
logpoint

Radpoint Summit 2017:

Etablera insyn och kontroll med SIEM

Tim Aronsson

Account Manager, LogPoint

Henrik Berggren

Technical Manager, LogPoint

logpoint

LogPoint Introduction

- Scandinavian SIEM vendor, European focus
- Headquartered in Copenhagen, Denmark
- 120 Employees : 90 developers, 30 sales
- Sales Offices in DK, SE, UK, DE, CH, FR

SOC Services

GDPR

PCI DSS

SECURITY ANALYSIS

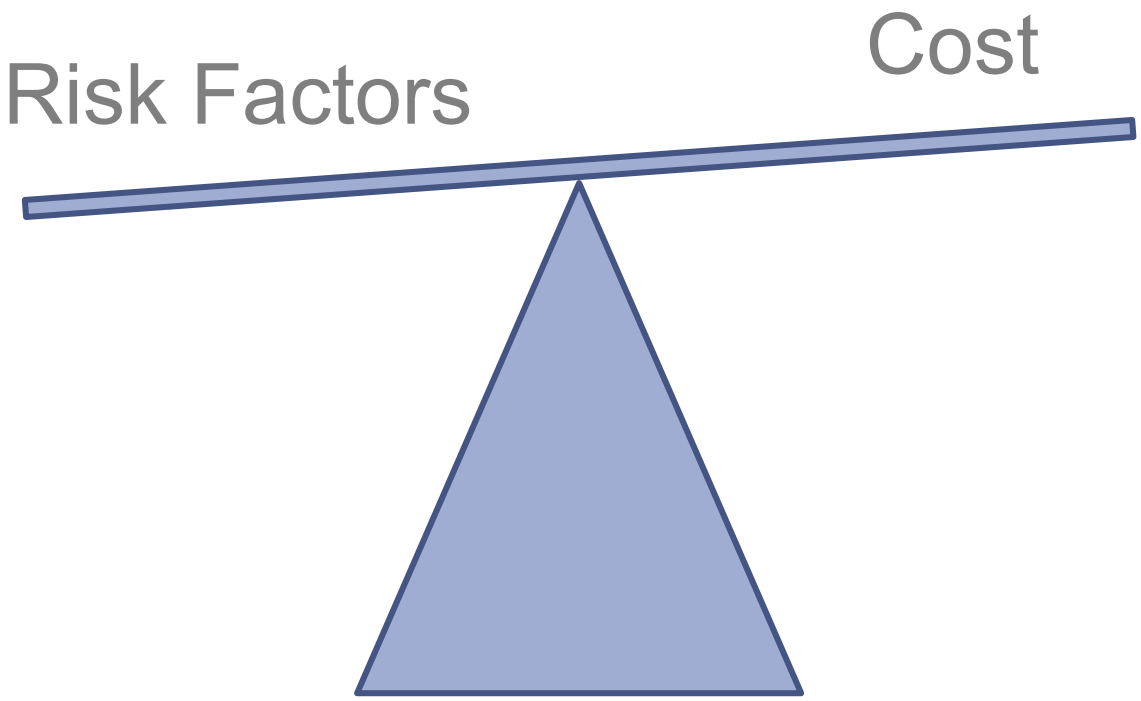
ISO27001

WHAT IS RISK?

The Perfect Storm?

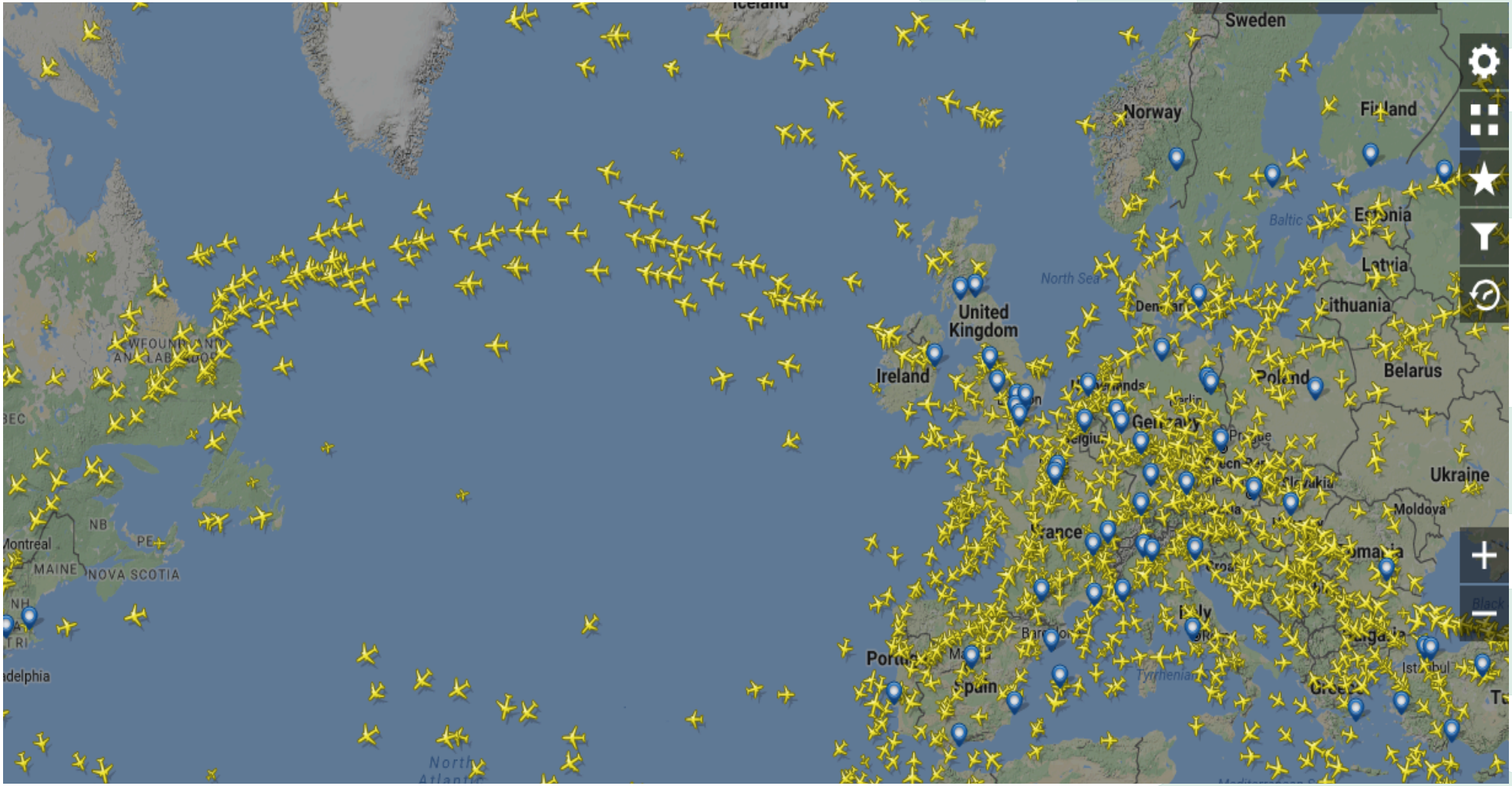
- Ever expanding complex networks
- Increasing data volumes
- Multi-vendor security landscapes
- Lack of skilled expertise
- Growing threat levels - cyber crime
- Huge financial impact for data loss (GDPR)

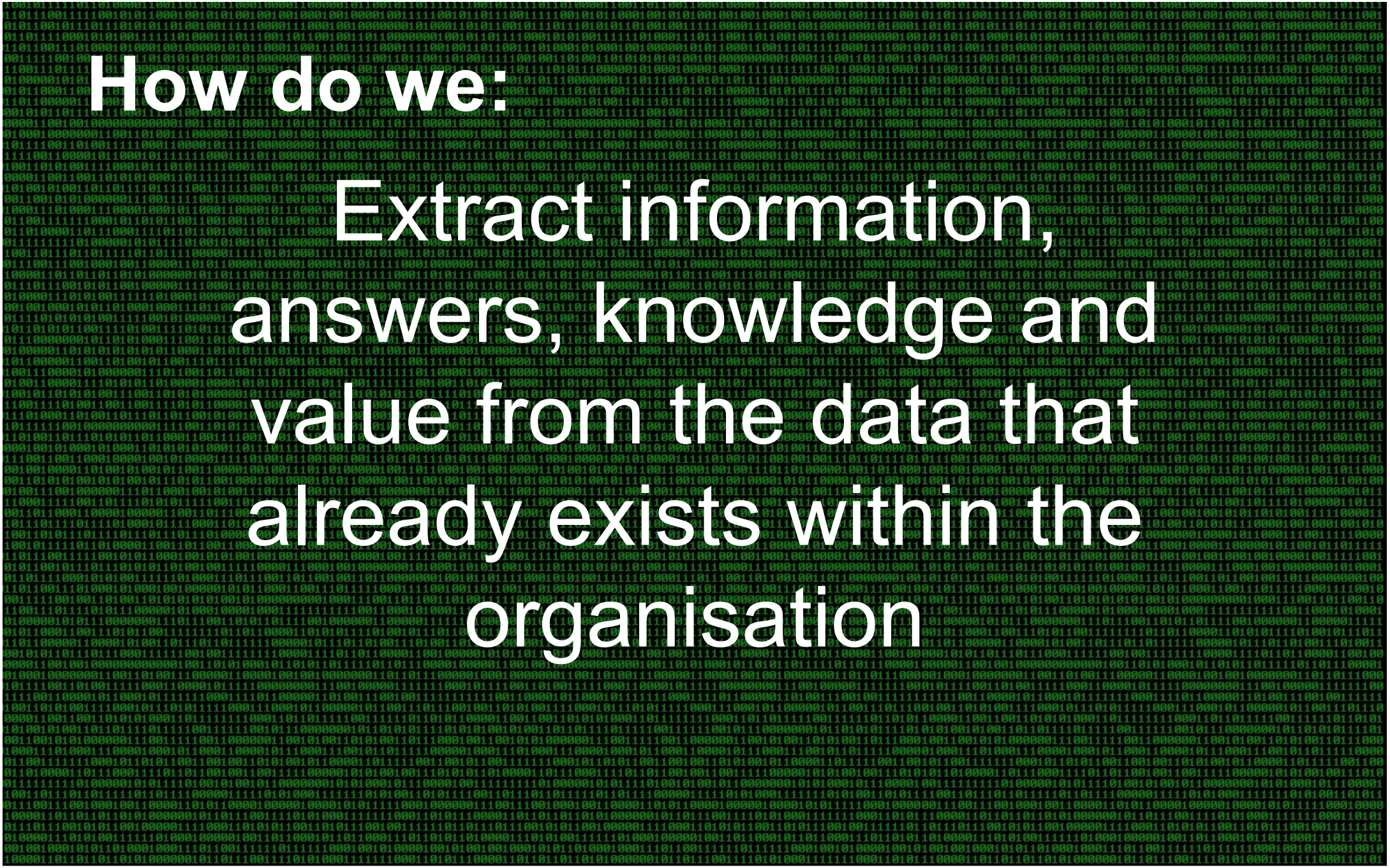
Models for managing risk…



Based on Information!

WHAT IS SIEM?


Sweden
Norway
Finland
Estonia
Latvia
Lithuania
Belarus
United Kingdom
Ireland
Poland
Ukraine
Moldova
France
Spain
Portugal
Italy
Romania
Greece
Istanbul
North Sea
Baltic Sea
Tyrrhenian
Montreal
MAINE
NOVA SCOTIA
NB
PE
NH


How do we:
Extract information, answers, knowledge and value from the data that already exists within the organisation

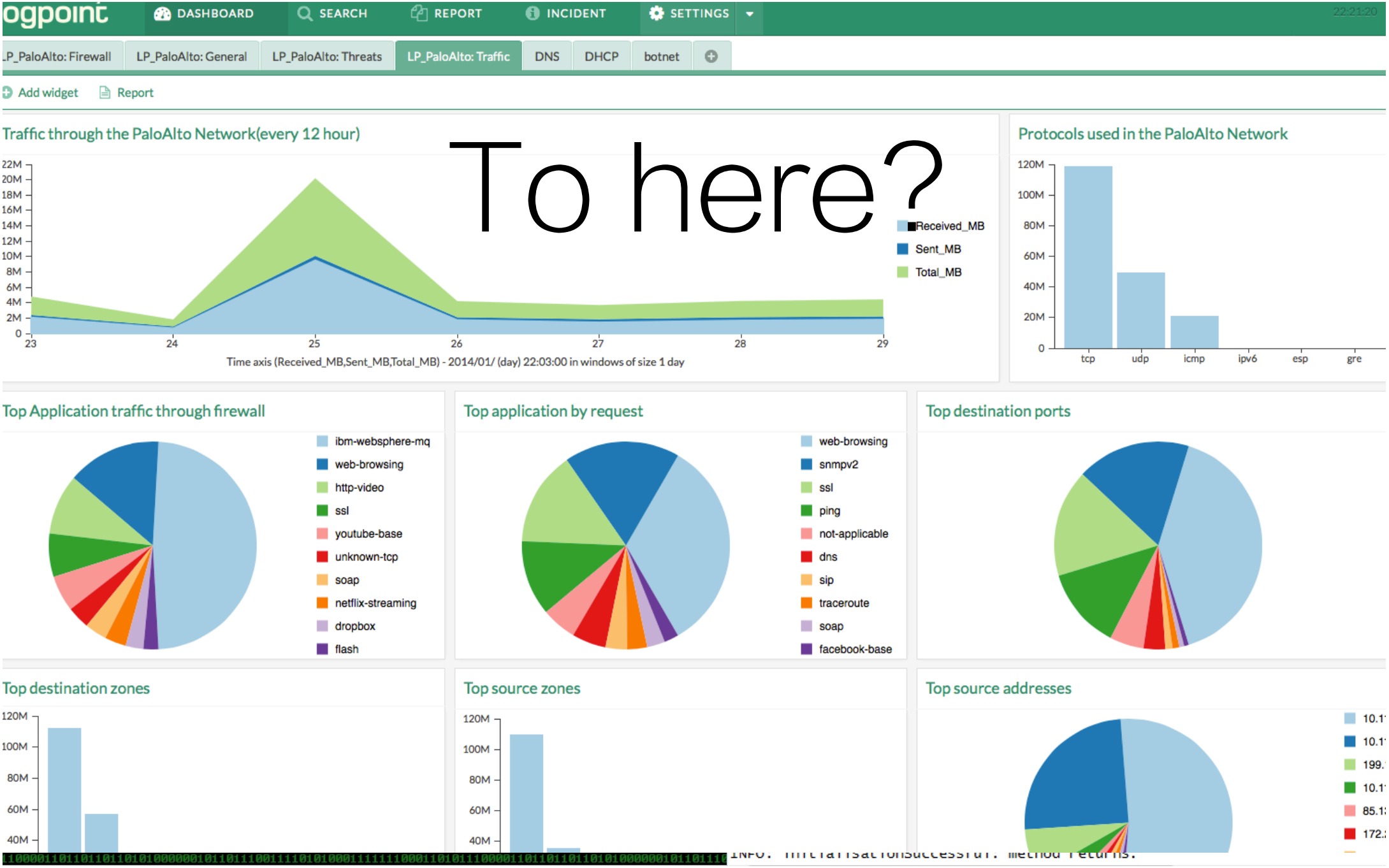
Decentralized logging
– Problematic areas

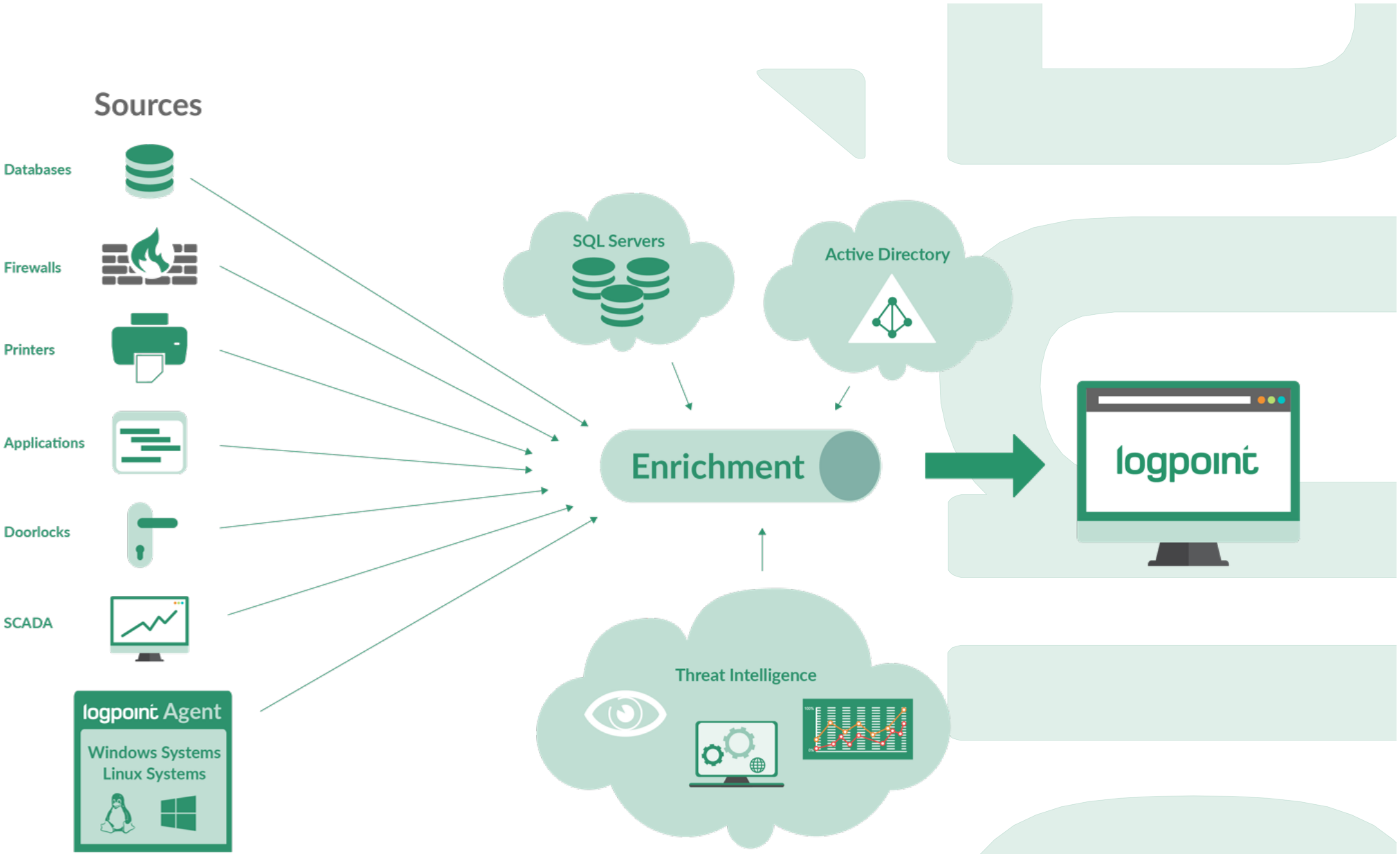
- Separate logging of different systems
  - *Eg searching in AD requires manual search of X logs*
- Some logs and systems are not handled today
- Difficult and timeconsuming to search information
  - *Eg up to X working days for basic reports*
- No overview of the entire environment
- Highly dependent on individual employees
- (Way) too short retention times on some systems

logpoint

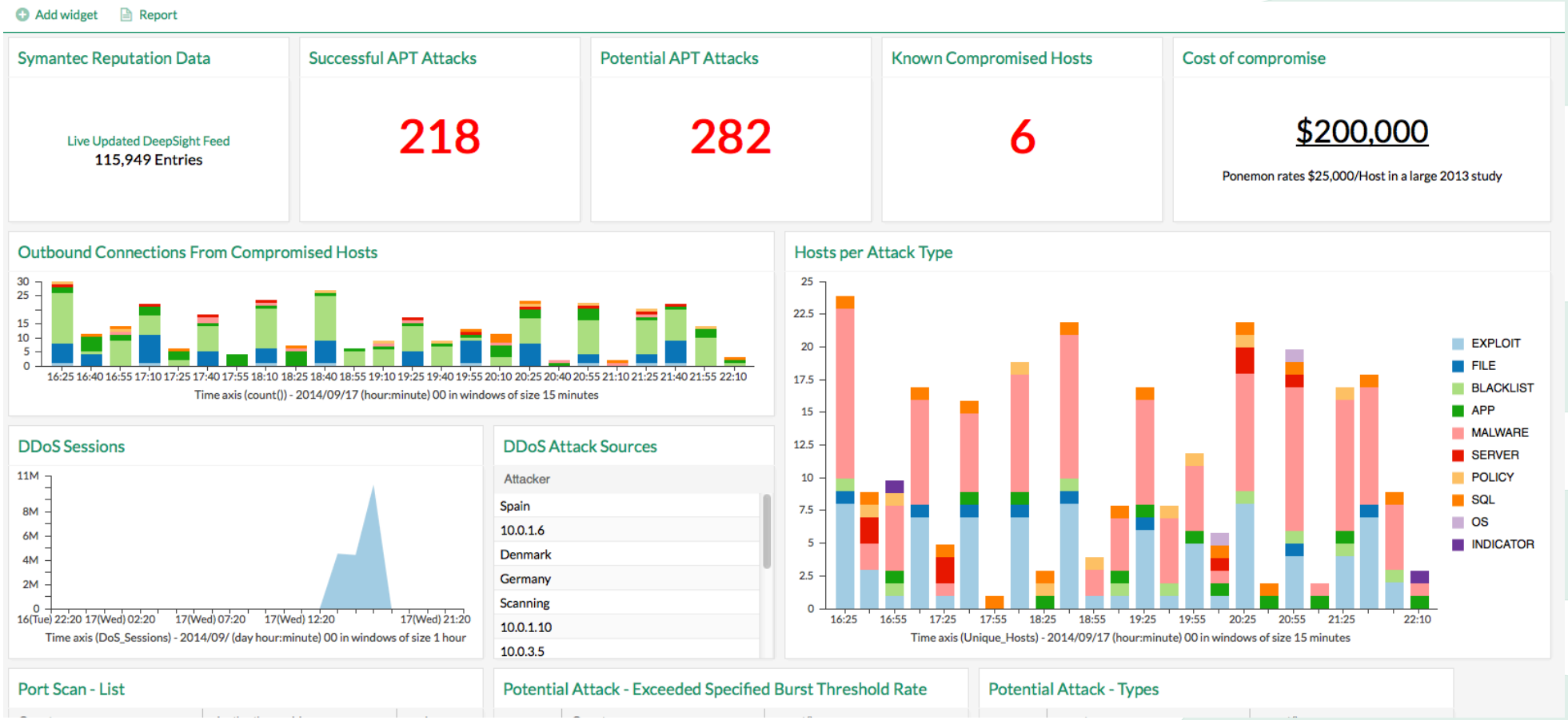
”Can you go get the…, please?”

Easy! Row 19, Shelf 23!


ogpoint
DASHBOARD
SEARCH
REPORT
INCIDENT
SETTINGS
22:21:20
LP_PaloAlto: Firewall
LP_PaloAlto: General
LP_PaloAlto: Threats
LP_PaloAlto: Traffic
DNS
DHCP
botnet
Add widget
Report
Traffic through the PaloAlto Network(every 12 hour)
To here?
22M
20M
18M
16M
14M
12M
10M
8M
6M
4M
2M
0
23
24
25
26
27
28
29
Received_MB
Sent_MB
Total_MB
Time axis (Received_MB,Sent_MB,Total_MB) - 2014/01/ (day) 22:03:00 in windows of size 1 day
Protocols used in the PaloAlto Network
120M
100M
80M
60M
40M
20M
0
tcp
udp
icmp
ipv6
esp
gre
Top Application traffic through firewall
ibm-websphere-mq
web-browsing
http-video
ssl
youtube-base
unknown-tcp
soap
netflix-streaming
dropbox
flash
Top application by request
web-browsing
snmpv2
ssl
ping
not-applicable
dns
sip
traceroute
soap
facebook-base
Top destination ports
Top destination zones
120M
100M
80M
60M
40M
Top source zones
120M
100M
80M
60M
40M
Top source addresses


Sources
Databases
Firewalls
Printers
Applications
Doorlocks
SCADA
logpoint Agent
Windows Systems
Linux Systems
SQL Servers
Active Directory
Enrichment
Threat Intelligence
logpoint

Example: Security Overview

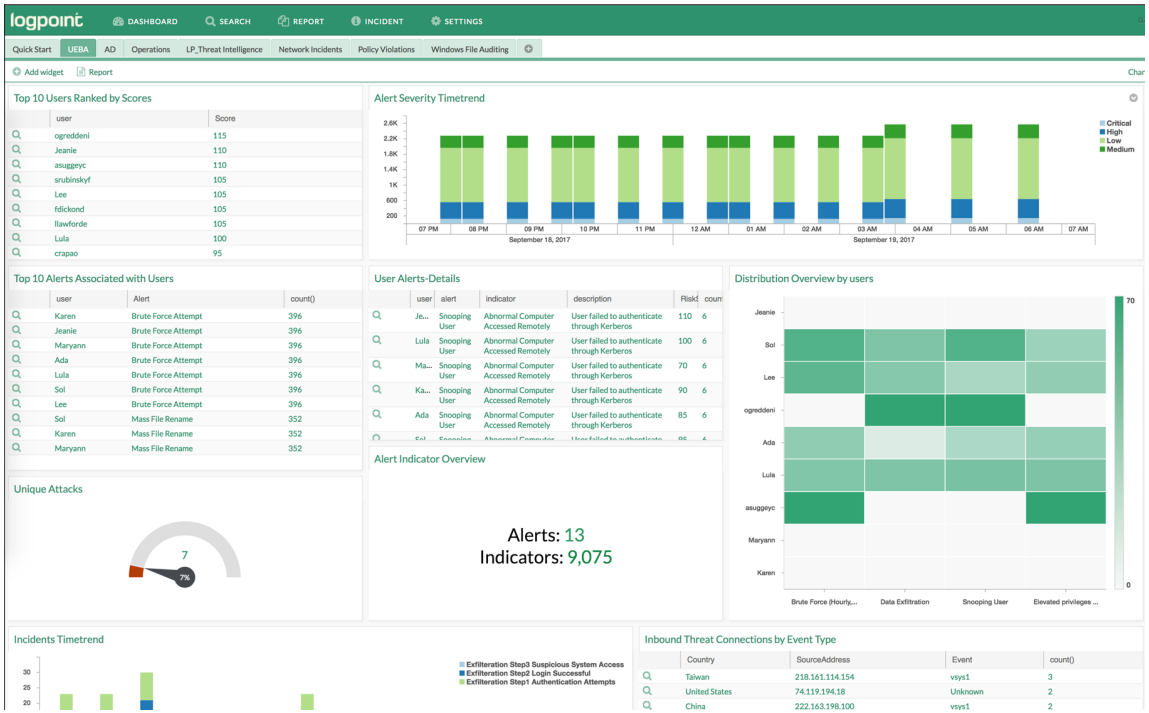


Introducing advanced UEBA

Enables analysts to:

- Achieve situational awareness before, during and after responding to breaches.
- Correlate, observe and report unusual activities

Reduces the time to detection and effectively managing the breach



logpoint

Machine Learning and UEBA

Benefits

- Accelerate response through detection of anomalous behavior
- Catch unknown threats that go under the radar of rule based systems
- Easy to setup, easy to configure directly in the LogPoint user interphase
- Reduce cost of SIEM implementation by eliminating many “expert-rules”
- Predictive licensing

How

- First version contains support for
  - AD
  - Authentication
  - File
  - Print actions
- Use cases includes
  - Credentials misuse
  - Data exfiltration
  - Lateral movements
- Continuously updating the risk posture of entities
- Extend value of UEBA outside of defined use cases
  - By using the risk scores as enrichment meta-data on existing logs

UEBA architecture

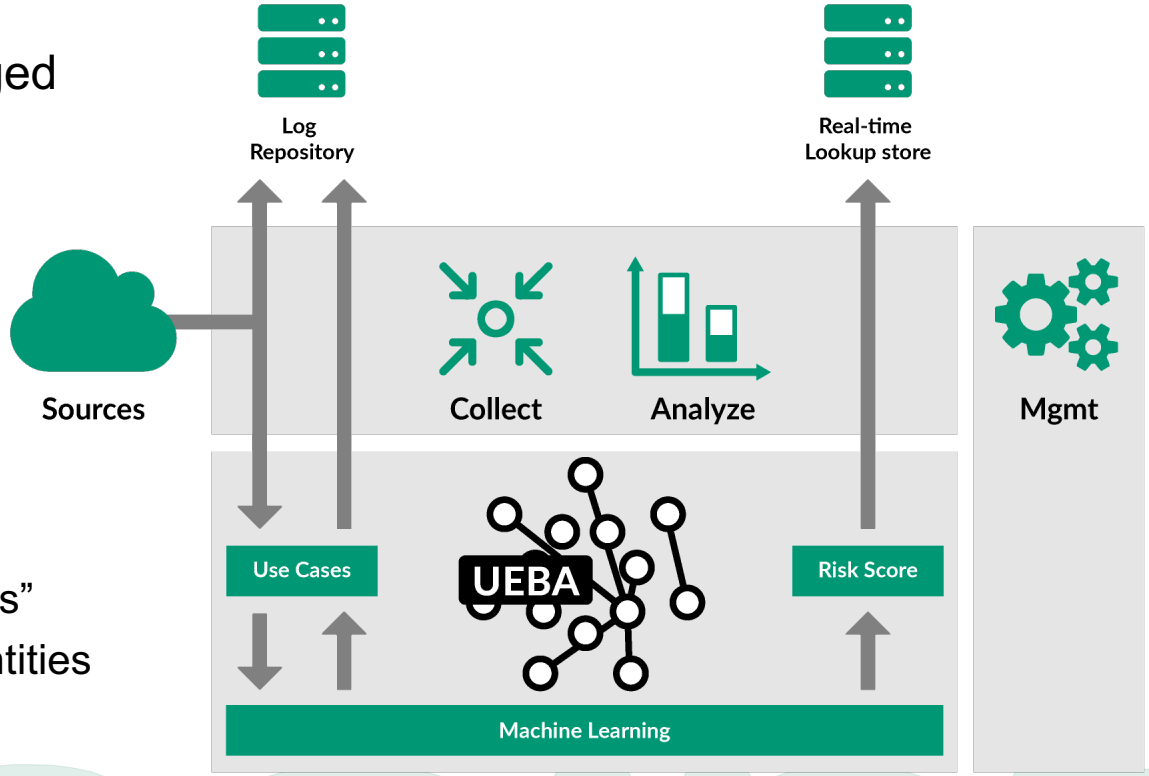
The UEBA Module is centrally managed from LogPoint

The UEBA Module accepts use-cases

- Anomalous AD Activity
- Data Exfiltration
- Misuse of credentials

Output is two fold

- Alerts and observations sent as “logs”
- Real-time updated risk scores for entities sent as a lookup-store



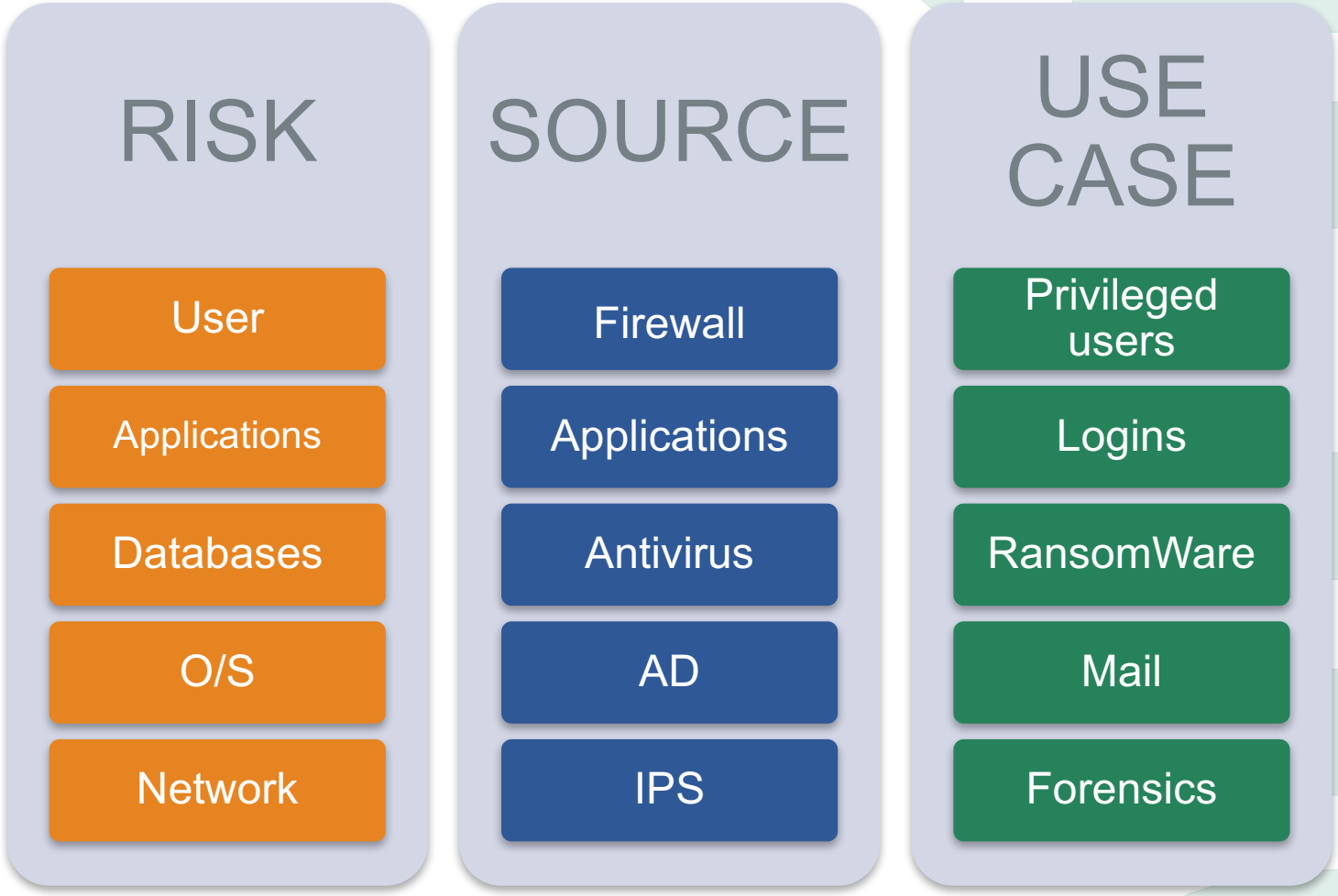
What is SIEM used for?

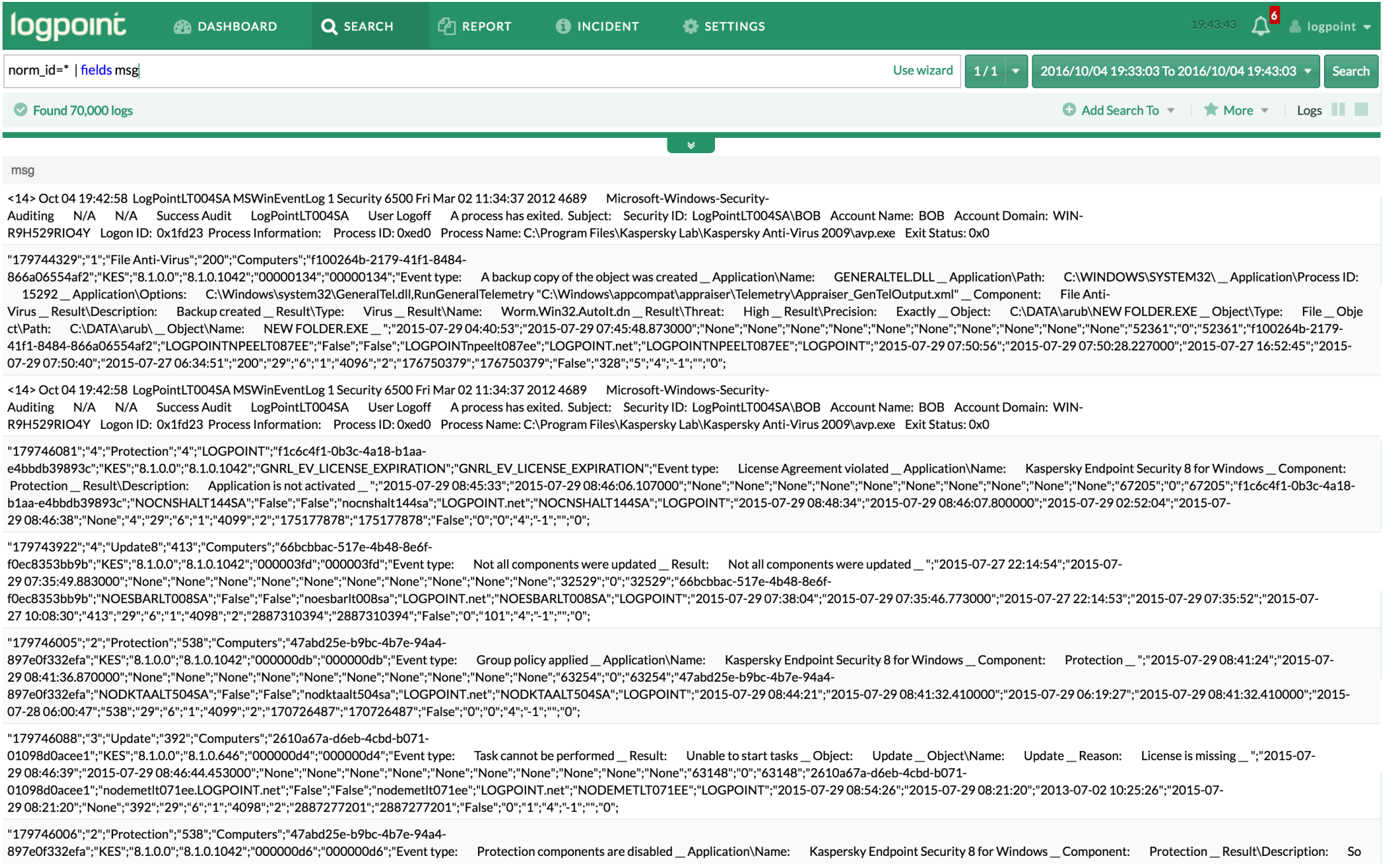
Compliance and Reporting

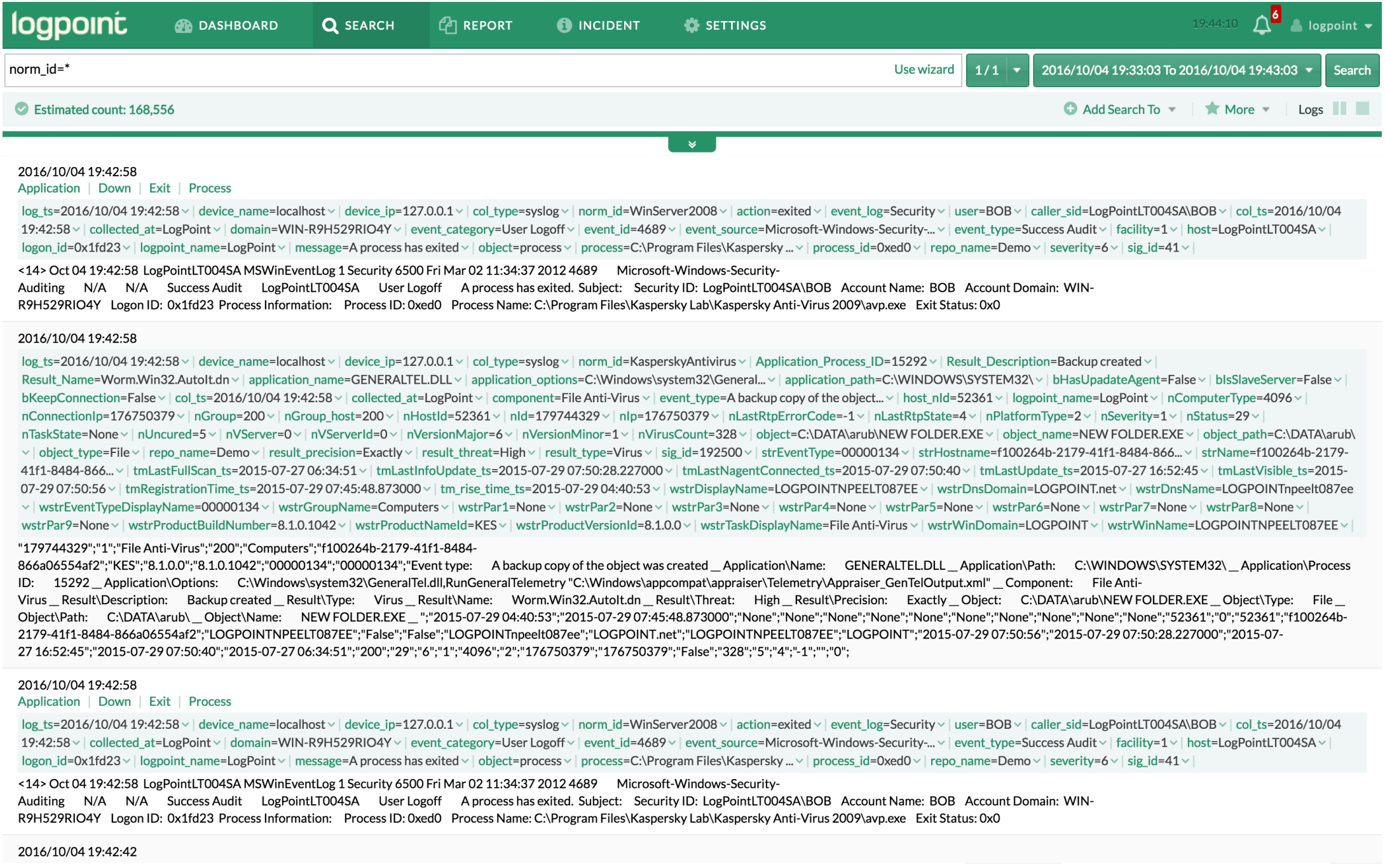
Security and Threat Management

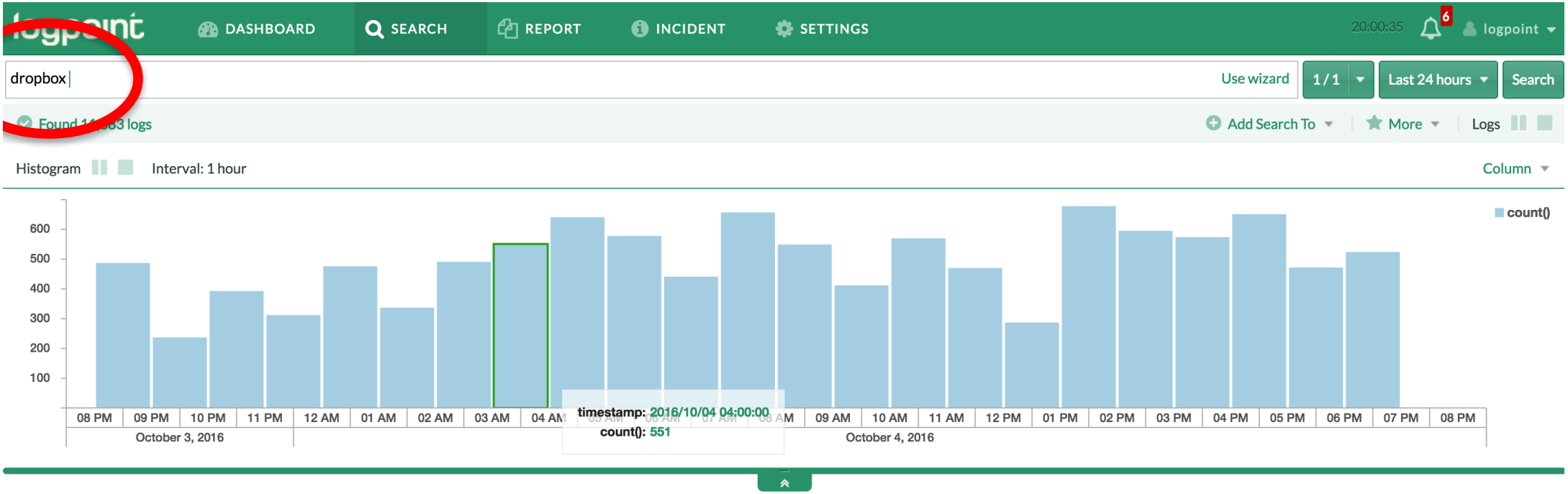
IT Operations

USE CASES


RISK
User
Applications
Databases
O/S
Network
SOURCE
Firewall
Applications
Antivirus
AD
IPS
USE CASE
Privileged users
Logins
RansomWare
Mail
Forensics


logpoint
DASHBOARD
SEARCH
REPORT
INCIDENT
SETTINGS
19:43:43
6
logpoint
norm_id=* | fields msg
Use wizard
1 / 1
2016/10/04 19:33:03 To 2016/10/04 19:43:03
Search
Found 70,000 logs
Add Search To
More
Logs
msg
<14> Oct 04 19:42:58 LogPointLT004SA MSWinEventLog 1 Security 6500 Fri Mar 02 11:34:37 2012 4689 Microsoft-Windows-Security-Auditing N/A N/A Success Audit LogPointLT004SA User Logoff A process has exited. Subject: Security ID: LogPointLT004SA\BOB Account Name: BOB Account Domain: WIN-R9H529RIO4Y Logon ID: 0x1fd23 Process Information: Process ID: 0xed0 Process Name: C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2009\avp.exe Exit Status: 0x0
"179744329";"1";"File Anti-Virus";"200";"Computers";"f100264b-2179-41f1-8484-866a06554af2";"KES";"8.1.0.0";"8.1.0.1042";"00000134";"00000134";"Event type: A backup copy of the object was created __ Application\Name: GENERALTEL.DLL __ Application\Path: C:\WINDOWS\SYSTEM32\ __ Application\Process ID: 15292 __ Application\Options: C:\Windows\system32\GeneralTel.dll,RunGeneralTelemetry "C:\Windows\appcompat\appraiser\Telemetry\Appraiser_GenTelOutput.xml" __ Component: File Anti-Virus __ Result\Description: Backup created __ Result\Type: Virus __ Result\Name: Worm.Win32.AutoIt.dn __ Result\Threat: High __ Result\Precision: Exactly __ Object: C:\DATA\arub\NEW FOLDER.EXE __ Object\Type: File __ Object\Path: C:\DATA\arub\ __ Object\Name: NEW FOLDER.EXE __ ";"2015-07-29 04:40:53";"2015-07-29 07:45:48.873000";"None";"None";"None";"None";"None";"None";"None";"None";"None";"None";"52361";"0";"52361";"f100264b-2179-41f1-8484-866a06554af2";"LOGPOINTNPEELT087EE";"False";"False";"LOGPOINTnpeelt087ee";"LOGPOINT.net";"LOGPOINTNPEELT087EE";"LOGPOINT";"2015-07-29 07:50:56";"2015-07-29 07:50:28.227000";"2015-07-27 16:52:45";"2015-07-29 07:50:40";"2015-07-27 06:34:51";"200";"29";"6";"1";"4096";"2";"176750379";"176750379";"False";"328";"5";"4";"-1";"";"0";
<14> Oct 04 19:42:58 LogPointLT004SA MSWinEventLog 1 Security 6500 Fri Mar 02 11:34:37 2012 4689 Microsoft-Windows-Security-Auditing N/A N/A Success Audit LogPointLT004SA User Logoff A process has exited. Subject: Security ID: LogPointLT004SA\BOB Account Name: BOB Account Domain: WIN-R9H529RIO4Y Logon ID: 0x1fd23 Process Information: Process ID: 0xed0 Process Name: C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2009\avp.exe Exit Status: 0x0
"179746081";"4";"Protection";"4";"LOGPOINT";"f1c6c4f1-0b3c-4a18-b1aa-e4bbdb39893c";"KES";"8.1.0.0";"8.1.0.1042";"GNRL_EV_LICENSE_EXPIRATION";"GNRL_EV_LICENSE_EXPIRATION";"Event type: License Agreement violated __ Application\Name: Kaspersky Endpoint Security 8 for Windows __ Component: Protection __ Result\Description: Application is not activated __ ";"2015-07-29 08:45:33";"2015-07-29 08:46:06.107000";"None";"None";"None";"None";"None";"None";"None";"None";"None";"None";"67205";"0";"67205";"f1c6c4f1-0b3c-4a18-b1aa-e4bbdb39893c";"NOCNSHALT144SA";"False";"False";"nocnshalt144sa";"LOGPOINT.net";"NOCNSHALT144SA";"LOGPOINT";"2015-07-29 08:48:34";"2015-07-29 08:46:07.800000";"2015-07-29 02:52:04";"2015-07-29 08:46:38";"None";"4";"29";"6";"1";"4099";"2";"175177878";"175177878";"False";"0";"0";"4";"-1";"";"0";
"179743922";"4";"Update8";"413";"Computers";"66bcbbac-517e-4b48-8e6f-f0ec8353bb9b";"KES";"8.1.0.0";"8.1.0.1042";"000003fd";"000003fd";"Event type: Not all components were updated __ Result: Not all components were updated __ ";"2015-07-27 22:14:54";"2015-07-29 07:35:49.883000";"None";"None";"None";"None";"None";"None";"None";"None";"None";"None";"32529";"0";"32529";"66bcbbac-517e-4b48-8e6f-f0ec8353bb9b";"NOESBARLT008SA";"False";"False";"noesbarlt008sa";"LOGPOINT.net";"NOESBARLT008SA";"LOGPOINT";"2015-07-29 07:38:04";"2015-07-29 07:35:46.773000";"2015-07-27 22:14:53";"2015-07-29 07:35:52";"2015-07-27 10:08:30";"413";"29";"6";"1";"4098";"2";"2887310394";"2887310394";"False";"0";"101";"4";"-1";"";"0";
"179746005";"2";"Protection";"538";"Computers";"47abd25e-b9bc-4b7e-94a4-897e0f332efa";"KES";"8.1.0.0";"8.1.0.1042";"000000db";"000000db";"Event type: Group policy applied __ Application\Name: Kaspersky Endpoint Security 8 for Windows __ Component: Protection __ ";"2015-07-29 08:41:24";"2015-07-29 08:41:36.870000";"None";"None";"None";"None";"None";"None";"None";"None";"None";"None";"63254";"0";"63254";"47abd25e-b9bc-4b7e-94a4-897e0f332efa";"NODKTAALT504SA";"False";"False";"nodktaalt504sa";"LOGPOINT.net";"NODKTAALT504SA";"LOGPOINT";"2015-07-29 08:44:21";"2015-07-29 08:41:32.410000";"2015-07-29 06:19:27";"2015-07-29 08:41:32.410000";"2015-07-28 06:00:47";"538";"29";"6";"1";"4099";"2";"170726487";"170726487";"False";"0";"0";"4";"-1";"";"0";
"179746088";"3";"Update";"392";"Computers";"2610a67a-d6eb-4cbd-b071-01098d0acee1";"KES";"8.1.0.0";"8.1.0.646";"000000d4";"000000d4";"Event type: Task cannot be performed __ Result: Unable to start tasks __ Object: Update __ Object\Name: Update __ Reason: License is missing __ ";"2015-07-29 08:46:39";"2015-07-29 08:46:44.453000";"None";"None";"None";"None";"None";"None";"None";"None";"None";"None";"63148";"0";"63148";"2610a67a-d6eb-4cbd-b071-01098d0acee1";"nodemetlt071ee.LOGPOINT.net";"False";"False";"nodemetlt071ee";"LOGPOINT.net";"NODEMETLT071EE";"LOGPOINT";"2015-07-29 08:54:26";"2015-07-29 08:21:20";"2013-07-02 10:25:26";"2015-07-29 08:21:20";"None";"392";"29";"6";"1";"4098";"2";"2887277201";"2887277201";"False";"0";"1";"4";"-1";"";"0";
"179746006";"2";"Protection";"538";"Computers";"47abd25e-b9bc-4b7e-94a4-897e0f332efa";"KES";"8.1.0.0";"8.1.0.1042";"000000d6";"000000d6";"Event type: Protection components are disabled __ Application\Name: Kaspersky Endpoint Security 8 for Windows __ Component: Protection __ Result\Description: So


logpoint
DASHBOARD
SEARCH
REPORT
INCIDENT
SETTINGS
19:44:10
6
logpoint
norm_id=*
Use wizard
1 / 1
2016/10/04 19:33:03 To 2016/10/04 19:43:03
Search
Estimated count: 168,556
Add Search To
More
Logs
2016/10/04 19:42:58
Application | Down | Exit | Process
log_ts=2016/10/04 19:42:58 | device_name=localhost | device_ip=127.0.0.1 | col_type=syslog | norm_id=WinServer2008 | action=exited | event_log=Security | user=BOB | caller_sid=LogPointLT004SA\BOB | col_ts=2016/10/04 19:42:58 | collected_at=LogPoint | domain=WIN-R9H529RIO4Y | event_category=User Logoff | event_id=4689 | event_source=Microsoft-Windows-Security-... | event_type=Success Audit | facility=1 | host=LogPointLT004SA | logon_id=0x1fd23 | logpoint_name=LogPoint | message=A process has exited | object=process | process=C:\Program Files\Kaspersky ... | process_id=0xed0 | repo_name=Demo | severity=6 | sig_id=41 |
<14> Oct 04 19:42:58 LogPointLT004SA MSWinEventLog 1 Security 6500 Fri Mar 02 11:34:37 2012 4689 Microsoft-Windows-Security-
Auditing N/A N/A Success Audit LogPointLT004SA User Logoff A process has exited. Subject: Security ID: LogPointLT004SA\BOB Account Name: BOB Account Domain: WIN-
R9H529RIO4Y Logon ID: 0x1fd23 Process Information: Process ID: 0xed0 Process Name: C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2009\avp.exe Exit Status: 0x0
2016/10/04 19:42:58
log_ts=2016/10/04 19:42:58 | device_name=localhost | device_ip=127.0.0.1 | col_type=syslog | norm_id=KasperskyAntivirus | Application_Process_ID=15292 | Result_Description=Backup created | Result_Name=Worm.Win32.AutoIt.dn | application_name=GENERALTEL.DLL | application_options=C:\Windows\system32\General... | application_path=C:\WINDOWS\SYSTEM32\ | bHasUpadateAgent=False | bIsSlaveServer=False | bKeepConnection=False | col_ts=2016/10/04 19:42:58 | collected_at=LogPoint | component=File Anti-Virus | event_type=A backup copy of the object... | host_nId=52361 | logpoint_name=LogPoint | nComputerType=4096 | nConnectionIp=176750379 | nGroup=200 | nGroup_host=200 | nHostId=52361 | nId=179744329 | nIp=176750379 | nLastRtpErrorCode=-1 | nLastRtpState=4 | nPlatformType=2 | nSeverity=1 | nStatus=29 | nTaskState=None | nUncured=5 | nVServer=0 | nVServerId=0 | nVersionMajor=6 | nVersionMinor=1 | nVirusCount=328 | object=C:\DATA\arub\NEW FOLDER.EXE | object_name=NEW FOLDER.EXE | object_path=C:\DATA\arub\ | object_type=File | repo_name=Demo | result_precision=Exactly | result_threat=High | result_type=Virus | sig_id=192500 | strEventType=00000134 | strHostname=f100264b-2179-41f1-8484-866... | strName=f100264b-2179-41f1-8484-866... | tmLastFullScan_ts=2015-07-27 06:34:51 | tmLastInfoUpdate_ts=2015-07-29 07:50:28.227000 | tmLastNagentConnected_ts=2015-07-29 07:50:40 | tmLastUpdate_ts=2015-07-27 16:52:45 | tmLastVisible_ts=2015-07-29 07:50:56 | tmRegistrationTime_ts=2015-07-29 07:45:48.873000 | tm_rise_time_ts=2015-07-29 04:40:53 | wstrDisplayName=LOGPOINTNPEELT087EE | wstrDnsDomain=LOGPOINT.net | wstrDnsName=LOGPOINTnpeelt087ee | wstrEventTypeDisplayName=00000134 | wstrGroupName=Computers | wstrPar1=None | wstrPar2=None | wstrPar3=None | wstrPar4=None | wstrPar5=None | wstrPar6=None | wstrPar7=None | wstrPar8=None | wstrPar9=None | wstrProductBuildNumber=8.1.0.1042 | wstrProductNameId=KES | wstrProductVersionId=8.1.0.0 | wstrTaskDisplayName=File Anti-Virus | wstrWinDomain=LOGPOINT | wstrWinName=LOGPOINTNPEELT087EE |
"179744329";"1";"File Anti-Virus";"200";"Computers";"f100264b-2179-41f1-8484-
866a06554af2";"KES";"8.1.0.0";"8.1.0.1042";"00000134";"00000134";"Event type: A backup copy of the object was created __ Application\Name: GENERALTEL.DLL __ Application\Path: C:\WINDOWS\SYSTEM32\ __ Application\Process ID: 15292 __ Application\Options: C:\Windows\system32\GeneralTel.dll,RunGeneralTelemetry "C:\Windows\appcompat\appraiser\Telemetry\Appraiser_GenTelOutput.xml" __ Component: File Anti-Virus __ Result\Description: Backup created __ Result\Type: Virus __ Result\Name: Worm.Win32.AutoIt.dn __ Result\Threat: High __ Result\Precision: Exactly __ Object: C:\DATA\arub\NEW FOLDER.EXE __ Object\Type: File __ Object\Path: C:\DATA\arub\ __ Object\Name: NEW FOLDER.EXE __ ";"2015-07-29 04:40:53";"2015-07-29 07:45:48.873000";"None";"None";"None";"None";"None";"None";"None";"None";"None";"None";"52361";"0";"52361";"f100264b-2179-41f1-8484-866a06554af2";"LOGPOINTNPEELT087EE";"False";"False";"LOGPOINTnpeelt087ee";"LOGPOINT.net";"LOGPOINTNPEELT087EE";"LOGPOINT";"2015-07-29 07:50:56";"2015-07-29 07:50:28.227000";"2015-07-27 16:52:45";"2015-07-29 07:50:40";"2015-07-27 06:34:51";"200";"29";"6";"1";"4096";"2";"176750379";"176750379";"False";"328";"5";"4";"-1";"";"0";
2016/10/04 19:42:58
Application | Down | Exit | Process
log_ts=2016/10/04 19:42:58 | device_name=localhost | device_ip=127.0.0.1 | col_type=syslog | norm_id=WinServer2008 | action=exited | event_log=Security | user=BOB | caller_sid=LogPointLT004SA\BOB | col_ts=2016/10/04 19:42:58 | collected_at=LogPoint | domain=WIN-R9H529RIO4Y | event_category=User Logoff | event_id=4689 | event_source=Microsoft-Windows-Security-... | event_type=Success Audit | facility=1 | host=LogPointLT004SA | logon_id=0x1fd23 | logpoint_name=LogPoint | message=A process has exited | object=process | process=C:\Program Files\Kaspersky ... | process_id=0xed0 | repo_name=Demo | severity=6 | sig_id=41 |
<14> Oct 04 19:42:58 LogPointLT004SA MSWinEventLog 1 Security 6500 Fri Mar 02 11:34:37 2012 4689 Microsoft-Windows-Security-
Auditing N/A N/A Success Audit LogPointLT004SA User Logoff A process has exited. Subject: Security ID: LogPointLT004SA\BOB Account Name: BOB Account Domain: WIN-
R9H529RIO4Y Logon ID: 0x1fd23 Process Information: Process ID: 0xed0 Process Name: C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2009\avp.exe Exit Status: 0x0
2016/10/04 19:42:42



2016/10/04 19:59:31
Connection | Traffic

log_ts=2016/10/04 19:59:31 | device_name=localhost | device_ip=127.0.0.1 | col_type=syslog | norm_id=PaloAltoNetworkFirewall | source_address=102.14.189.215 | destination_address=16.32.67.118 | target_user=Michael | action=allow | application=dropbox | datasize=77007 | sent_datasize=69851 | received_datasize=7156 | user=Jacob | destination_location=US | action_flags=0x1 | col_ts=2016/10/04 19:59:31 | collected_at=LogPoint | destination_interface=ethernet13 | destination_port=23 | destination_zone=tunnel.2 | elapsed_time=45 | event_category=TRAFFIC | flags=0x00002000 | generated_ts=10/04/error 19:59:31 | logpoint_name=LogPoint | nat_destination_address=1 | nat_destination_port=23 | nat_source_address=1 | nat_source_port=42887 | packet=9625 | protocol=udp | received_packet=894 | repeat_count=1 | repo_name=Demo | rule_name=PAN-known-APPS | sent_packet=8731 | sequence_number=37188786291 | serial_number=707519685 | session_id=54848076 | sig_id=127001 | source_interface=ethernet11 | source_location=102.14.189.215 | source_port=19601 | source_zone=untrust | start_ts=2016/01/26 19:28:35 | sub_category=end | url_category=streaming media | virtual_firewall=vsys2 |

1,1/26/2016 19:27:38,707519685,TRAFFIC,end,0, 10/04/error 19:59:31 ,102.14.189.215,16.32.67.118,1,1,PAN-known-APPS,Jacob,Michael,dropbox,vsys2,untrust,tunnel.2,ethernet11,ethernet13,Log-forwarding,2,54848076,1,19601,23,42887,23,0x00002000,udp,allow,77007,69851,7156,9625,1/26/2016 19:28:35,45,streaming media,1,37188786291,0x1,102.14.189.215,US,1,8731,894,tcp-rst-from-client,

2016/10/04 19:59:31
Connection | Traffic

log_ts=2016/10/04 19:59:31 | device_name=localhost | device_ip=127.0.0.1 | col_type=syslog | norm_id=PaloAltoNetworkFirewall | source_address=66.172.183.12 | destination_address=155.44.99.229 | target_user=Myrtle | action=deny | application=dropbox | datasize=21319 | sent_datasize=3884 | received_datasize=17435 | user=Kathy | destination_location=US | action_flags=0x2 | col_ts=2016/10/04 19:59:31 | collected_at=LogPoint | destination_interface=ethernet14 | destination_port=42 | destination_zone=tunnel.1 | elapsed_time=20 | event_category=TRAFFIC | flags=0x00008000 | generated_ts=10/04/error 19:59:31 | logpoint_name=LogPoint | nat_destination_address=1 | nat_destination_port=42 | nat_source_address=6 | nat_source_port=34991 | packet=2664 | protocol=udp | received_packet=2179 | repeat_count=1 | repo_name=Demo | rule_name=PAN-known-APPS | sent_packet=485 | sequence_number=37188786291 | serial_number=229994050 | session_id=23213122 | sig_id=127001 | source_interface=ethernet11 | source_location=US | source_port=53725 | source_zone=untrust | start_ts=2016/01/26 19:28:37 | sub_category=start | url_category=streaming media | virtual_firewall=vsys1 |

4,1/26/2016 19:27:38,229994050,TRAFFIC,start,1, 10/04/error 19:59:31 ,66.172.183.12,155.44.99.229,6,1,PAN-known-APPS,Kathy,Myrtle,dropbox,vsys1,untrust,tunnel.1,ethernet11,ethernet14,Log-forwarding1,1,23213122,1,53725,42,34991,42,0x00008000,udp,deny,21319,3884,17435,2664,1/26/2016 19:28:37,20,streaming media,2,37188786291,0x2,US,US,2,485,2179,tcp-rst-from-client,

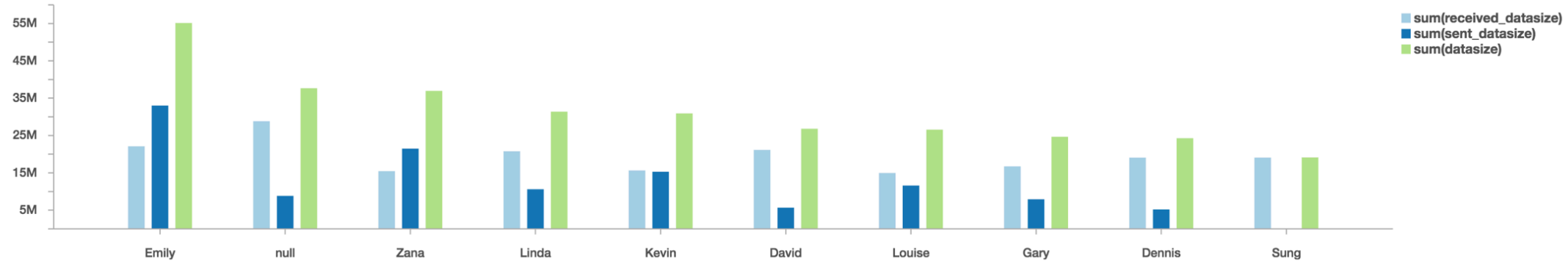
logpoint | DASHBOARD | SEARCH | REPORT | INCIDENT | SETTINGS | 20:04:00 | 7 | logpoint

```
dropbox | chart sum(received_datasize), sum(sent_datasize), sum(datasize) by user order by sum(datasize) desc limit 10
```

Use wizard | 1 / 1 | Last 24 hours | Search

Found 11,383 logs | Add Search To | More | Chart

Clustered Column



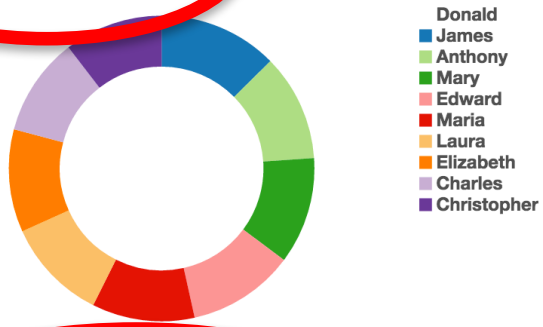
	user	sum(received_datasize)	sum(sent_datasize)	sum(datasize)
	Emily	22105828	33022945	55128773
	null	28827760	8830016	37657776
	Zana	15457729	21480429	36938158
	Linda	20780147	10605448	31385595
	Kevin	15628105	15301551	30929656
	David	21139906	5665231	26805137
	Louise	14955761	11602972	26558733
	Gary	16734175	7919278	24653453
	Dennis	19072952	5197384	24270336
	Sung	19079135	40533	19119668

logpoint | DASHBOARD | SEARCH | REPORT | INCIDENT | SETTINGS | 19:23:09 | 6 | logpoint

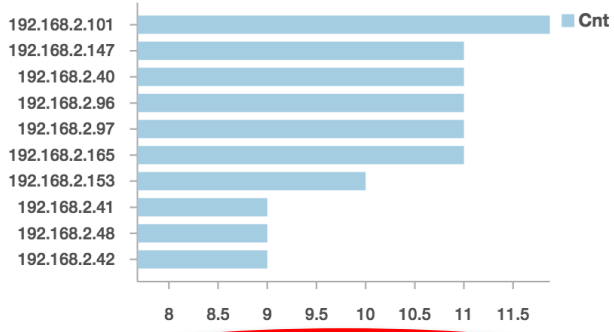
Security Incidents | Mail Incidents | Privileged Users | Operations | File System incidents | Network Incidents | Possible Data Theft | AD | Malware Incidents | Printouts | LP_Black Energy v3 | IndexSearche

Add widget | Repo | Change Repos | Auto Arrange

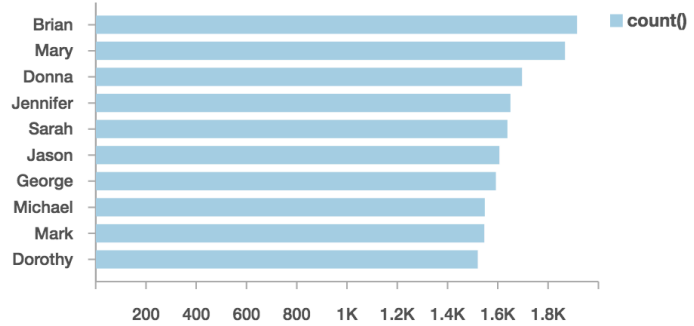
Top 10 Account Lockouts



Top 10 Sources with Higher User Account Lockouts



Top 10 Failed User Authentication



Login Attempts on Disabled Accounts

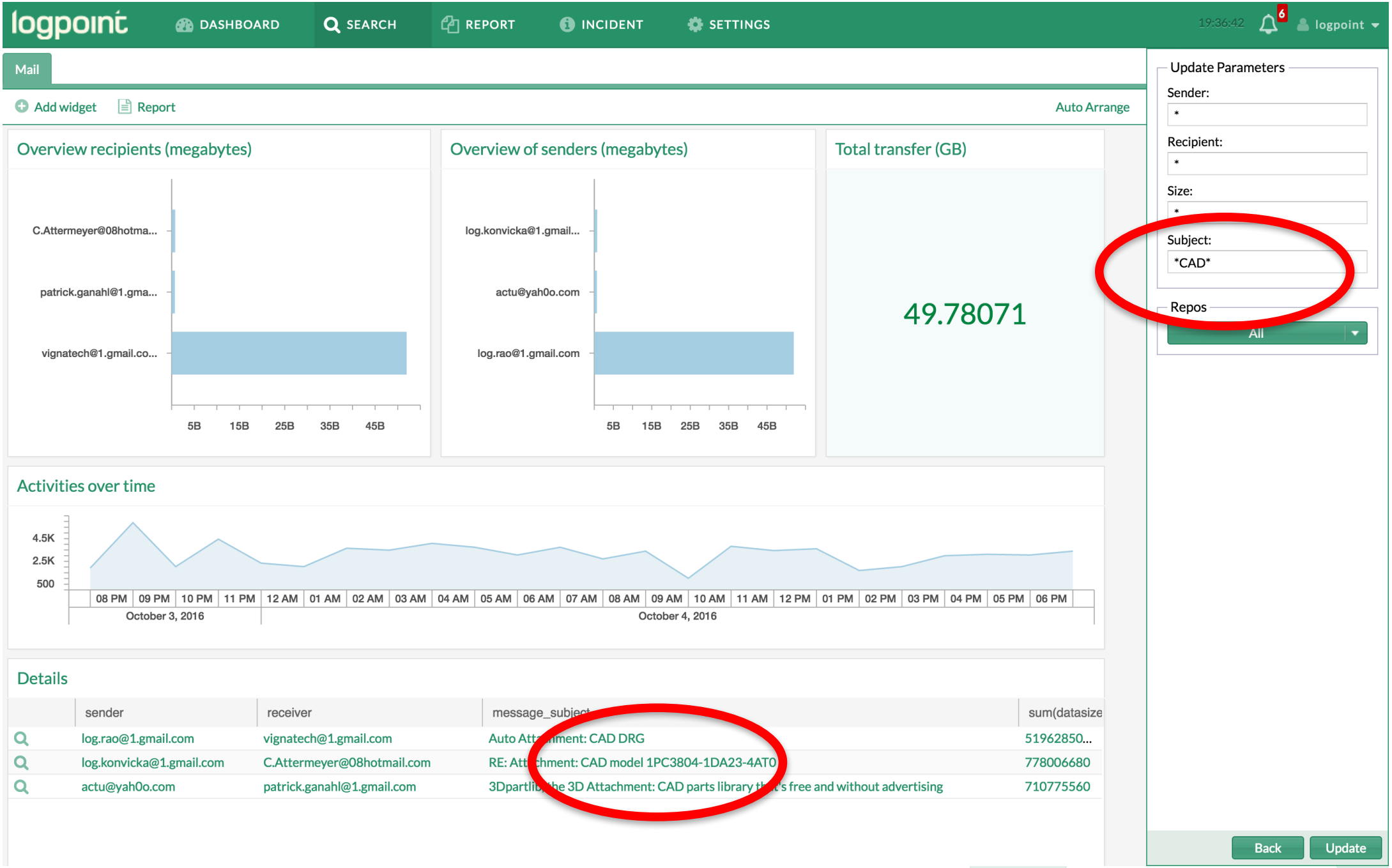
user	Account	count()
[illegible]	[illegible]	145
Patricia	Patricia	116
Barbara	Barbara	116
Ronald	Ronald	116
Sandra	Sandra	87
Christopher	Christopher	87
Mark	Mark	87
George	George	87
Brian	Brian	87

Failed Login Attempts from Same Source with Multiple Accounts

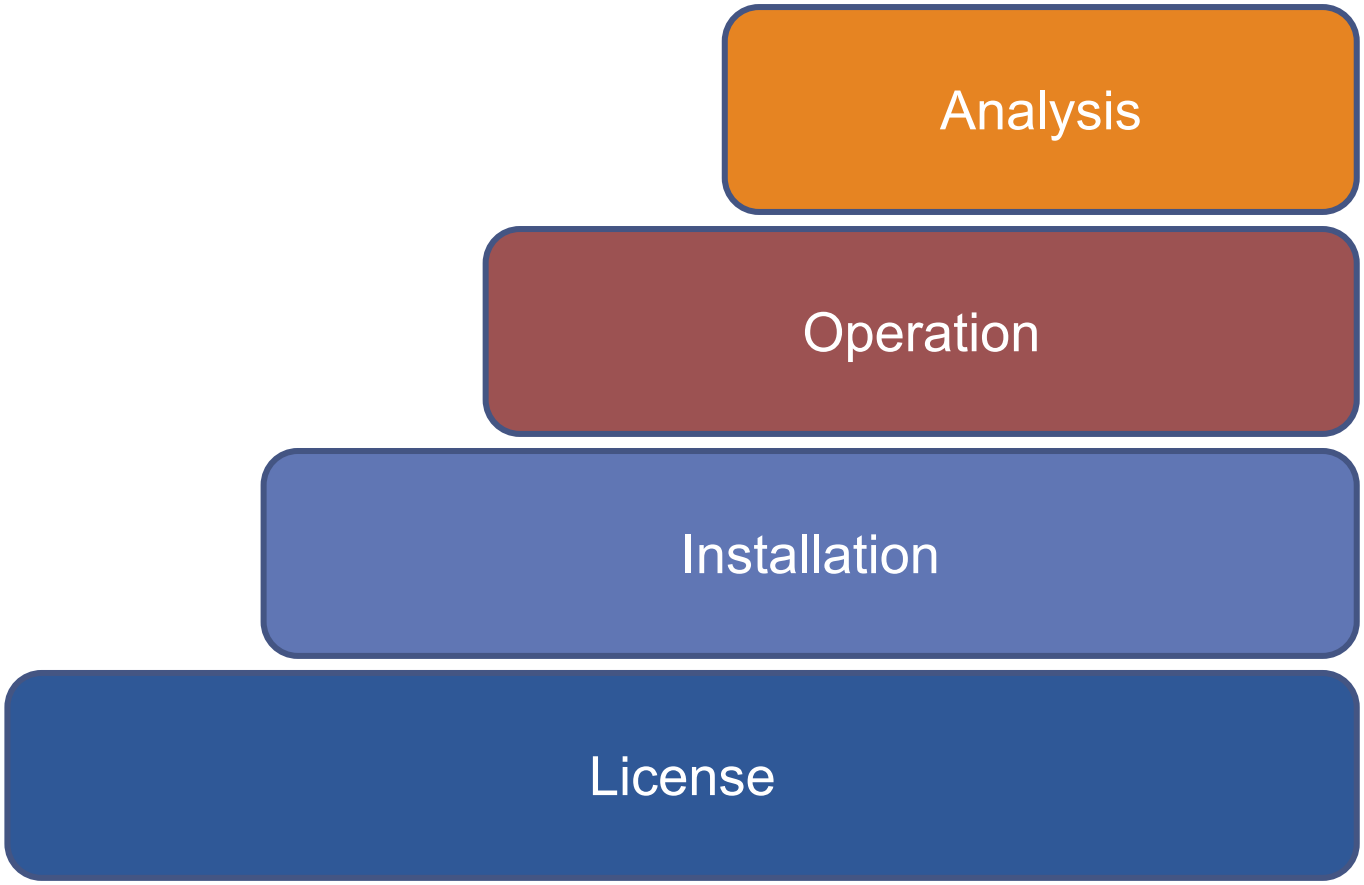
source_address	Account
[illegible]	[illegible]
192.168.2.147	11
192.168.2.40	11
192.168.2.96	11
192.168.2.97	11
192.168.2.165	11
192.168.2.153	10
192.168.2.41	9
192.168.2.48	9

Top 10 User In Excessive Failed Authentication

user	count()
Brian	1915
Mary	1867
Donna	1696
Jennifer	1650
Sarah	1638
Jason	1606
George	1592
Michael	1548
Mark	1546


logpoint
DASHBOARD
SEARCH
REPORT
INCIDENT
SETTINGS
19:36:42
6
logpoint
Mail
Add widget
Report
Auto Arrange
Overview recipients (megabytes)
C.Attermeyer@08hotma...
patrick.ganahl@1.gma...
vignatech@1.gmail.co...
5B
15B
25B
35B
45B
Overview of senders (megabytes)
log.konvicka@1.gmail...
actu@yah0o.com
log.rao@1.gmail.com
5B
15B
25B
35B
45B
Total transfer (GB)
49.78071
Activities over time
4.5K
2.5K
500
08 PM
09 PM
10 PM
11 PM
12 AM
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM
October 3, 2016
October 4, 2016
Details
sender
receiver
message_subject
sum(datasize
log.rao@1.gmail.com
vignatech@1.gmail.com
Auto Attachment: CAD DRG
51962850...
log.konvicka@1.gmail.com
C.Attermeyer@08hotmail.com
RE: Attachment: CAD model 1PC3804-1DA23-4AT0
778006680
actu@yah0o.com
patrick.ganahl@1.gmail.com
3Dpartlib the 3D Attachment: CAD parts library that's free and without advertising
710775560
Update Parameters
Sender:
*
Recipient:
*
Size:
*
Subject:
CAD
Repos
All
Back
Update

Models for providing SIEM



Radpoints LogPoint offering

LogPoint Certified consultants provide:

- License and Hardware
- Installation and Training
- Workshops
- Operational Services
- MSS and Reporting
- SIEM Security Consultancy

Ready for GDPR?

DO

- Workshop
- Identify Use Cases
- Prioritize
- **Get started!**

DON'T

- Over-engineer
- Collect "everything" and figure it out later

LogPoint *FREE* – try it out

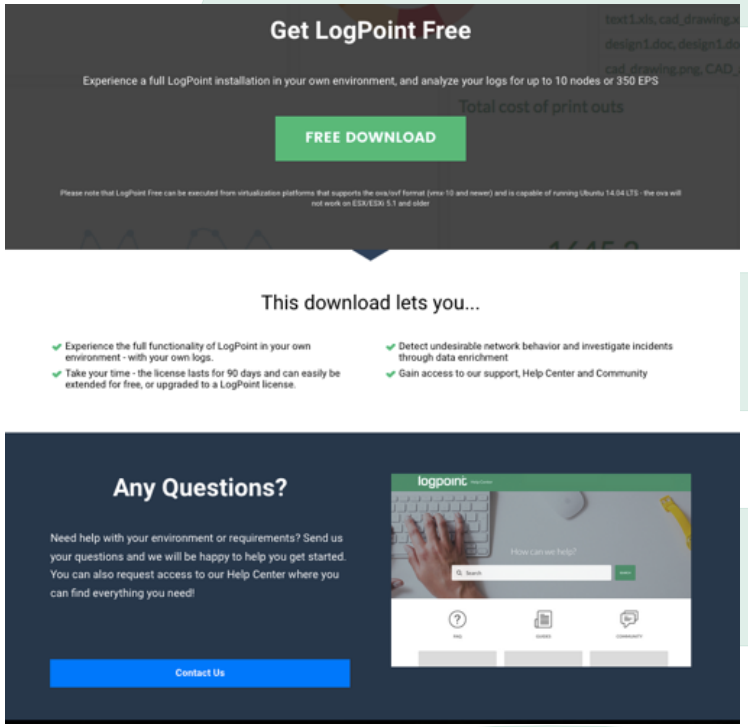
Full LogPoint functionality and experience

90 Day initial license with possible free extension

Up to **10 Nodes and 350 events per second**

Full access to **Community & Help Center**

Full access to **Support**



Why LogPoint?

- Easy to use : ready to go out of the box
- Easy to buy : simple license model, fixed price
- Easy to own : support and new versions included

- Provided by our strong reseller partners and MSSPs
- Common Criteria **EAL3+** Certified
- Gartner **Customer Choice Award** 2017


Thank you!
www.logpoint.com