote File Copy Remote File Copy." category="Authentication and File Transfer"
created_at="2022-01-22T04:01:38Z" dest="192.168.2.2" dest_dragos_id="65" dest_host="rslogix5000"
dest_ip="192.168.2.2" dest_mac="00:0C:29:D8:6E:C1" dest_name="rslogix5000.local"
dragos_detection_quad="Threat Behavior" dragos_detector_id="" dvc="" dvc_dragos_id=""
dvc_host="" dvc_ip="" dvc_mac="" dvc_name="" id="64950" ids_type=network severity_id="1"
signature="" src="192.168.193.12" src_dragos_id="67" src_host="srv-hq-bkup01"
src_ip="192.168.193.12" src_mac="00:50:56:86:53:6B" src_name="range.local"
subject="Communication" type="alert" vendor_product="Dragos Platform"  Less
```

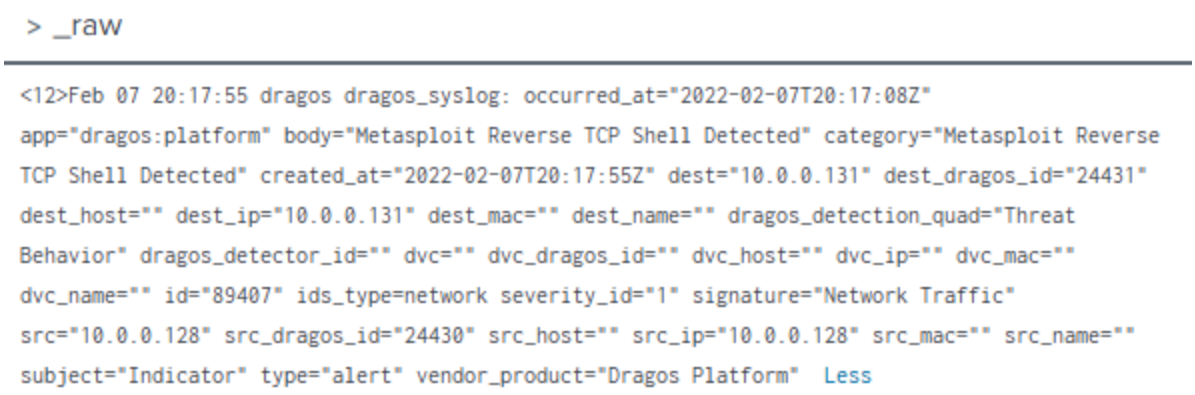
In the above, the attacker did not provide any authentication credentials, it was done on their behalf by the operating system.

🟢 Query 118⟶ Adversaries can use reverse shells or other types of connections from hosts back to their machines for established C2. Being able to differentiate between normal connections and anomalies may help highlight activity in the environment that may be malicious.

Question: There was a Metasploit reverse TCP shell detected, started from 10.0.0.128. Provide the IPv4 address of where it was connecting to.

Answer guidance: Provide the IPv4 address.

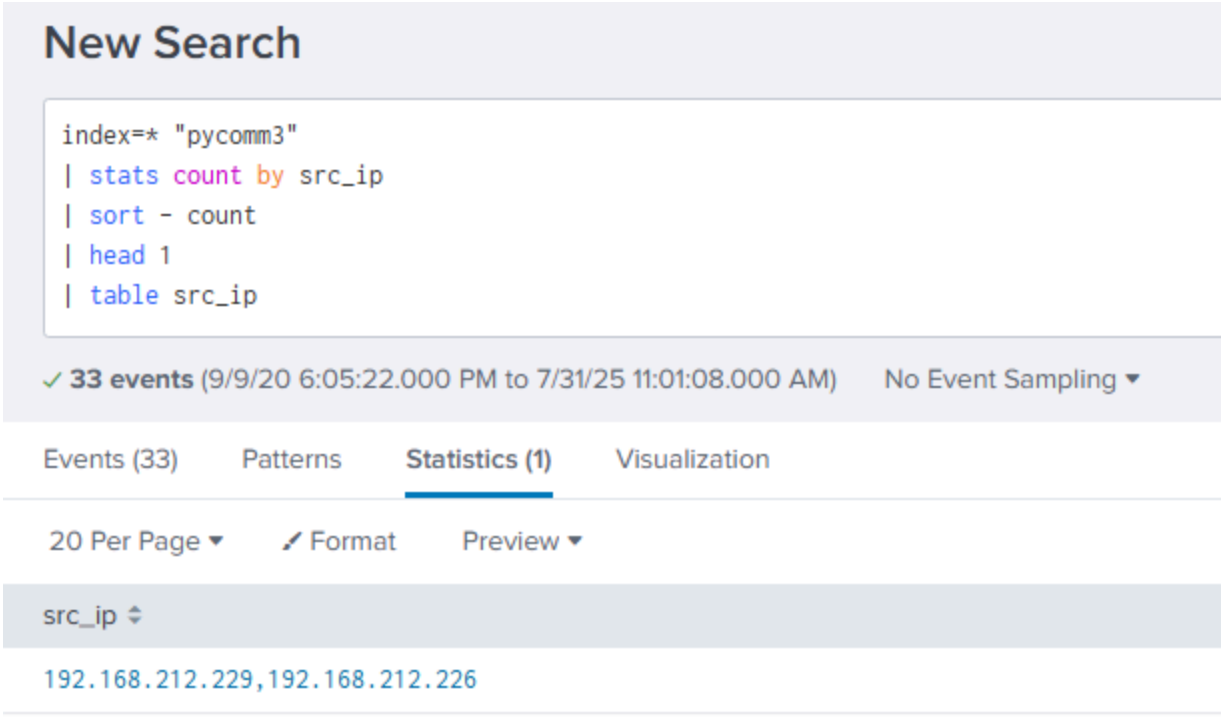
🔎 index=* src="10.0.0.128" "reverse tcp shell”



🟢 Query 119⟶ Pycomm3 is an open source python library for communicating with Allen-Bradley PLCs using Ethernet/IP. As the name suggests, pycomm3 is for python 3 from it's python 2 predecessor, pycomm.

Question: What is the IPv4 address of the host that uses pycomm3 the most?

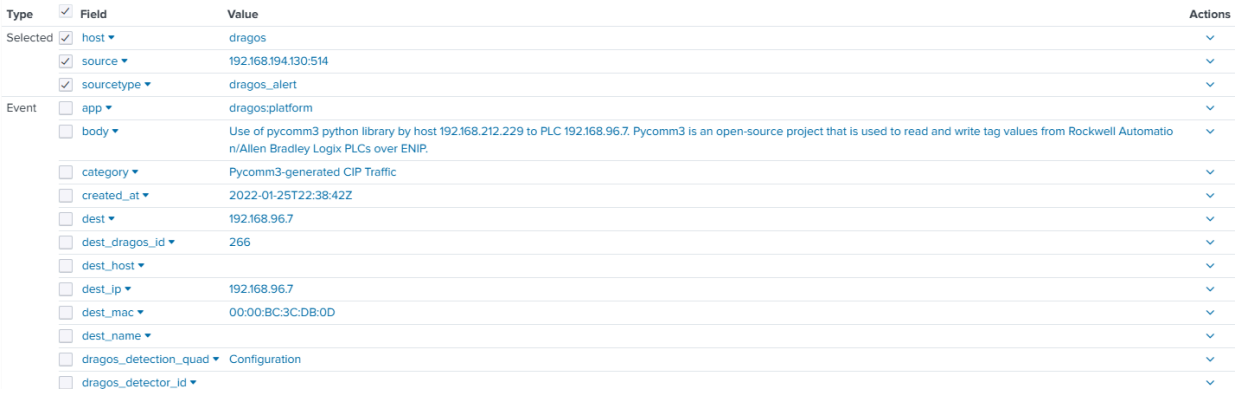
🔎 # index=* "pycomm3"
| stats count by src_ip (count the number of time each src ip appears)
| sort - count (sort by most used to be first)
| head 1 (then display the first)
| table src_ip (plus display in a table)



🟢 Query 120→ Not only can pycomm3 read files in different PLCs, but it can also write changes as well. The documentation, instructions and README files with programs are very informative regarding the full capabilities of tools.

Question: What protocol does Pycomm3 to use to read and write tag values?

🔎 index=* "pycomm3"



Type	Field	Value	Actions
Selected	host	dragos	
	source	192.168.194.130:514	
	sourcetype	dragos_alert	
Event	app	dragos:platform	
	body	Use of pycomm3 python library by host 192.168.212.229 to PLC 192.168.96.7. Pycomm3 is an open-source project that is used to read and write tag values from Rockwell Automation/Allen Bradley Logix PLCs over ENIP.	
	category	Pycomm3-generated CIP Traffic	
	created_at	2022-01-25T22:38:42Z	
	dest	192.168.96.7	
	dest_dragos_id	266	
	dest_host		
	dest_ip	192.168.96.7	
	dest_mac	00:00:BC:3C:DB:0D	
	dest_name		
	dragos_detection_quad	Configuration	
	dragos_detector_id		

🟢 **Query** 121 →Reading data from PLCs can be beneficial for checking values, settings and configurations.

Question: What type of data can be used with the 'request_data' command?

🟢 Query **122** → There are multiple drivers in pycomm3, that each add their own support for different devices or PLCs

Question: In alphabetical order, and separated by commas, i.e. a,b,c - What three drivers come installed with pycomm3?

https://docs.pycomm3.dev/en/latest/

🟢 Query 123 →

Understanding applicability of tools and programs is useful when testing. Some tools are specific to one system or device. Others may be applied to more than one.

Question: What type of PLCs can be used with Pycomm3

Answer guidance: Provide the manufacturers with a comma separating each one. For example: alpha,gamma

Allen-Bradley,Rockwell automation

🟢 Query 124→ Being able to search for and identify asset information within your monitoring solutions is important to be able to verify vulnerabilities, as well as identify exploitation attempts on those vulnerable assets.

Question: What is the IP address of the Honeywell DSA Primary?

🔎 index=* ("Honeywell" OR "DSA") AND "Primary"

<12>Jan 26 14:50:12 dragos dragos_syslog: occurred_at="2022-01-26T14:43:46Z"
app="dragos:platform" body="Asset:15 Asset: with change to Primary CPU status: Backup"
category="Honeywell DSA Primary CPU Change" created_at="2022-01-26T14:50:12Z" dest=""
dest_dragos_id="" dest_host="" dest_ip="" dest_mac="" dest_name=""
dragos_detection_quad="Configuration" dragos_detector_id="" dvc="10.1.0.101" dvc_dragos_id="15"
dvc_host="srv-hq-experion" dvc_ip="10.1.0.101" dvc_mac="00:0C:29:90:BF:71" dvc_name=""
id="73155" ids_type=network severity_id="1" signature="05d0a363-b85b-4779-99ba-52ab4e099a19"
src="" src_dragos_id="" src_host="" src_ip="" src_mac="" src_name="" subject="Asset"
type="alert" vendor_product="Dragos Platform" Less

Honeywell DSA Primary is the main node in Honeywell's Distributed System Architecture that manages communication between controllers, servers, and HMIs. If it fails, the Backup node takes over to keep the system running.

🟢 Query 125⟶ Not all adversaries use proprietary software, malware, and tools to gain access to systems. Being able to detect open source and popular tools available online can upgrade detection capabilities.

Question: What popular shell was used to execute commands on remote hosts from the MSSQL server?

🔎 #index=* "shell" OR "mssql"

> _raw

<12>Feb 07 20:22:58 dragos dragos_syslog: occurred_at="2022-02-07T20:17:08Z"
app="dragos:platform" body="Host on 10.0.0.128 attempted to execute commands on remote host on
10.0.0.131 using xp_cmdshell." category="MSSQL server remote usage of xp_cmdshell"
created_at="2022-02-07T20:22:58Z" dest="10.0.0.131" dest_dragos_id="24431" dest_host=""
dest_ip="10.0.0.131" dest_mac="" dest_name="" dragos_detection_quad="Threat Behavior"
dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name=""
id="89455" ids_type=network severity_id="1" signature="1f99b742-74d5-4549-970c-1c97b5df0c62"
src="10.0.0.128" src_dragos_id="24430" src_host="" src_ip="10.0.0.128" src_mac="" src_name=""
subject="Communication" type="alert" vendor_product="Dragos Platform" Less

🔎 index=* "xp_cmdshell"

<12>Feb 07 19:52:57 dragos dragos_syslog: occurred_at="2022-02-07T19:48:29Z" app="dragos:platform" body="Host on 10.0.0.128 attempted to execute commands on remote host on 10.0.0.131 using xp_cmdshell." category="MSSQL server remote usage of xp_cmdshell" created_at="2022-02-07T19:52:57Z" dest="10.0.0.131" dest_dragos_id="24431" dest_host="" dest_ip="10.0.0.131" dest_mac="" dest_name="" dragos_detection_quad="Threat Behavior" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name="" id="89144" ids_type=network severity_id="1" signature="84c8caba-22f4-4560-8bf6-72e011071d38" src="10.0.0.128" src_dragos_id="24430" src_host="" src_ip="10.0.0.128" src_mac="" src_name="" subject="Communication" type="alert" vendor_product="Dragos Platform" Less

This is a feature in SQL Server that allows you to execute system commands on the computer directly from SQL queries. This means you can run command-line tasks such as creating or deleting files, listing directories, or starting programs from within the database. It essentially bridges the SQL Server environment with the underlying operating system, giving you a way to automate tasks or interact with the server without leaving SQL Server.

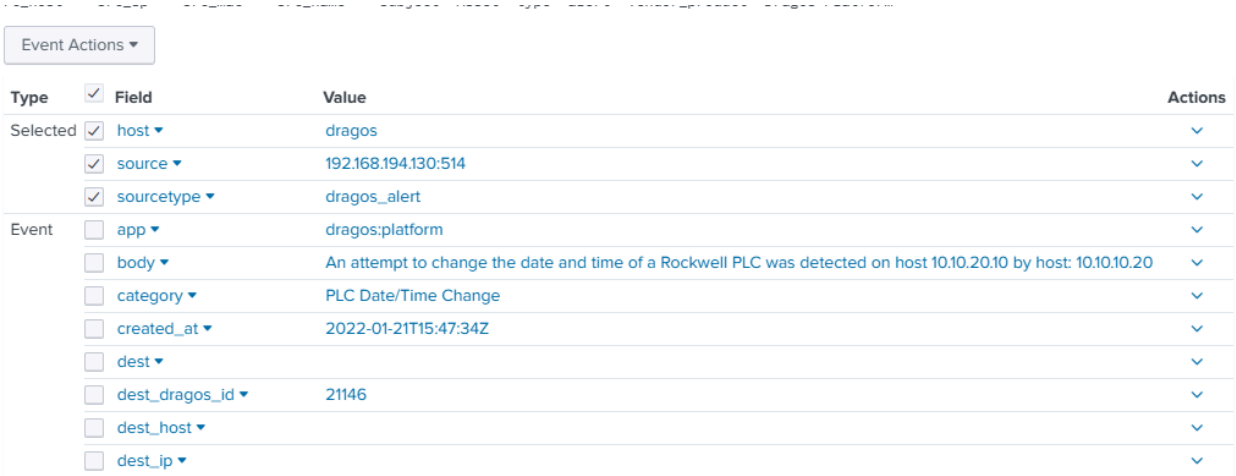
🟢 **Query #126 →** Mitigation of some vulnerabilities are as simple as turning off some commands or functionality, that may be turned on by default. As always, confirm with your vendor, OEM, system integrator before turning anything off to ensure it is not needed for operational use.

Question: By default that command is disabled. What command is used to enable it?

Research sp_configure

🟢 **Query 127 → Asset 21151 was potentially compromised. What was the first notification related to the asset after compromise was detected?**

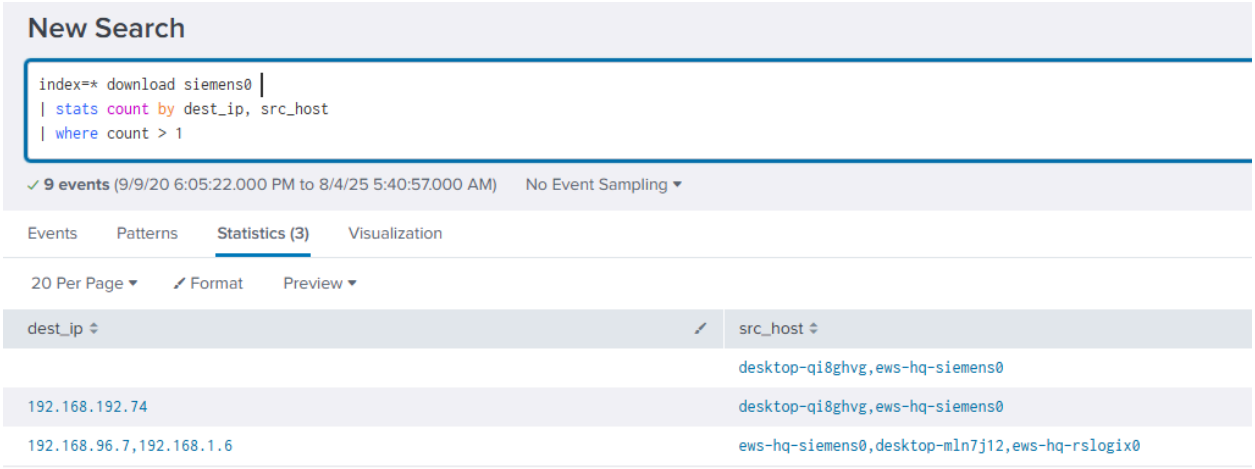
🔎 index=* "21151"
| sort -_time



🟢 Query 128—→ Downloading files could be an indication of malicious intent. It could be either an adversary trying to download files to a device, or possibly attempting to exfiltrate information. Being able to detect these actions on a network can alert upon possible compromise. Sometimes it may be part of normal operations of an OT environment, such as copying data to a historian.

Question: One of the hosts on the network is used for running certain pieces of Siemens software and is named accordingly. It looks like one of the hosts was attempting to download a file multiple times. What is the IPv4 address of the destination it was trying to download the file from?

Answer guidance: Provide the IPv4 address of the destination the Siemens host machine was trying to download the software from.



🟢Query **129→** The type of files being downloaded can make a difference as well. Being able to detect upon different file extensions can help improve detection capabilities.

Question: Referring to the previous question, what was the extension of the file that was downloaded?

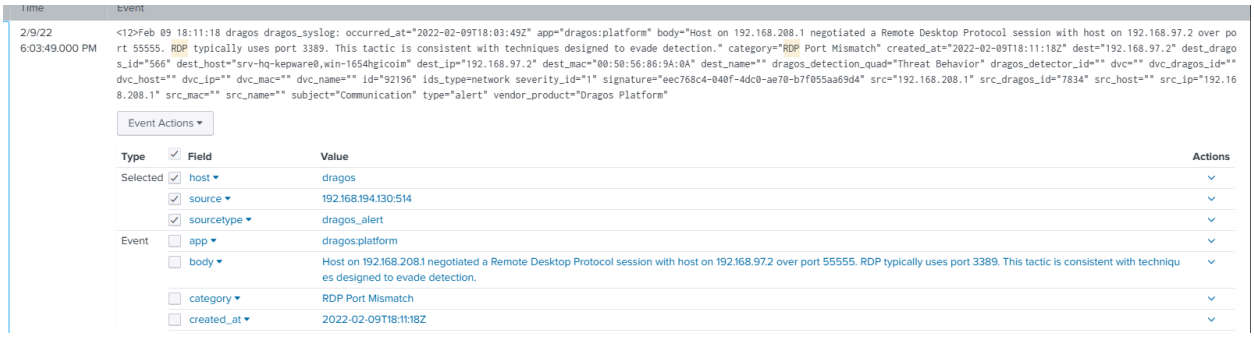
🔎 **index=* download AND siemens0**

🔎 index=* ("download" OR "GET" OR "http" OR "https")

🟢 Query **130→** An obfuscation strategy often found is that of ports and protocols attempting usage to non-default ports as a method to obfuscate the systems on the network. While a quick enumeration is a good place to get started, it may not give the full picture of a network.

Question: What is the source IP address that tried to negotiate RDP on port 55555?

🔎 index=* "RDP" "port”



🟢 Query **131→** RDP (Remote Desktop Protocol) is a windows tool that provides the user access to another system remotely.

Question: What is the common port number used for RDP?

Answer guidance: Provide the port number commonly used for RDP

🟢 Query 132→ RDP is a normal method for users and operators to access workstations and similar servers within a different network domain. Firewall rules and DMZ should be configured correctly to limit the connections between the different zones.

Question: During a forwarded RDP Negotiation request with a nonstandard destination port with a Dragos Source ID of 7834, what was the destination host name?

🔎 index=* "RDP" "src_dragos_id=" 7834 "dest_host=”

```
<12>Feb 09 18:01:30 dragos dragos_syslog: occurred_at="2022-02-09T18:00:43Z"
app="dragos:platform" body="Forwarded RDP Negotiation Request - nonstandard dst port"
category="Forwarded RDP Negotiation Request - nonstandard dst port" created_at="2022-02-
09T18:01:30Z" dest="192.168.2.66" dest_dragos_id="33" dest_host="rshistorian"
dest_ip="192.168.2.66" dest_mac="00:0C:29:72:28:87" dest_name="" dragos_detection_quad="Threa
Behavior" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac=""
dvc_name="" id="91945" ids_type=network severity_id="1" signature="Network Traffic"
src="192.168.208.1" src_dragos_id="7834" src_host="" src_ip="192.168.208.1" src_mac=""
src_name="" subject="Indicator" type="alert" vendor_product="Dragos Platform"  Less
```

🟢 Query 133→ A historian is a system used to collect and store logs or process data from SCADA or similar devices. They are usually configured to automatically log and process data from those environments.

Question: What is the Dragos ID number of the rshistorian host?

RHistorian is a software from Rockwell Automation that collects data from industrial controllers like PLCs. It stores this data over time so you can track changes in processes such as temperature or production. You can also analyze and visualize the data to monitor and improve operations.

🔎 index=* "RDP" "src_dragos_id=" 7834 rshistorian

a sourcetype	> _raw
dragos_alert	<12>Feb 09 18:01:30 dragos dragos_syslog: occurred_at="2022-02-09T18:00:43Z" app="dragos:platform" body="Forwarded RDP Negotiation Request - nonstandard dst port" category="Forwarded RDP Negotiation Request - nonstandard dst port" created_at="2022-02-09T18:01:30Z" dest="192.168.2.66" dest_dragos_id="33" dest_host="rshistorian" dest_ip="192.168.2.66" dest_mac="00:0C:29:72:28:87" dest_name="" dragos_detection_quad="Threat Behavior" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name="" id="91945" ids_type=network severity_id="1" signature="Network Traffic" src="192.168.208.1" src_dragos_id="7834" src_host="" src_ip="192.168.208.1" src_mac="" src_name="" subject="Indicator" type="alert" vendor_product="Dragos Platform" Less

🟢 Query 134 → Nmap is a popular open-source enumeration tool to scan networks for hosts. Nmap can also provide open ports, protocols, version numbers and more; depending on the systems or devices being scanned

Question: Which test asset IP address was scanned by NMAP from the source IP of 192.168.208.1?

🔎 index=* src_ip 192.168.208.1 "src_name=" nmap

In summary, this tells who scanned who in the network.

> _raw

<12>Feb 09 17:33:42 dragos dragos_syslog: occurred_at="2022-02-09T17:27:52Z" app="dragos:platform" body="New Nmap Scanner detected at asset: 7834 at 192.168.208.1" category="New Nmap Scanner" created_at="2022-02-09T17:33:42Z" dest="192.168.192.74" dest_dragos_id="23048" dest_host="sw-hq-lab01-cb08_mfg01" dest_ip="192.168.192.74" dest_mac="EC:E5:55:A7:CE:4F,EC:E5:55:A7:CE:40,EC:E5:55:A7:CE:38" dest_name="" dragos_detection_quad="Configuration" dragos_detector_id="" dvc="" dvc_dragos_id="" dvc_host="" dvc_ip="" dvc_mac="" dvc_name="" id="91904" ids_type=network severity_id="1" signature="2ad95a0e-6cef-4e37-bbf2-a8e68c81e444" src="192.168.208.1" src_dragos_id="7834" src_host="" src_ip="192.168.208.1" src_mac="" src_name="" subject="Communication" type="alert" vendor_product="Dragos Platform" Less