Building Your Defensive Line: Selecting MSS to Increase Your Cyber Resilience

Greg Gray

Patrick Dalton

What is MSS?

Asset Discovery
Know who and what is connected to your environment at all times

Vulnerability Assessment
Know where the vulnerabilities are on your assets to avoid compromise

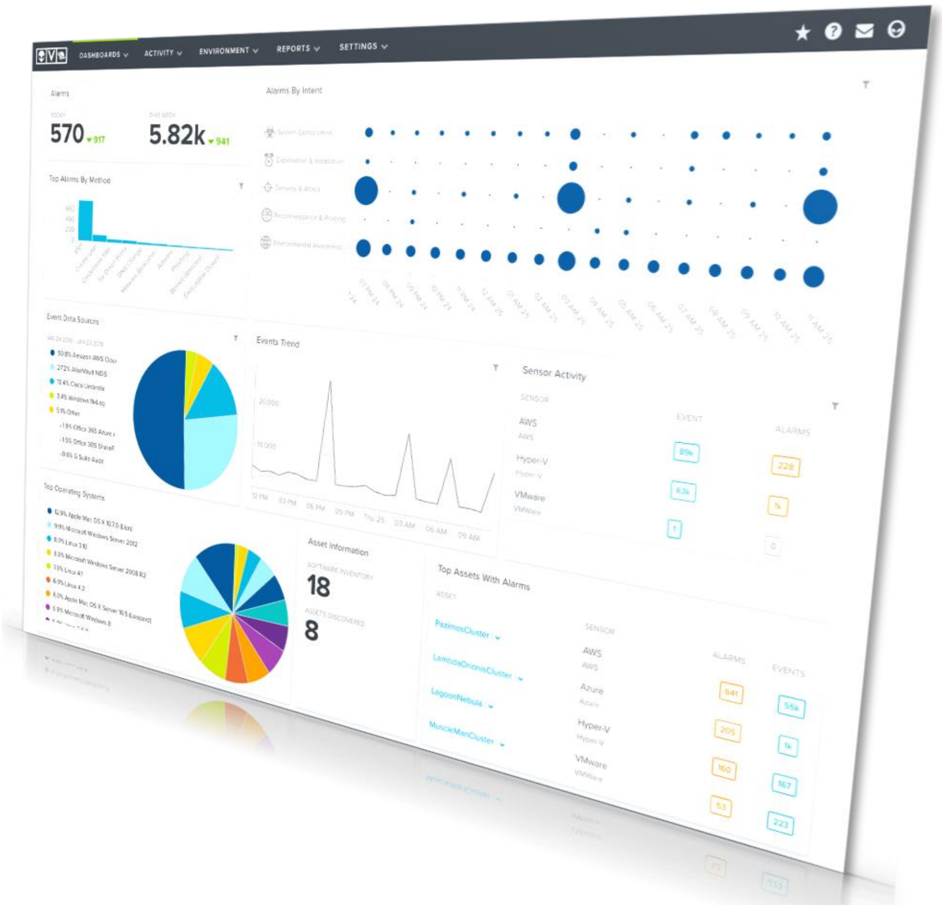
Intrusion Detection
Know when suspicious activities happen in your environment

Endpoint Detection & Response
Continuously monitor your endpoints in the cloud and on premises to detect threats and changes to critical files.

Behavioral Monitoring
Identify suspicious behavior and potentially compromised systems

SIEM & Log Management
Correlate and analyze security event data from across your network and respond

Security & Compliance Reporting
Pre-built, customizable reports for regulation standards and compliance frameworks

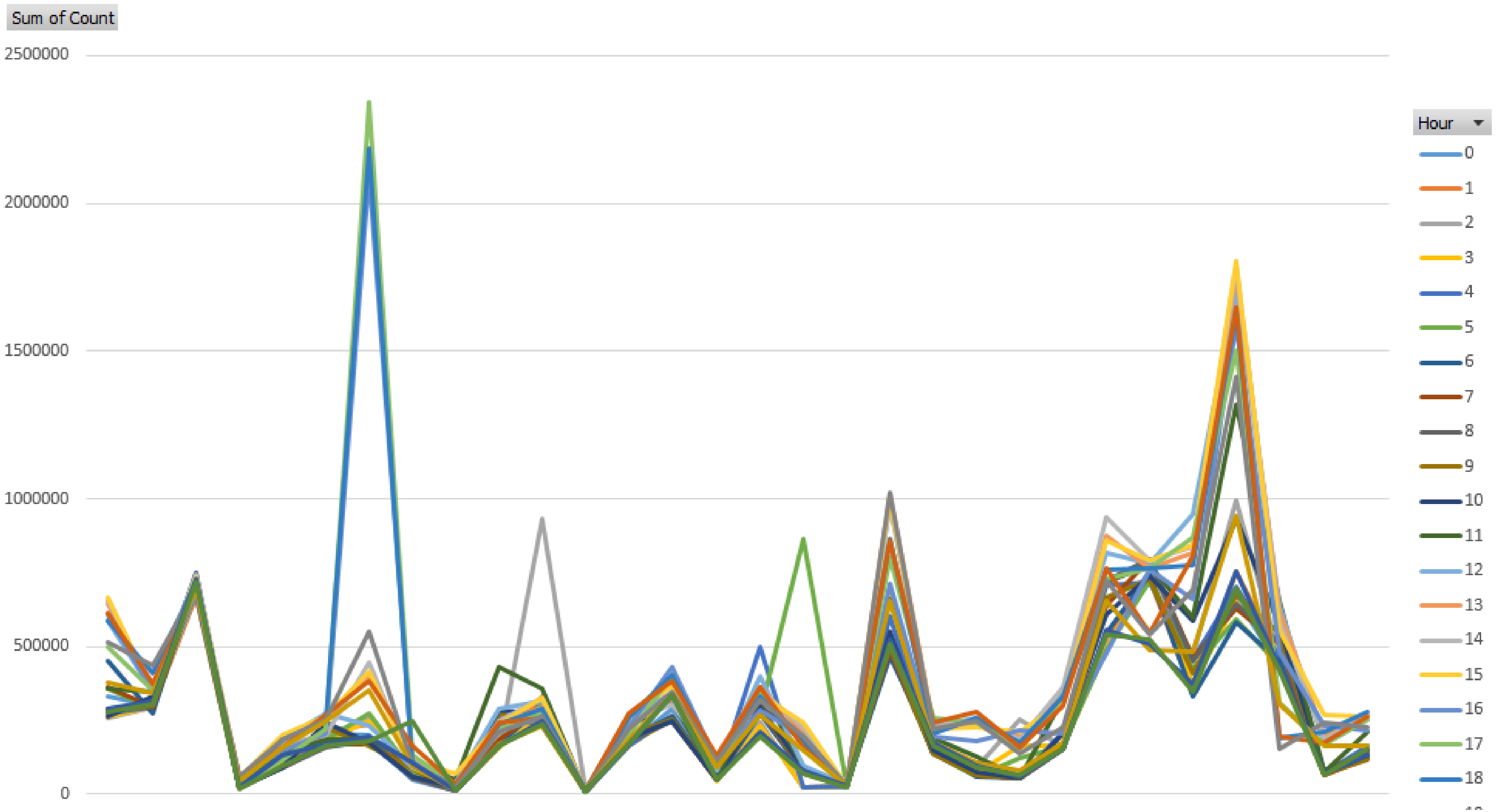


A Unified Security Platform for Threat Detection, Incident Response & Compliance

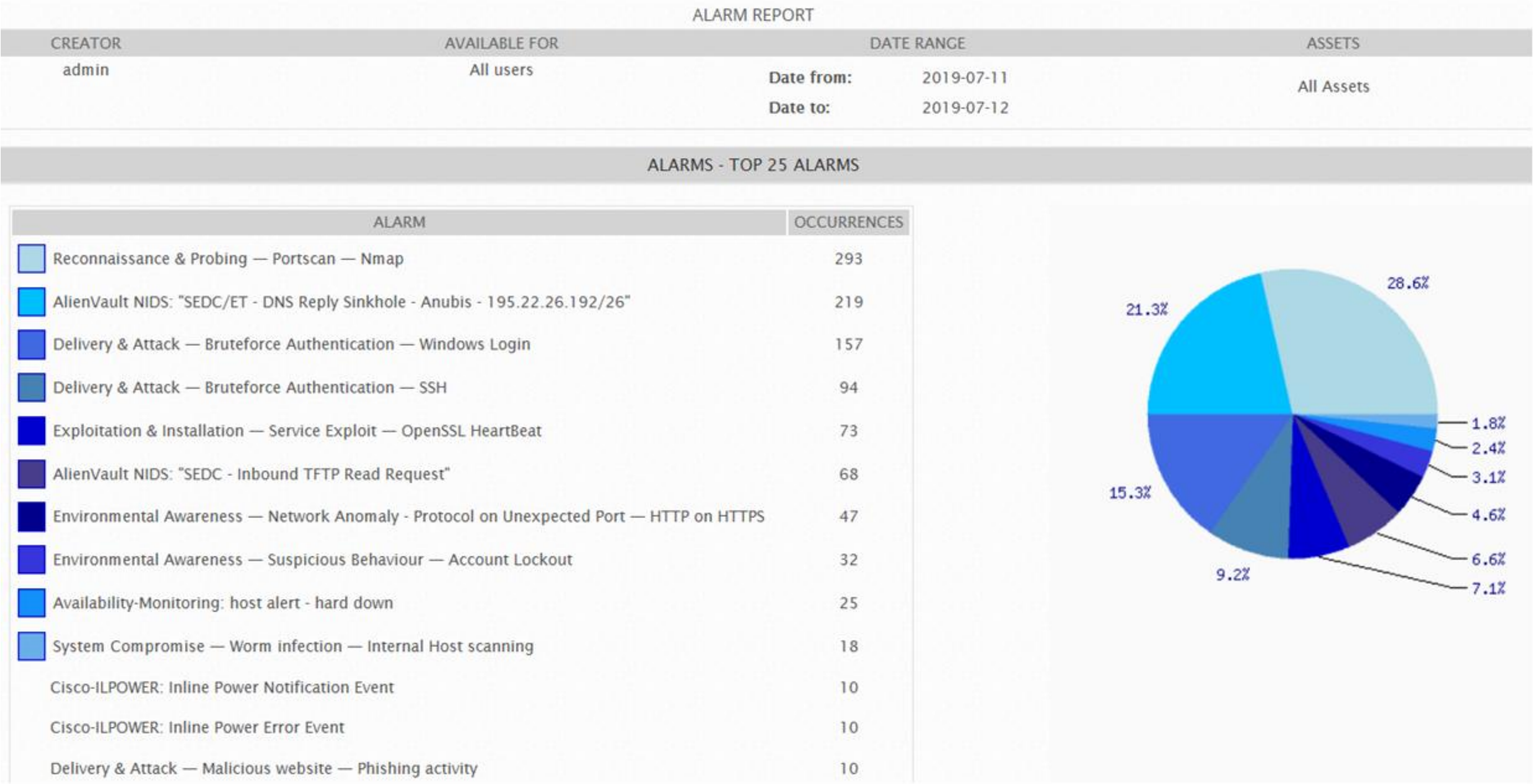
History of SEDC MSS

- SEDC MSS (powered by AlienVault)
  - 3 pilots in Q4 2016
  - Serving 36 utilities today
- SEDC EDR (powered by Carbon Black)
  - Serving 15 utilities today
- SEDC MFA (powered by Duo)
  - Serving 15 utilities today

Millions of Events Daily (36 Clients)



1000+ Alarms Daily (36 Clients)



ALARM REPORT

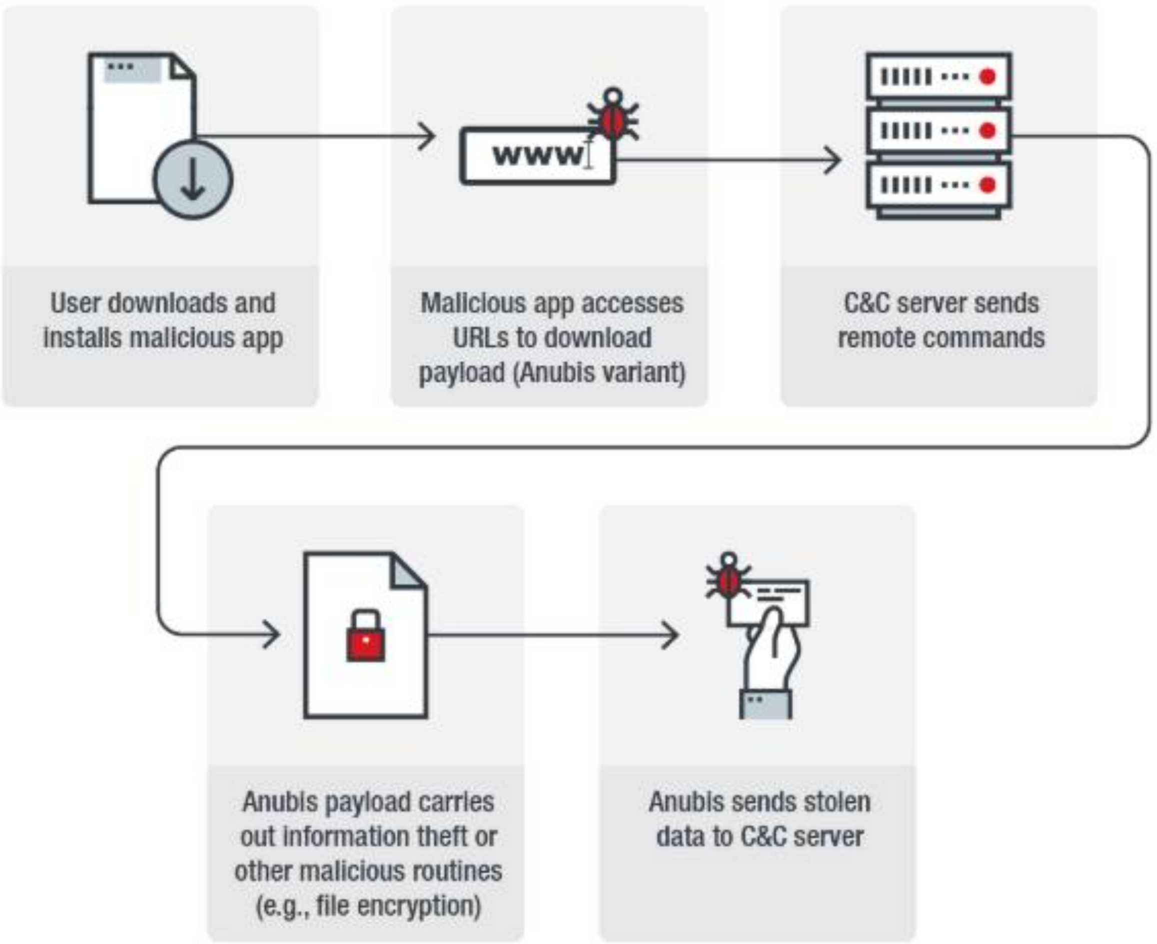
CREATOR	AVAILABLE FOR	DATE RANGE		ASSETS
admin	All users	**Date from:**	2019-07-11	All Assets
		Date to:	2019-07-12	

ALARMS - TOP 25 ALARMS

	ALARM	OCCURRENCES
■	Reconnaissance & Probing — Portscan — Nmap	293
■	AlienVault NIDS: "SEDC/ET - DNS Reply Sinkhole - Anubis - 195.22.26.192/26"	219
■	Delivery & Attack — Bruteforce Authentication — Windows Login	157
■	Delivery & Attack — Bruteforce Authentication — SSH	94
■	Exploitation & Installation — Service Exploit — OpenSSL HeartBeat	73
■	AlienVault NIDS: "SEDC - Inbound TFTP Read Request"	68
■	Environmental Awareness — Network Anomaly - Protocol on Unexpected Port — HTTP on HTTPS	47
■	Environmental Awareness — Suspicious Behaviour — Account Lockout	32
■	Availability-Monitoring: host alert - hard down	25
■	System Compromise — Worm infection — Internal Host scanning	18
	Cisco-ILPOWER: Inline Power Notification Event	10
	Cisco-ILPOWER: Inline Power Error Event	10
	Delivery & Attack — Malicious website — Phishing activity	10

DNS Reply Sinkhole (TP or FP)

- True Positive Alarm
- Malware on Android phone on corporate WiFi contacting DNS sinkhole in Portugal



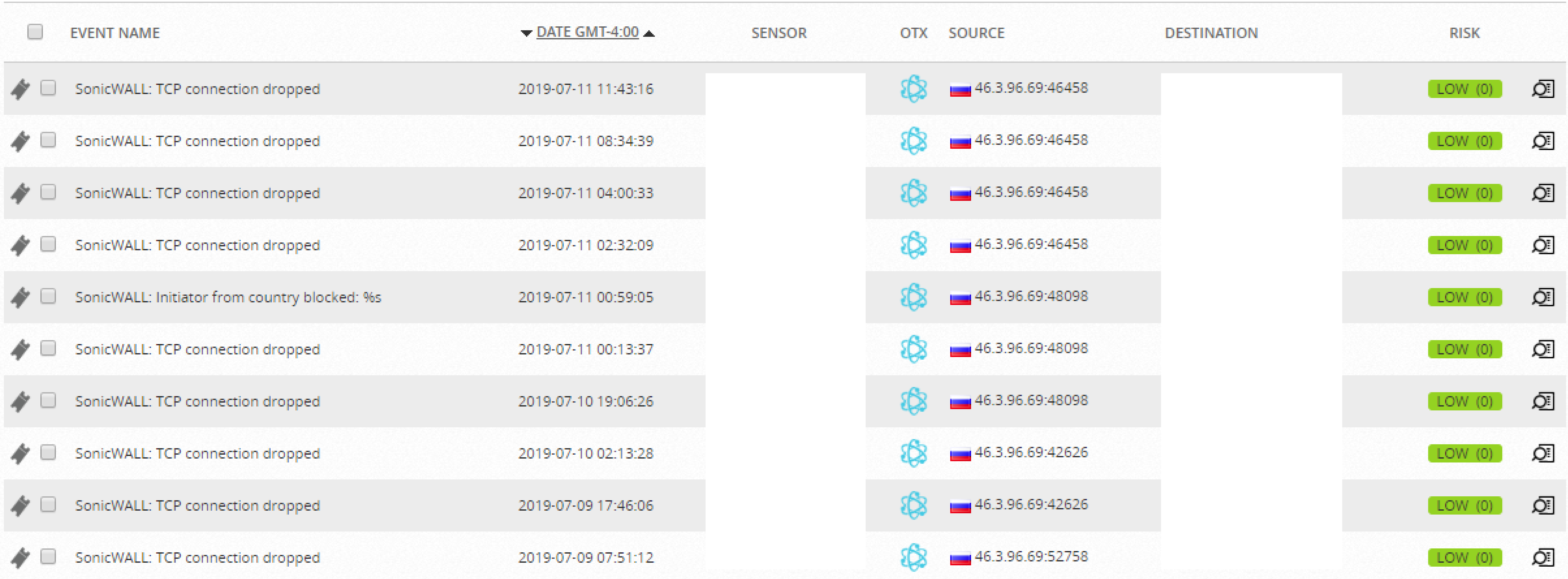
www
User downloads and installs malicious app
Malicious app accesses URLs to download payload (Anubis variant)
C&C server sends remote commands
Anubis payload carries out information theft or other malicious routines (e.g., file encryption)
Anubis sends stolen data to C&C server

https://blog.trendmicro.com/trendlabs-security-intelligence/anubis-android-malware-returns-with-over-17000-samples/#gallery-6

DNS Reply Sinkhole (TP or FP)

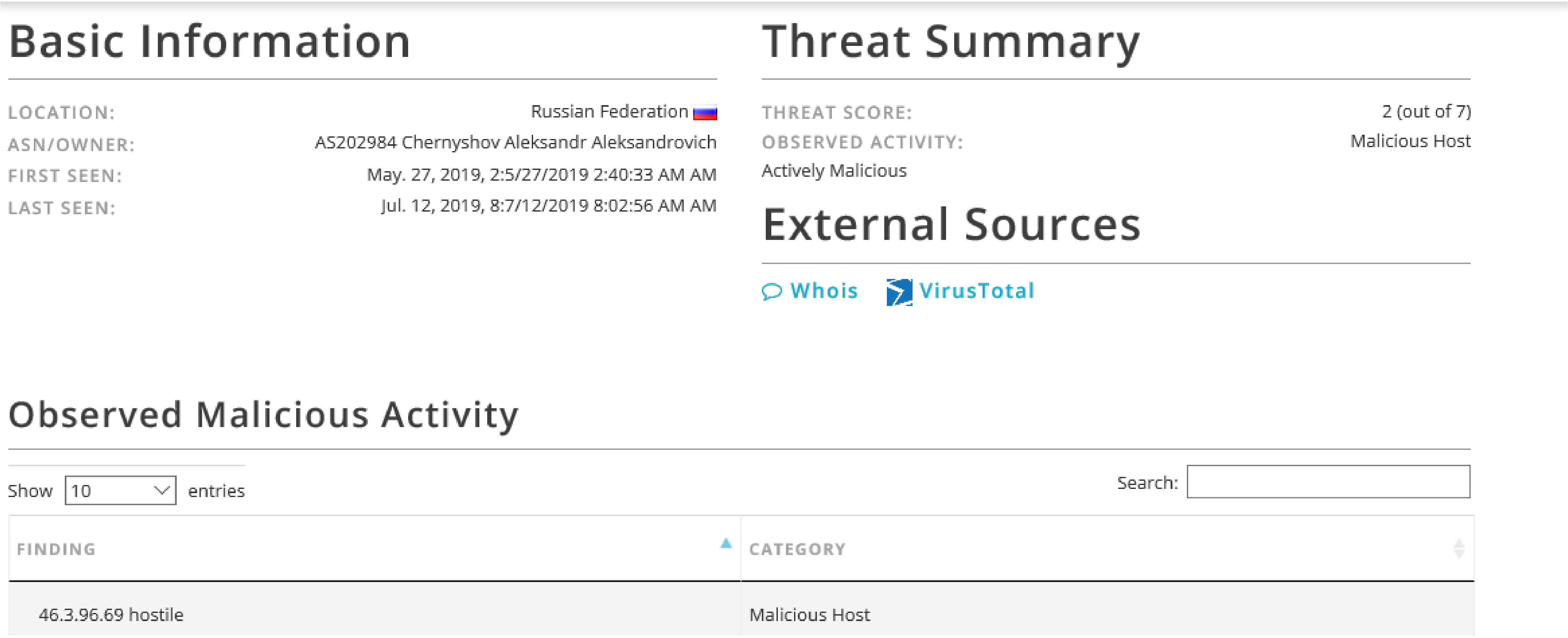
- False Positive Alarm but still sketchy and requires research
- Firewall is making reverse DNS lookups to determine domain name of IP from Russia who was port scanning utility
- Domain registered by Dom Tehniki Ltd. from Russia

False Positive Alarm



□	EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
□	SonicWALL: TCP connection dropped	2019-07-11 11:43:16	[redacted]		46.3.96.69:46458	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-11 08:34:39	[redacted]		46.3.96.69:46458	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-11 04:00:33	[redacted]		46.3.96.69:46458	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-11 02:32:09	[redacted]		46.3.96.69:46458	[redacted]	LOW (0)
□	SonicWALL: Initiator from country blocked: %s	2019-07-11 00:59:05	[redacted]		46.3.96.69:48098	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-11 00:13:37	[redacted]		46.3.96.69:48098	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-10 19:06:26	[redacted]		46.3.96.69:48098	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-10 02:13:28	[redacted]		46.3.96.69:42626	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-09 17:46:06	[redacted]		46.3.96.69:42626	[redacted]	LOW (0)
□	SonicWALL: TCP connection dropped	2019-07-09 07:51:12	[redacted]		46.3.96.69:52758	[redacted]	LOW (0)

False Positive Alarm



Basic Information

LOCATION: Russian Federation 🇷🇺

ASN/OWNER: AS202984 Chernyshov Aleksandr Aleksandrovich

FIRST SEEN: May. 27, 2019, 2:5/27/2019 2:40:33 AM AM

LAST SEEN: Jul. 12, 2019, 8:7/12/2019 8:02:56 AM AM

Threat Summary

THREAT SCORE: 2 (out of 7)

OBSERVED ACTIVITY: Malicious Host

Actively Malicious

External Sources

Whois VirusTotal

Observed Malicious Activity

Show 10 entries

Search:

FINDING	CATEGORY
46.3.96.69 hostile	Malicious Host

The Importance of Threat Intelligence

THREAT	DISCOVERED	AVAILABLE FOR ALIENVAULT CUSTOMERS	TIME TO DETECTION ABILITY IN USM
Meltdown / Spectre	January 3, 2018	January 4, 2018	1 day
“Petya” / NotPetya	June 27, 2017	June 27, 2017	Same day
WannaCry	May 12, 2017	May 12, 2017	Same day
Samba CVE-2017-7494	May 25, 2017	May 25, 2017	Same day
EternalBlue	April 14, 2017	April 18, 2017	4 days
WordPress Content Injection	February 1, 2017	January 26, 2017	6 days BEFORE
Adobe 0-day (CVE-2015-0311)	January 22, 2015	November 16, 2014**	3 months BEFORE

SEDC MSS: Threat Intel Feeds

OTX
OPEN THREAT EXCHANGE

OVER 19 MILLION THREAT INDICATORS CONTRIBUTED DAILY

EMERGING THREATS
now part of proofpoint

SEDC

U.S. DEPARTMENT OF HOMELAND SECURITY

INFRAGARD
MEMBERS ALLIANCE
ATLANTA

Bit9 + CARBON BLACK
SOFTWARE REPUTATION TRUST

Cb REPUTATION THREAT

National Vulnerability Database
nvd.nist.gov

abuse.ch
The Swiss Security Blog

Cb ADVANCED THREAT

SANS

THREATCONNECT

Tor

Cb KNOWN IOC FEED

ThreatExchange

SEDC SOC - Atlanta, GA

SEDC MSS (Managed Security Services)

Why SEDC MSS?

- SEDC MSS is Cost Effective
  - Under SEDC umbrella, utility gains Security Operations Center (SOC) experts at a fraction of the cost
- 24x7 monitoring
  - of your network so you don’t have to…
- PCI-DSS
  - Satisfy 37+ of the most challenging PCI-DSS requirements while improving the security of your network

SEDC MSS Demo

Sign up with SEDC MSS!

Please contact
techsales@sedata.com or
cri@sedata.com

CERTIFIED MSSP PARTNER ™