CyberRes

Open Text Cyber Security

Logging and Investigation

With ArcSight Recon

鉅晶國際JJNET

Market Statistics

207	Average days to identify a breach in 2020*
315	Average days from malicious attack breach to containment*
69%	Companies see compliance mandates driving spending**
50%	Companies believed they were GDPR compliant by end of 2018***

* 2020 Cost of a Data Breach Report – Ponemon Institute, IBM
** 2019 Cost of a Data Breach Report – Ponemon Institute, IBM
*** 50 Percent of Firms Still Not GDPR Compliant: How About Your Data Center? –Data Center Frontier

ArcSight Recon - Log Storage for Today’s SOC

Unified Storage

Threat Hunting

Reporting

Intelligent Log Storage

Enhanced Visibility

Intelligent Log Storage

Unified Storage

- Collect, store and use data across the organization

Threat Hunting

- Powerful investigation tools and technology

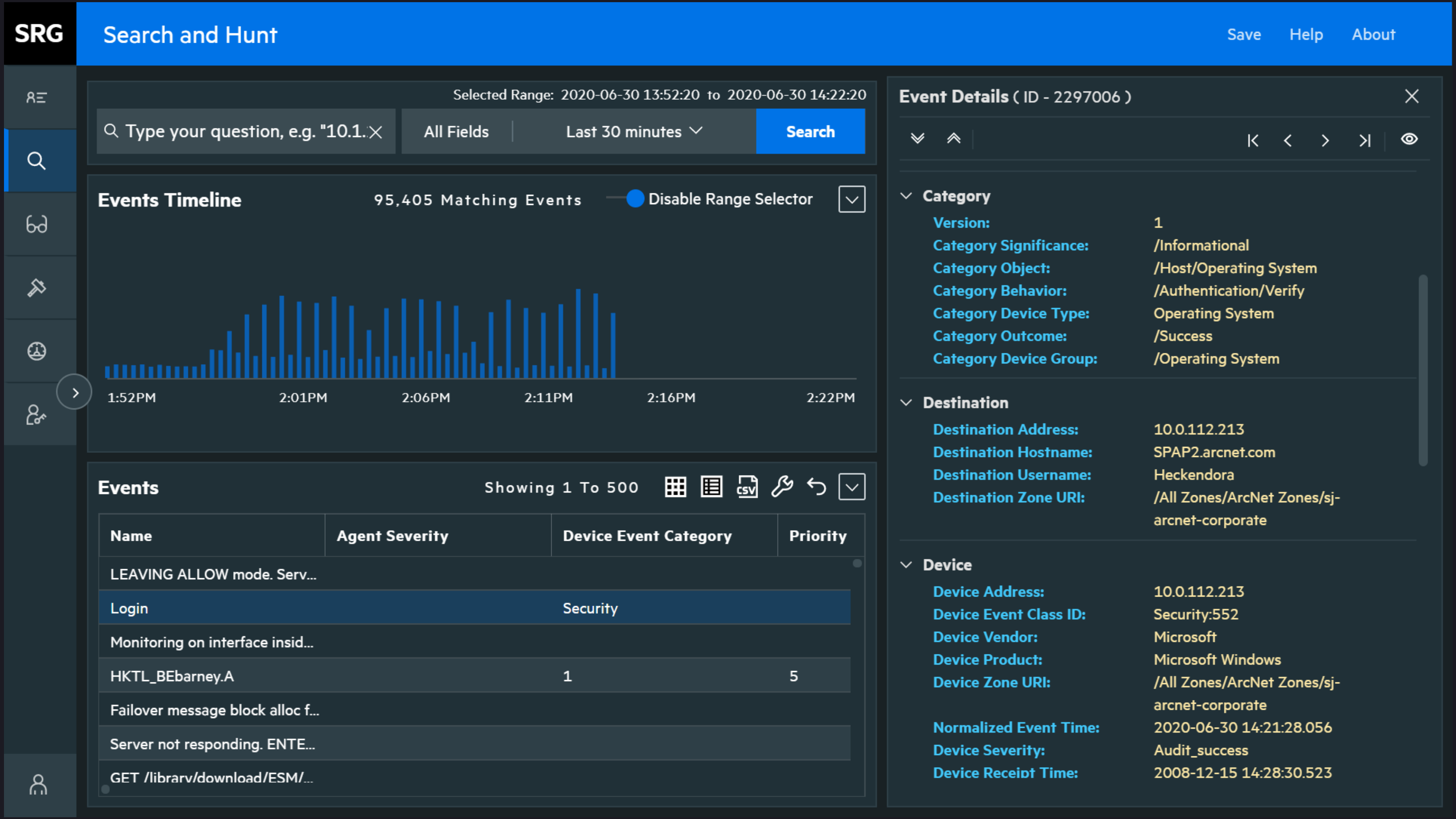
Compliance Reporting

- Reporting templates for compliance and MITRE alignment

Scalable and Customizable

- Works with minimal infrastructure, scales as needed

ArcSight Recon



Selected Range: 2020-06-30 13:52:20 to 2020-06-30 14:22:20

95,405 Matching Events

Showing 1 To 500

Name	Agent Severity	Device Event Category	Priority
LEAVING ALLOW mode. Serv...			
Login		Security	
Monitoring on interface insid...			
HKTL_BEbarney.A		1	5
Failover message block alloc f...			
Server not responding. ENTE...			
GET /library/download/ESM/...			

Event Details (ID - 2297006)

Category

Version:	1
Category Significance:	/Informational
Category Object:	/Host/Operating System
Category Behavior:	/Authentication/Verify
Category Device Type:	Operating System
Category Outcome:	/Success
Category Device Group:	/Operating System

Destination

Destination Address:	10.0.112.213
Destination Hostname:	SPAP2.arcnet.com
Destination Username:	Heckendora
Destination Zone URI:	/All Zones/ArcNet Zones/sj-arcnet-corporate

Device

Device Address:	10.0.112.213
Device Event Class ID:	Security:552
Device Vendor:	Microsoft
Device Product:	Microsoft Windows
Device Zone URI:	/All Zones/ArcNet Zones/sj-arcnet-corporate
Normalized Event Time:	2020-06-30 14:21:28.056
Device Severity:	Audit_success
Device Receipt Time:	2008-12-15 14:28:30.523

ArcSight Recon

KUP LIST (0 fields)

All Fields

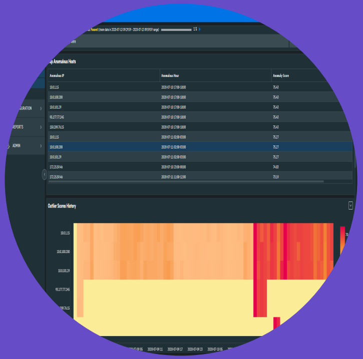
+ CREATE NEW

- ☑ Agent DNS Domain
- ☑ Agent Receipt Time
- ☑ Agent Translated Zone URI
- ☑ Application Protocol
- ☑ Category Behavior
- ☑ Category Significance
- ☑ Customer URI
- ☑ Destination Geo Longitude
- ☑ Destination Mac Address
- Destination Service Name
- ☑ Agent Hostname
- ☑ Agent Severity
- ☑ Agent Type
- ☑ Base Event Count
- ☑ Category Device Group
- ☑ Category Technique
- ☑ Destination Address
- ☑ Destination Geo Postal Co...
- ☑ Destination NT Domain
- ☑ Destination Translated Ad...
- ☑ Agent ID
- ☑ Agent Timezone
- ☑ Agent Version
- ☑ Base Event Ids
- ☑ Category Device Type
- ☑ Correlated Event Id
- ☑ Destination DNS Domain
- ☑ Destination Geo Region C...
- ☑ Destination Port
- ☑ Destination Translated Port

SecurityLog 3

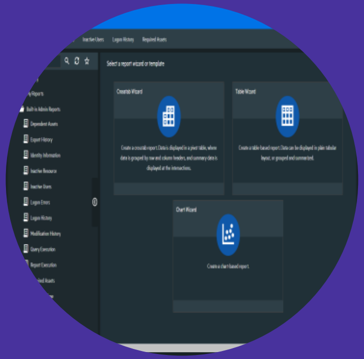
Unified Storage

- Shared Schema
- Centralized



Threat Hunting

- Speed
- Visualizations
- Insights



Compliance Reporting

- Reporting
- MITRE ATT&CK Reports

Security Devices
Cloud Services
Applications
Web Data
Ric
k Traffic

Scalable Infrastructure

- Growth
- Integration

Unified Storage

Shared Schema

- Shared schema to use data across all ArcSight solutions

Centralized

- Collect once, store once, use often

Analysis

Speed

- Distributed searching across all Recon nodes
- Smart suggestion to help build queries
- Big Data search technology embedded for faster search results

Visualizations

- Choose the visualization that suites your data
- Drill-down visualizations for ease-of-use

Insights

- Use pre-built data science packages to amplify your threat hunting

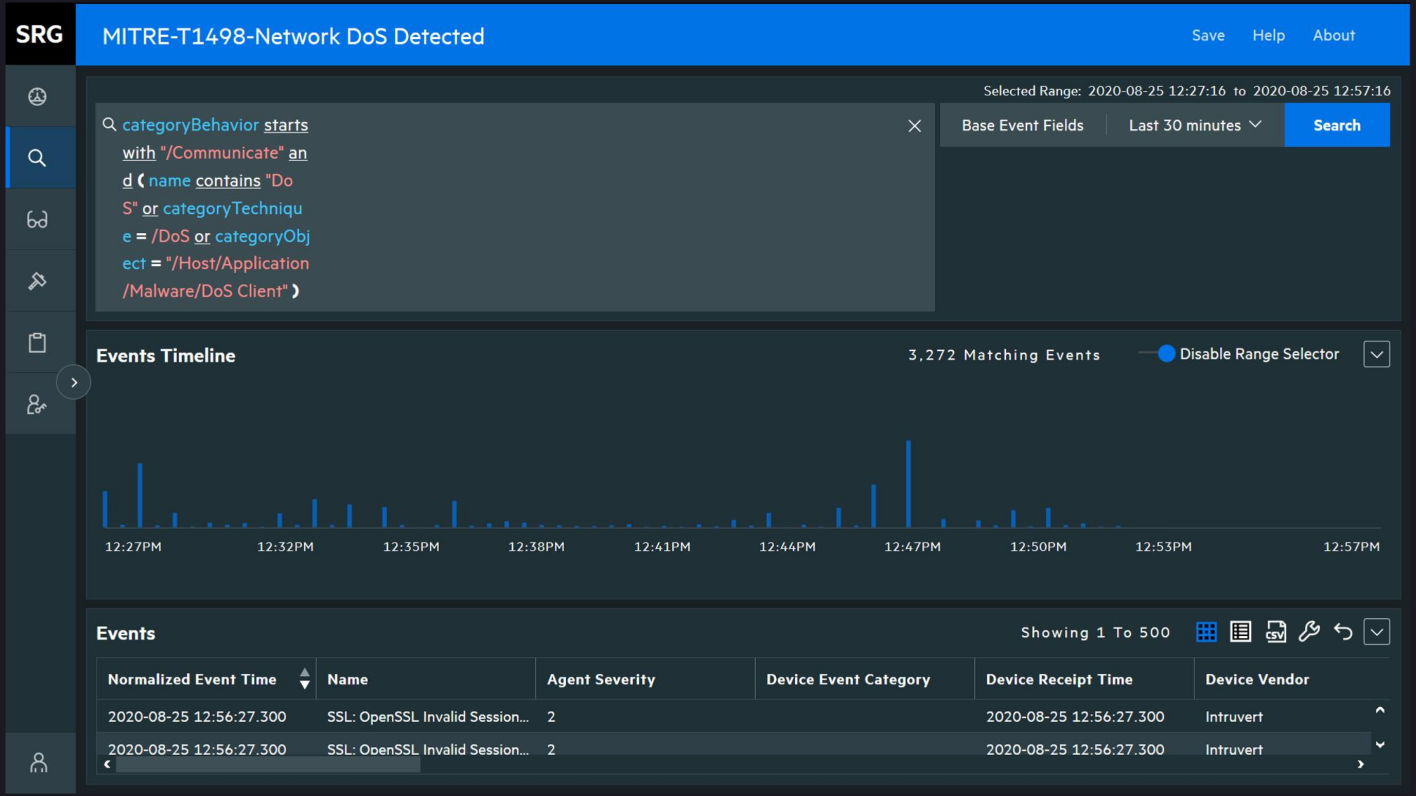
Compliance

Reporting

- Pre-built reports assist in documenting security compliance

MITRE ATT&CK Reports

- Pre-built reports aligned to MITRE Framework



MITRE-T1498-Network DoS Detected

Selected Range: 2020-08-25 12:27:16 to 2020-08-25 12:57:16

```
categoryBehavior starts with "/Communicate" and ( name contains "DoS" or categoryTechnique = /DoS or categoryObject = "/Host/Application/Malware/DoS Client" )
```

Events Timeline

3,272 Matching Events

Events

Showing 1 To 500

Normalized Event Time	Name	Agent Severity	Device Event Category	Device Receipt Time	Device Vendor
2020-08-25 12:56:27.300	SSL: OpenSSL Invalid Session...	2		2020-08-25 12:56:27.300	Intruvert
2020-08-25 12:56:27.300	SSL: OpenSSL Invalid Session...	2		2020-08-25 12:56:27.300	Intruvert

Scale

Growth

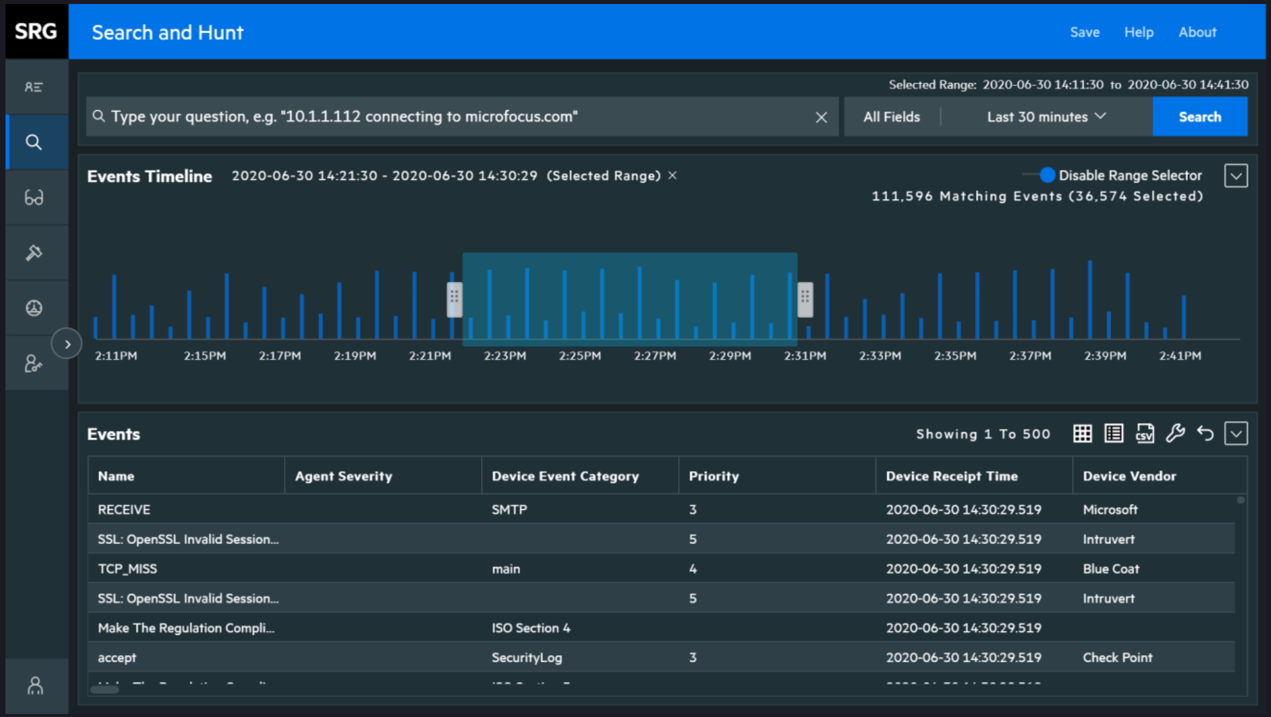
- Recon can be deployed on a single machine
- Multiple nodes work together to support extremely high event volume

Integration

- Recon integrates with many top-rated 3rd party solutions

  (integrations in the ArcSight Marketplace)

Search Interface



Selected Range: 2020-06-30 14:11:30 to 2020-06-30 14:41:30

Type your question, e.g. "10.1.1.112 connecting to microfocus.com"

Events Timeline 2020-06-30 14:21:30 - 2020-06-30 14:30:29 (Selected Range)

111,596 Matching Events (36,574 Selected)

Events Showing 1 To 500

Name	Agent Severity	Device Event Category	Priority	Device Receipt Time	Device Vendor
RECEIVE		SMTP	3	2020-06-30 14:30:29.519	Microsoft
SSL: OpenSSL Invalid Session...			5	2020-06-30 14:30:29.519	Intruvert
TCP_MISS		main	4	2020-06-30 14:30:29.519	Blue Coat
SSL: OpenSSL Invalid Session...			5	2020-06-30 14:30:29.519	Intruvert
Make The Regulation Compli...		ISO Section 4		2020-06-30 14:30:29.519	
accept		SecurityLog	3	2020-06-30 14:30:29.519	Check Point

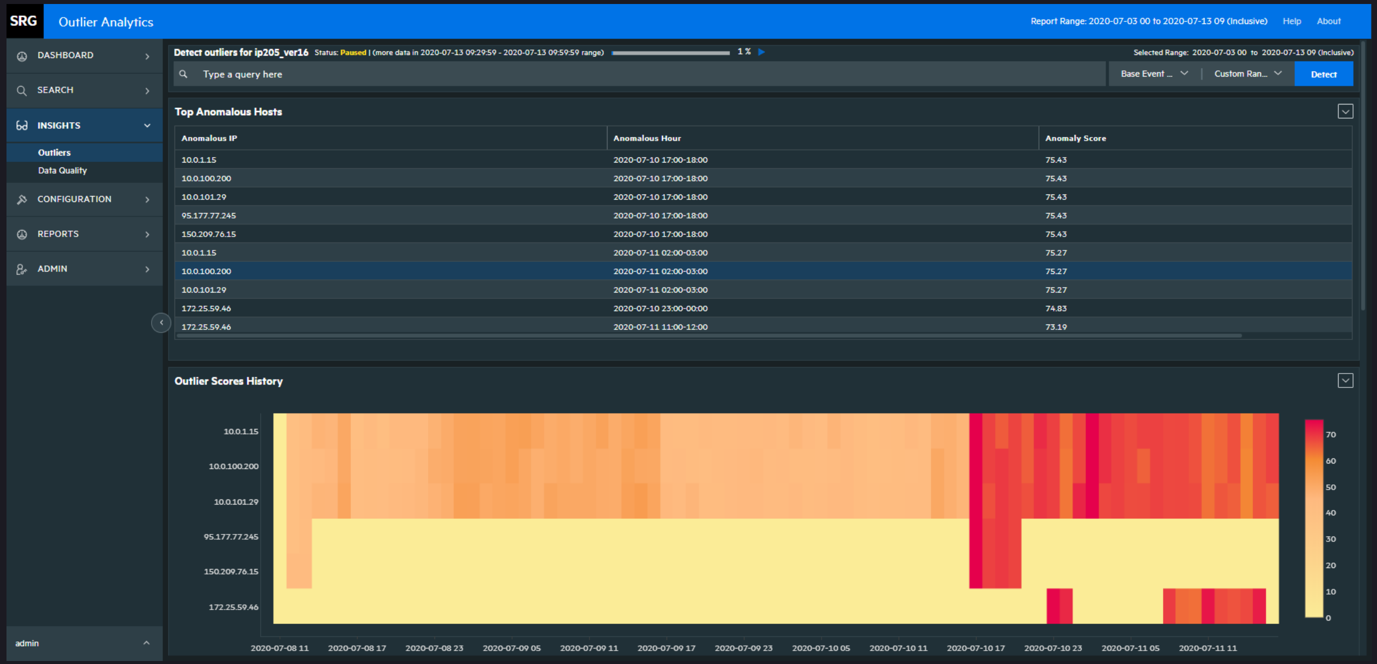
User Friendly Search:

- Grid display
- Message view
- Time-based histograms
- Dynamic query suggestions
- Raw message view

CyberRes

Outlier Detection

- Visualize deviations from baseline host behaviors



Detect outliers for ip205_ver16 Status: Paused | (more data in 2020-07-13 09:29:59 - 2020-07-13 09:59:59 range) 1 %

Selected Range: 2020-07-03 00 to 2020-07-13 09 (Inclusive)

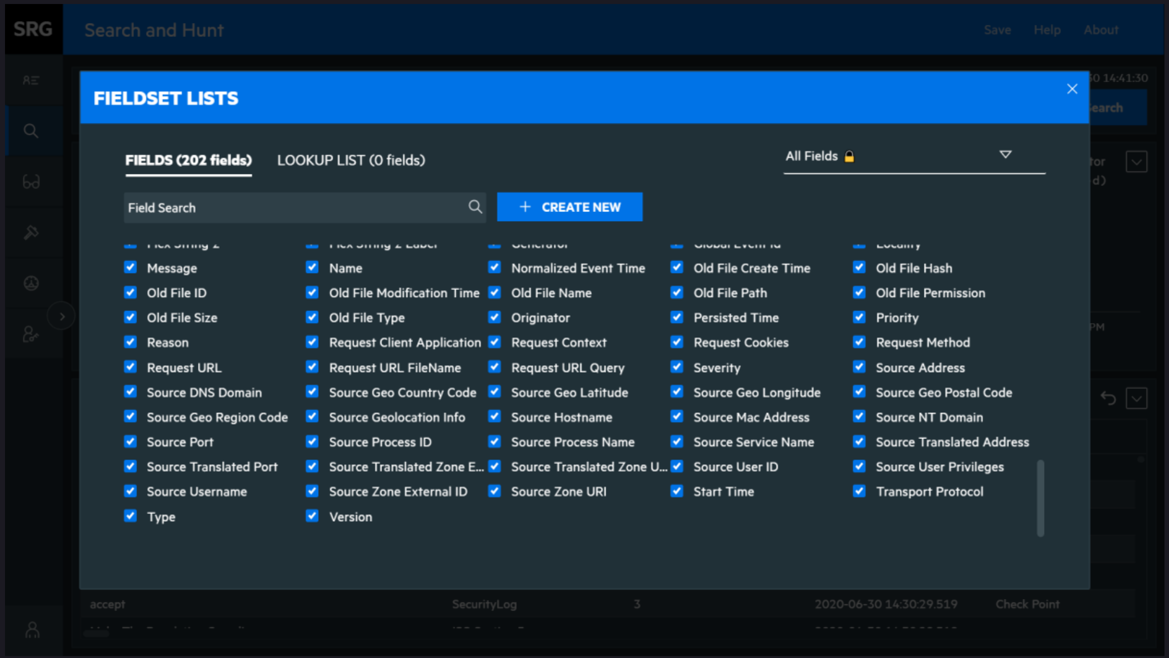
Top Anomalous Hosts

Anomalous IP	Anomalous Hour	Anomaly Score
10.0.1.15	2020-07-10 17:00-18:00	75.43
10.0.100.200	2020-07-10 17:00-18:00	75.43
10.0.101.29	2020-07-10 17:00-18:00	75.43
95.177.77.245	2020-07-10 17:00-18:00	75.43
150.209.76.15	2020-07-10 17:00-18:00	75.43
10.0.1.15	2020-07-11 02:00-03:00	75.27
10.0.100.200	2020-07-11 02:00-03:00	75.27
10.0.101.29	2020-07-11 02:00-03:00	75.27
172.25.59.46	2020-07-10 23:00-00:00	74.83
172.25.59.46	2020-07-11 11:00-12:00	73.19

Outlier Scores History

CyberRes

Unified Schema



FIELDSET LISTS

FIELDS (202 fields) LOOKUP LIST (0 fields)

All Fields

Field Search

+ CREATE NEW

☑ Flex String 2 ☑ Flex String 2 Label ☑ Generator ☑ Global Event Id ☑ Locality
☑ Message ☑ Name ☑ Normalized Event Time ☑ Old File Create Time ☑ Old File Hash
☑ Old File ID ☑ Old File Modification Time ☑ Old File Name ☑ Old File Path ☑ Old File Permission
☑ Old File Size ☑ Old File Type ☑ Originator ☑ Persisted Time ☑ Priority
☑ Reason ☑ Request Client Application ☑ Request Context ☑ Request Cookies ☑ Request Method
☑ Request URL ☑ Request URL FileName ☑ Request URL Query ☑ Severity ☑ Source Address
☑ Source DNS Domain ☑ Source Geo Country Code ☑ Source Geo Latitude ☑ Source Geo Longitude ☑ Source Geo Postal Code
☑ Source Geo Region Code ☑ Source Geolocation Info ☑ Source Hostname ☑ Source Mac Address ☑ Source NT Domain
☑ Source Port ☑ Source Process ID ☑ Source Process Name ☑ Source Service Name ☑ Source Translated Address
☑ Source Translated Port ☑ Source Translated Zone E... ☑ Source Translated Zone U... ☑ Source User ID ☑ Source User Privileges
☑ Source Username ☑ Source Zone External ID ☑ Source Zone URI ☑ Start Time ☑ Transport Protocol
☑ Type ☑ Version

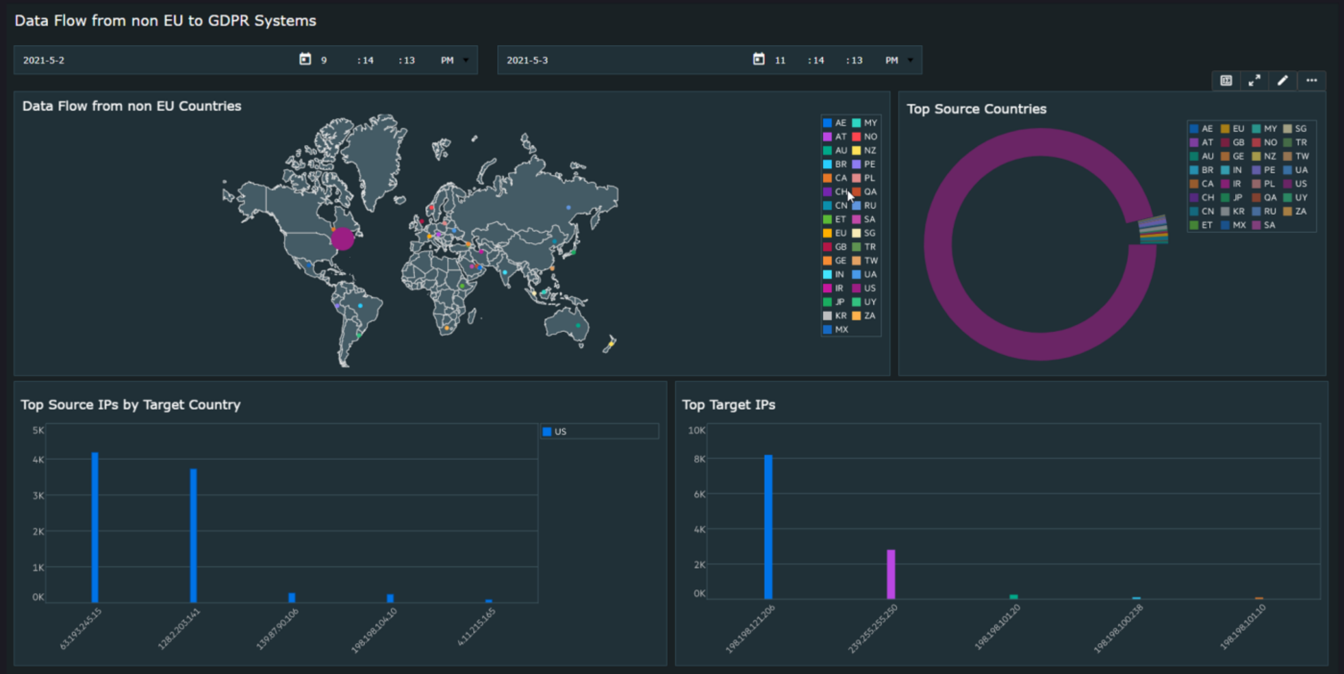
accept SecurityLog 3 2020-06-30 14:30:29.519 Check Point

- Enables routing, filtering, storage for all ArcSight Products

Compliance Reporting

Reporting Content Packages:

- Create, edit and publish reports
- Reporting for compliance including IT-GOV, GDPR, PCI
- MITRE Framework reports



Data Flow from non EU to GDPR Systems

2021-5-2 9 :14 :13 PM

2021-5-3 11 :14 :13 PM

Data Flow from non EU Countries
AE MY AT NO AU NZ BR PE CA PL CH QA CN RU ET SA EU SG GB TR GE TW IN UA IR US JP UY KR ZA MX
Top Source Countries
AE EU MY SG AT GB NO TR AU GE NZ TW BR IN PE UA CA IR PL US CH JP QA UY CN KR RU ZA ET MX SA
Top Source IPs by Target Country
5K
4K
3K
2K
1K
0K
US
63.193.245.15
128.2.203.141
139.87.90.106
198.198.104.10
4.11.215.165
Top Target IPs
10K
8K
6K
4K
2K
0K
198.198.121.206
239.255.255.250
198.198.101.20
198.198.100.238
198.198.101.10

CyberRes

What’s New: Recon 1.5 & Recon SaaS*

ArcSight Recon

ArcSight Recon on SaaS*

- In addition to Recon SaaS, Recon supports cloud-native deployment in Azure and AWS

Read Logger Data

- **Recon search** of Logger event data is now enabled

Compliance Packages

- Pre-Built content for IT-GOV, GDPR and PCI

Out of the Box Reports

- 100+ out of the box reports including MITRE ATT&CK, Cloud, Monitoring, OWASP

*ArcSight Recon SaaS will GA by July 14, 2021

Thank You.