Transforming Threat Intelligence Into Actionable Attack Surface Reduction

11:20am - 11:50am

Loris Minassian, Chief Executive Officer, CyberStash

Loris Minassian

Loris Minassian
Founder at CyberStash

Topic

Transforming threat intelligence into actionable attack surface reduction

Loris Minassian

Founder, CyberStash

2nd

25 years

100s

Loris Minassian

Founder & Principal Consultant at CyberStash

Agenda

1. Understanding the Threat Landscape
2. The Role of Threat Intelligence
3. Operationalising Threat Intelligence Challenges
4. Enhancing Defense with Network Analytics
5. Lowering Exposure & Detecting Unknown Threats

Understanding the Threat Landscape

Business Impact

Defensive Shortcomings

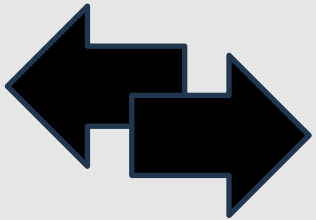
Operational and Budget Constraints

Escalating Threat Landscape

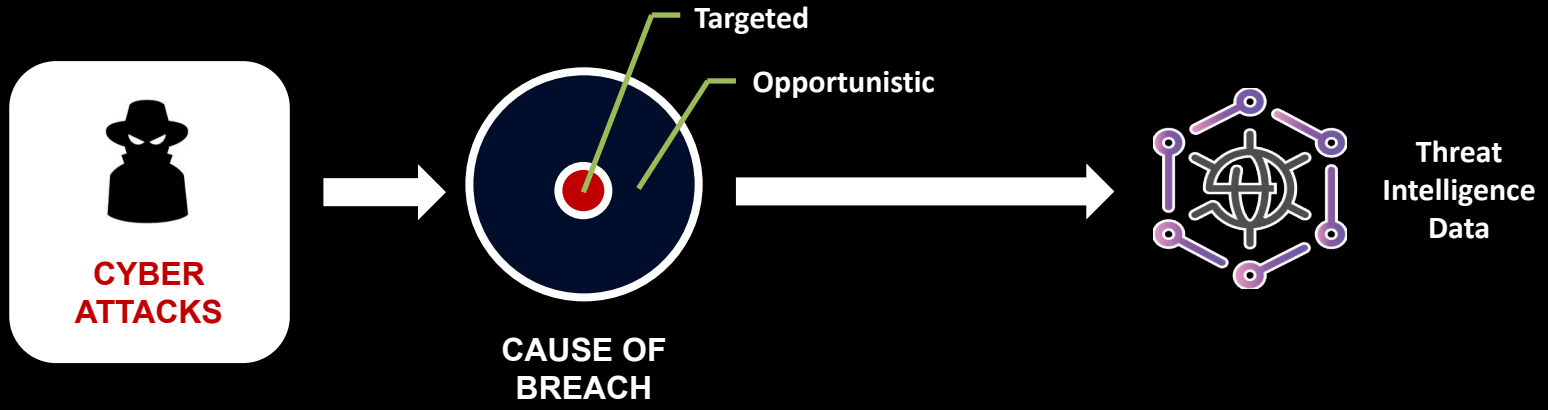
Expanding Attack Surface

Understanding the Threat Landscape

Increasingly Targeting	Ongoing Defensive Challenges
Human Weaknesses	User Behaviour
Persistent Vulnerabilities	Patch Management
Zero-Day Vulnerabilities	Unknown Vulnerabilities
High Value Organisations	In-Memory Fileless Detection
Supply Chains	Shadow Risks in Supply Chains
Vulnerable Procedures	Operationalising IT and Cybersecurity



Understanding the Threat Landscape



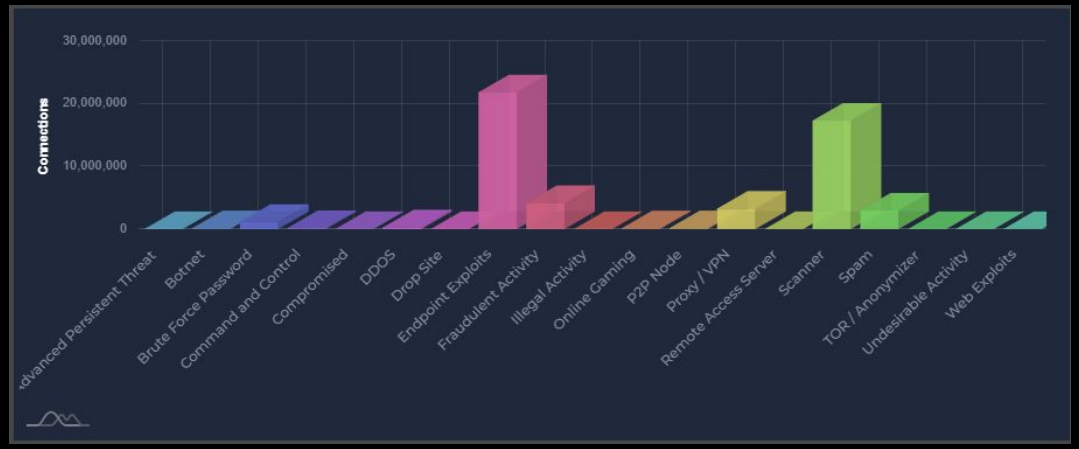
Opportunistic Cyber Attacks

MOUNTING THREAT VOLUMES

850,000
Malicious IPs Daily

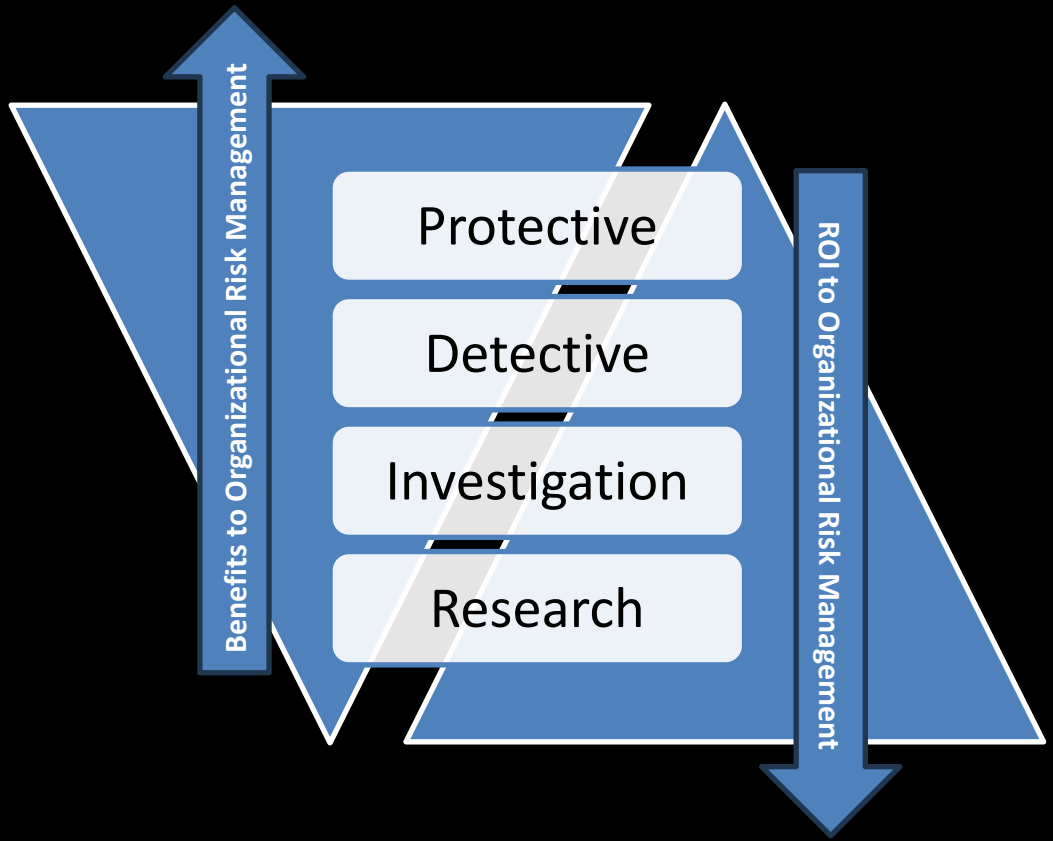
50 Million
Malicious Domains

20 Million
Phishing Attacks Daily



ATTACK CATEGORIES

. The Role of Threat Intelligence



. The Role of Threat Intelligence

EFFECTIVENESS/VALUE	Rating	Size of Organization's Security Team	
	Low	Small to Medium Enterprise	Large Enterprise
	Medium		
	High		
	Considerations Degree of Risk Mitigation Control Prioritization Risk and Resource Optimization	Between 1 and 5 FTEs Dedicated to Security	With 6 or More FTEs Dedicated to Security

CATEGORY	Use Case	Small to Medium Enterprise			Large Enterprise		
		Low Risk Target	Medium Risk Target	High Risk Target	Low Risk Target	Medium Risk Target	High Risk Target
PROTECTIVE	Blocking IP Addresses, Domains and URLs at the Perimeter						
	Blocking Processes, Files, DLLs on Endpoints						
	Vulnerability Remediation Prioritization						
	Using TTPs to Inform Protective Controls						

. The Role of Threat Intelligence

EFFECTIVENESS/VALUE	Rating	Size of Organization's Security Team					
	Low	Small to Medium Enterprise			Large Enterprise		
	Medium						
	High						
	Considerations Degree of Risk Mitigation Control Prioritization Risk and Resource Optimization	Between 1 and 5 FTEs Dedicated to Security			With 6 or More FTEs Dedicated to Security		
CATEGORY	Use Case	Low Risk Target	Medium Risk Target	High Risk Target	Low Risk Target	Medium Risk Target	High Risk Target
DETECTIVE	Detecting IP Addresses, Domains and URLs at the Perimeter			■	■	■	■
	Detecting Processes, Files, DLLs on Endpoints			■		■	■
	Proactively Hunting for Indicators (Automated)		■	■		■	■
	Proactively Hunting for Indicators (Manual)						■
	Using TTPs to Inform Detective Controls					■	■

. The Role of Threat Intelligence

EFFECTIVENESS/VALUE	Rating	Size of Organization's Security Team	
	Low	Small to Medium Enterprise	Large Enterprise
	Medium		
	High		
	Considerations Degree of Risk Mitigation Control Prioritization Risk and Resource Optimization	Between 1 and 5 FTEs Dedicated to Security	With 6 or More FTEs Dedicated to Security

CATEGORY	Use Case	Small to Medium Enterprise			Large Enterprise		
		Low Risk Target	Medium Risk Target	High Risk Target	Low Risk Target	Medium Risk Target	High Risk Target
INVESTIGATION	Informing Incident Response			■	■	■	■
	Adding Context to Investigations				■	■	■
	Adding Context to Compromise Assessments			■		■	■
	Research to Informing Protective Controls (Predictive Intelligence)					■	■
	Research to Inform Detective Controls (Predictive Intelligence)						■

. The Role of Threat Intelligence

EFFECTIVENESS/VALUE	Rating	Size of Organization's Security Team	
	Low	Small to Medium Enterprise	Large Enterprise
	Medium		
	High		
	Considerations Degree of Risk Mitigation Control Prioritization Risk and Resource Optimization	Between 1 and 5 FTEs Dedicated to Security	With 6 or More FTEs Dedicated to Security

CATEGORY	Use Case	Small to Medium Enterprise			Large Enterprise		
		Low Risk Target	Medium Risk Target	High Risk Target	Low Risk Target	Medium Risk Target	High Risk Target
RESEARCH	Producing Trends and Reports to Inform Strategic Decisions						
	Producing Trends and Reports to Inform Tactical & Operational Decisions						
	Using Indicators to Track and Report on APT Campaigns						
	Sharing Threat Intelligence on APTs						

Operationalising Threat Intelligence Challenges

57%

Lack the security staff to make threat intelligence actionable

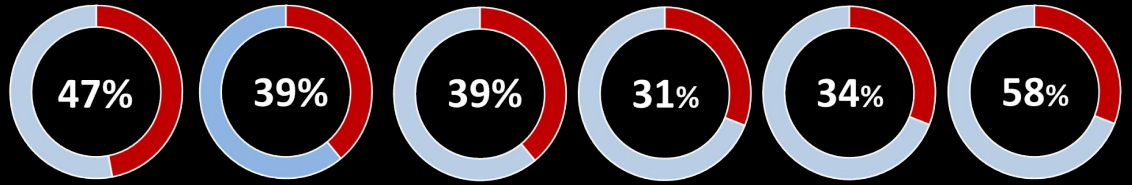
Major Contributors

Resources

Depending on people where we need to depend on technology

Technology Limitations

Unable to process and block at meaningful scale



Best Practice Framework for Threat Intelligence

ACCESS	AGGREGATE	AUTOMATE	HUNT
• Collect millions of accurate threat indicators • Multiple sources – commercial, open source, industry, & government • Multiple types – reputation feeds, blacklists, country IPs, organization IPs	• Multiple threat feeds consolidated into a single feed • Open platform that can easily integrate TI via standards like STIX/TAXII • Analytics applied for enhanced intelligence	• Trusted allow-lists dynamically updated in real time • Threat feeds dynamically updated in real time • Protective policies automatically applied • Threat hunting and incident response automatically triggered	• Pivot, Hunt and Investigate Suspicious Traffic • Block previously unknown threats & unwanted traffic

Enhancing Defense with Network Analytics

Objectives

- Systematically reduce exposure progressively without impacting business
- Defend against Advanced Persistent Threats and Sophisticated State Actors

MAPPING TO POTENTIAL ADVERSARY INFRASTRUCTURES

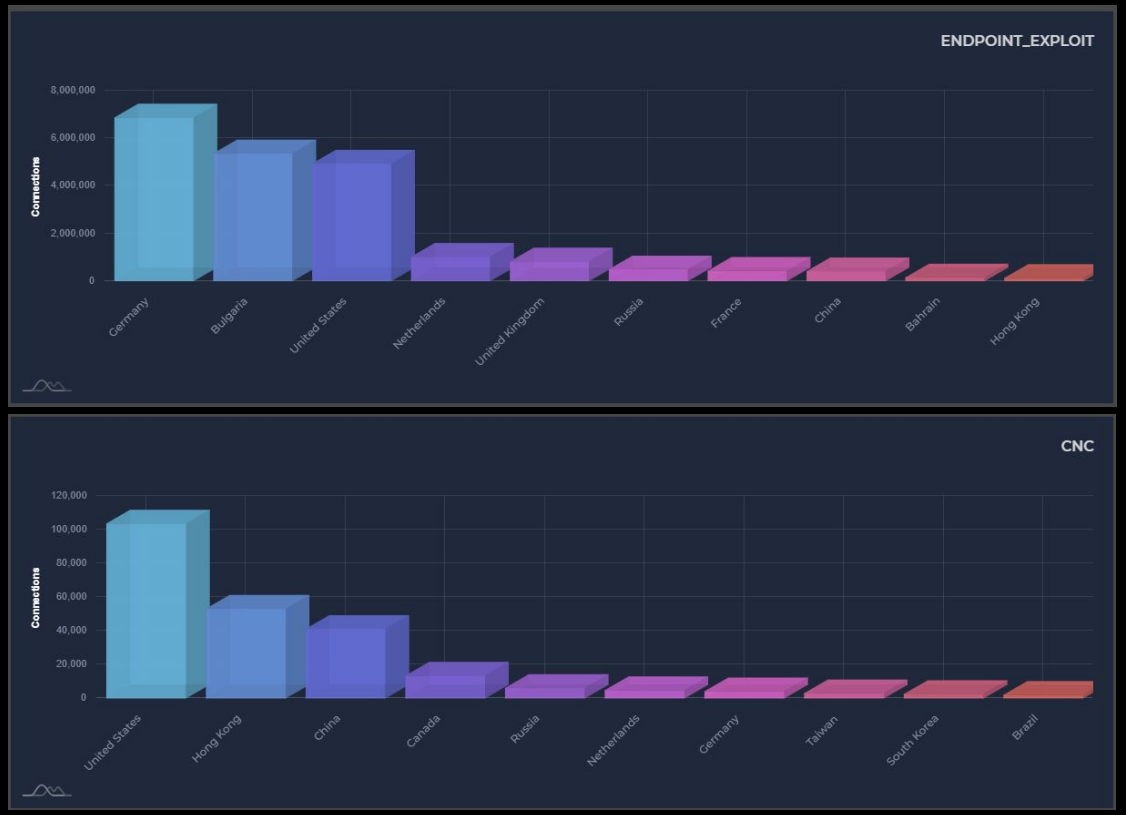
Threat Intelligence Data

Country (GEO-IP)	Autonomous System Numbers (ASNs)	Top Level Domains (TLDs)
Russia (46 Million)	AS4134 (111 Million IPs)	.XYZ (4.1 Million Domains)
China (352 Million)	AS4837 (58 Million IPs)	.ICU (1.2 Million Domains)
North Korea (Thousands)	AS9808 (36 Million IPs)	.CH (2.4 Million Domains)
Iran (12 Million)	AS9394 (20 Million IPs)	.RU (5.1 Million Domains)
Brazil (90 Million)	AS4538 (17 Million IPs)	.ML (77 Thousand Domains)
	AS12389 (9.3 Million IPs)	.TK (60 Thousand Domains)
	AS8402 (2.2 Million IPs)	.CF (70 Thousand Domains)
	AS8359 (1.2 Million IPs)	
	AS3216 (1.2 million IPs)	
	AS12714 (1.2 million IPs)	

Insightful Analytics

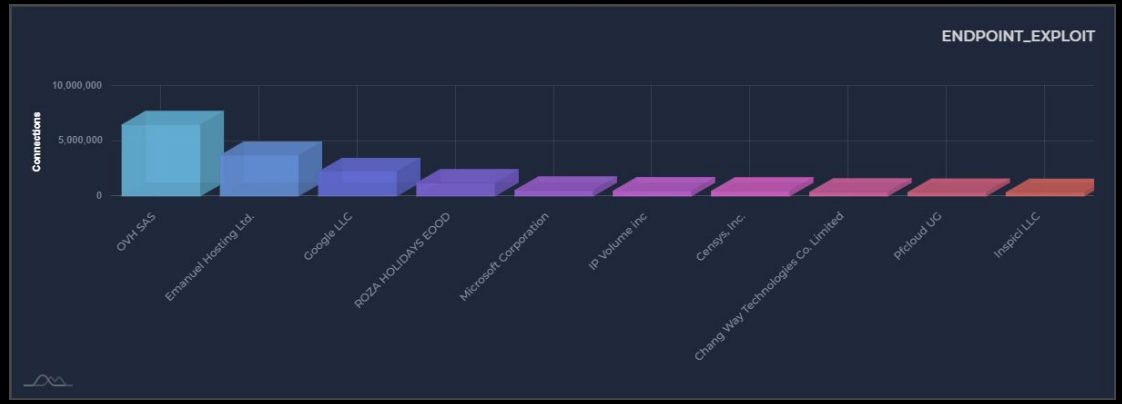
Enhancing Defense with Network Analytics

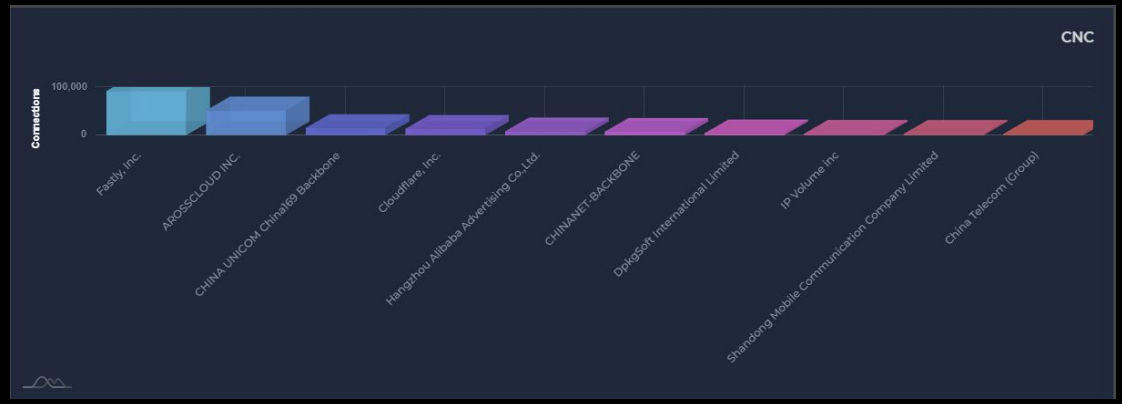
Country (GEO-IP)



Enhancing Defense with Network Analytics

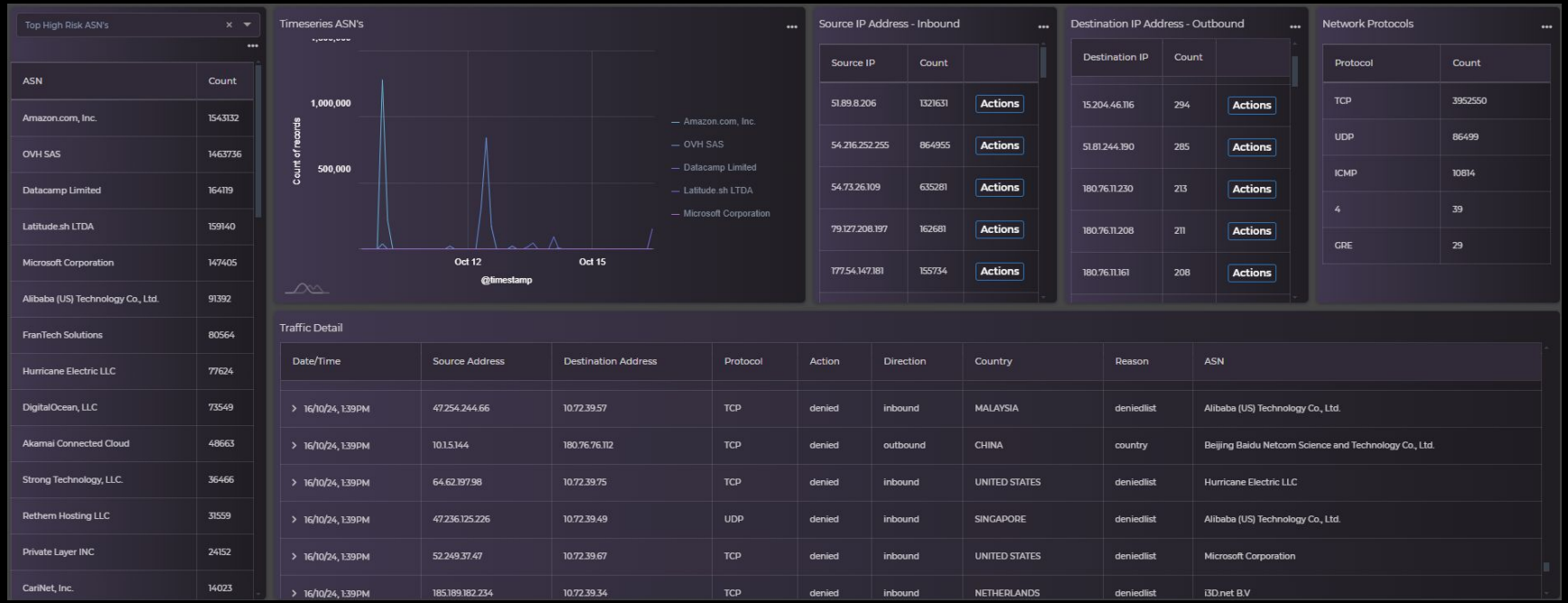
Autonomous Systems





Enhancing Defense with Network Analytics

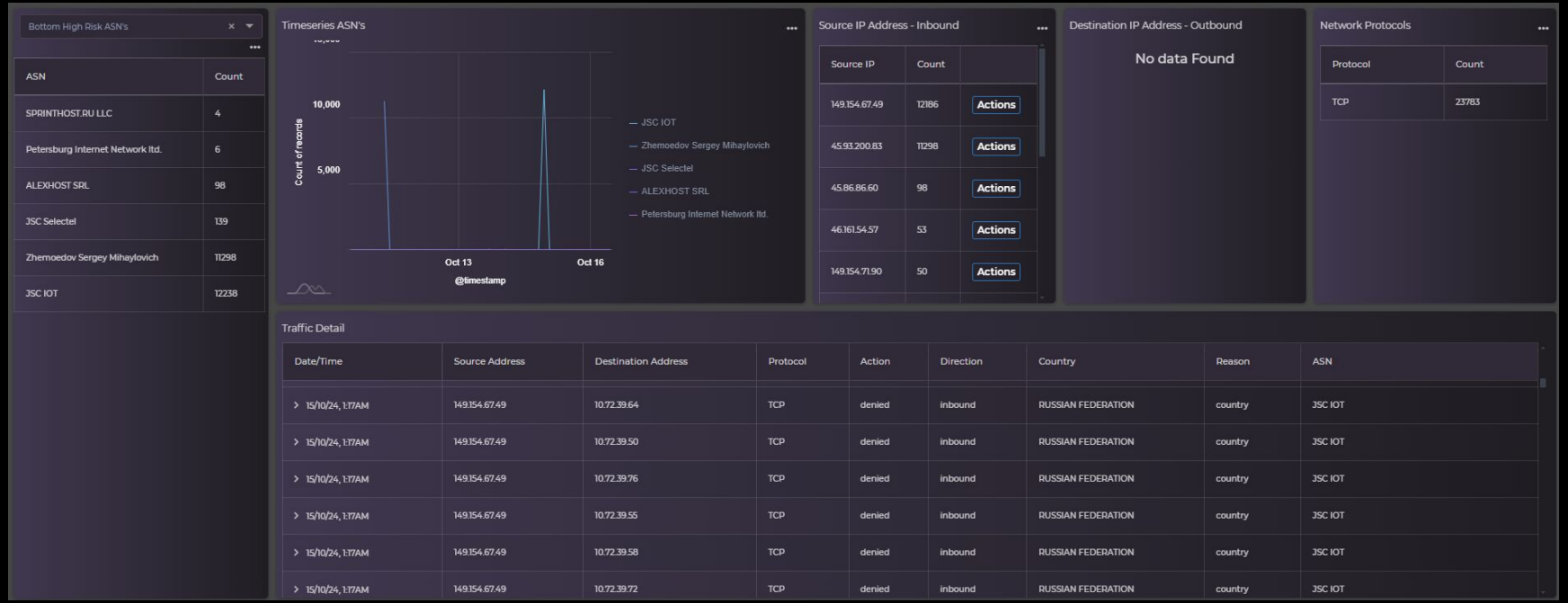
Correlate with High-Risk Autonomous Systems



Enhancing Defense with Network Analytics

Correlate with High-Risk Autonomous Systems

Filtering on Russian Federation and Inbound Traffic



Bottom High Risk ASN's

ASN	Count
SPRINTHOST.RU LLC	4
Petersburg Internet Network ltd.	6
ALEXHOST SRL	98
JSC Selectel	139
Zhernoedov Sergey Mihaylovich	11298
JSC IOT	12238

Timeseries ASN's

Source IP Address - Inbound

Source IP	Count	
149.154.67.49	12186	Actions
45.93.200.83	11298	Actions
45.86.86.60	98	Actions
46.161.54.57	53	Actions
149.154.71.90	50	Actions

Destination IP Address - Outbound

No data Found

Network Protocols

Protocol	Count
TCP	23783

Traffic Detail

Date/Time	Source Address	Destination Address	Protocol	Action	Direction	Country	Reason	ASN
15/10/24, 1:17AM	149.154.67.49	10.72.39.64	TCP	denied	inbound	RUSSIAN FEDERATION	country	JSC IOT
15/10/24, 1:17AM	149.154.67.49	10.72.39.50	TCP	denied	inbound	RUSSIAN FEDERATION	country	JSC IOT
15/10/24, 1:17AM	149.154.67.49	10.72.39.76	TCP	denied	inbound	RUSSIAN FEDERATION	country	JSC IOT
15/10/24, 1:17AM	149.154.67.49	10.72.39.55	TCP	denied	inbound	RUSSIAN FEDERATION	country	JSC IOT
15/10/24, 1:17AM	149.154.67.49	10.72.39.58	TCP	denied	inbound	RUSSIAN FEDERATION	country	JSC IOT
15/10/24, 1:17AM	149.154.67.49	10.72.39.72	TCP	denied	inbound	RUSSIAN FEDERATION	country	JSC IOT

Enhancing Defense with Network Analytics

Example: Real-Time Protection using Threat Intelligence

Perimeter Traffic Intelligence | Perimeter Domain Intelligence | Machine Learning Detections | Internal DNS Logs

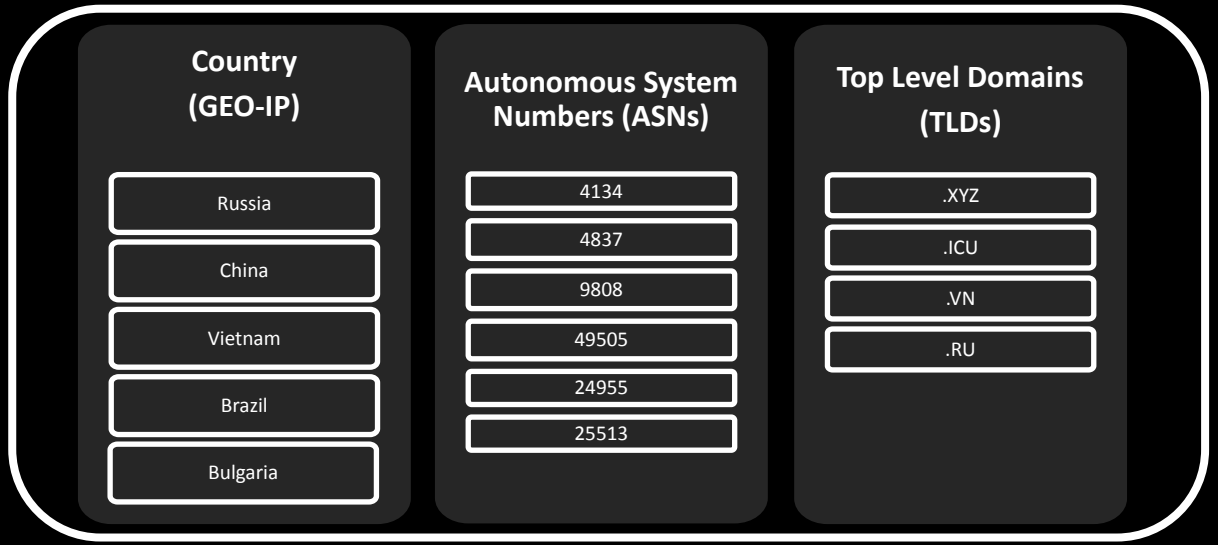
Date/Time	Country	AS Name	Protocol	Source Address	Destination Address	Action	Reason	Direction	Active Lists
16/10/24, 2:04 PM	UNITED STATES	Google LLC	UDP	205.210.31.82	10.72.39.50	denied	deniedlist	inbound	DHS Information Sharing,Blocklist.de,ET Block IPs,Cloud Attackers
16/10/24, 2:04 PM	UNITED STATES	Google LLC	TCP	198.235.24.202	10.72.39.47	denied	deniedlist	inbound	DHS Information Sharing,Blocklist.de,ET Block IPs,Cloud Attackers
16/10/24, 2:04 PM	BULGARIA	Emanuel Hosting Ltd.	TCP	79.110.62.133	10.72.39.57	denied	deniedlist	inbound	ET Block IPs
16/10/24, 2:04 PM	UNITED STATES	Hurricane Electric LLC	TCP	184.105.247.235	10.72.39.58	denied	deniedlist	inbound	CINS Army list,Cloud Attackers
16/10/24, 2:04 PM	VENEZUELA	CANTV Servicios, Venezuela	TCP	186.92.168.131	10.72.39.64	denied	threatlist	inbound	-
16/10/24, 2:04 PM	VENEZUELA	CANTV Servicios, Venezuela	TCP	186.94.51.146	10.72.39.33	denied	deniedlist	inbound	Cloud Attackers
16/10/24, 2:04 PM	UNITED STATES	Censys, Inc.	TCP	206.168.34.142	10.72.39.38	denied	deniedlist	inbound	Blocklist.de,ET Block IPs,CINS Army list,Cloud Attackers
16/10/24, 2:04 PM	UNITED STATES	Akamai Connected Cloud	TCP	74.207.253.22	10.72.39.212	denied	deniedlist	inbound	Blocklist.de,CINS Army list,Cloud Attackers
16/10/24, 2:04 PM	BULGARIA	Perfecto Consultoria E Apoio Administrativo LTDA	TCP	95.214.27.32	10.72.39.59	denied	deniedlist	inbound	ET Block IPs
16/10/24, 2:04 PM	SWEDEN	Kamatera, Inc.	TCP	185.139.228.190	10.72.39.33	denied	deniedlist	inbound	DHS Information Sharing,Blocklist.de,Cloud Attackers
16/10/24, 2:04 PM	UNITED STATES	HostPapa	TCP	107.174.79.187	10.72.39.46	denied	deniedlist	inbound	CINS Army list
16/10/24, 2:04 PM	UNITED STATES	HostPapa	TCP	107.174.79.187	10.72.39.73	denied	deniedlist	inbound	CINS Army list
16/10/24, 2:04 PM	NETHERLANDS	Alsycon B.V.	TCP	185.224.128.83	10.72.39.64	denied	deniedlist	inbound	DHS Information Sharing,State of Missouri SOC,Blocklist.de,ET Block IPs,CINS Army list,Cloud Attackers
16/10/24, 2:04 PM	INDONESIA	PT Telekomunikasi Indonesia	TCP	36.82.252.120	10.72.39.195	denied	asn	inbound	-

Lowering Exposure & Detecting Unknown Threats

Actionable Next Steps

Begin Your Journey to Stronger Cybersecurity

1. Gather analytics on network traffic flowing to and from the following infrastructures.
2. Review whether any of this traffic is essential for school operations
3. Assess whether it can be safely blocked without disrupting business activities.



QUESTIONS AND DICUSSION

Contact

Loris Minassian
loris.minassian@cyberstash.com
0416 048 967

Loris Minassian
Founder & Principal Consultant at CyberStash