IBM QRadar: the Security Operations Center for All seasons

Technical report
Instructor: Ross Millerick
Supervisor: Daniel Fortson
Student: Sadegh Bamohabbat Chafjiri
7/26/2019

AGENDA

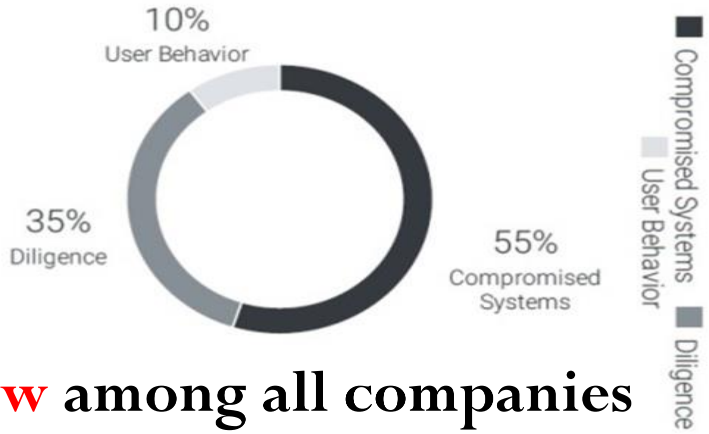
- SUMMARY
- Analysis of the GGU’s infrastructure
- Alternative solutions
- Proposed solution
- SWOT Analysis of alternatives
- IT Business Values- SWOT of solution
- Operating Plans
- Financial Analysis
- Conclusion

SUMMARY

Vulnerability analysis on Golden Gate University based on public information

Bitsight's Analysis:

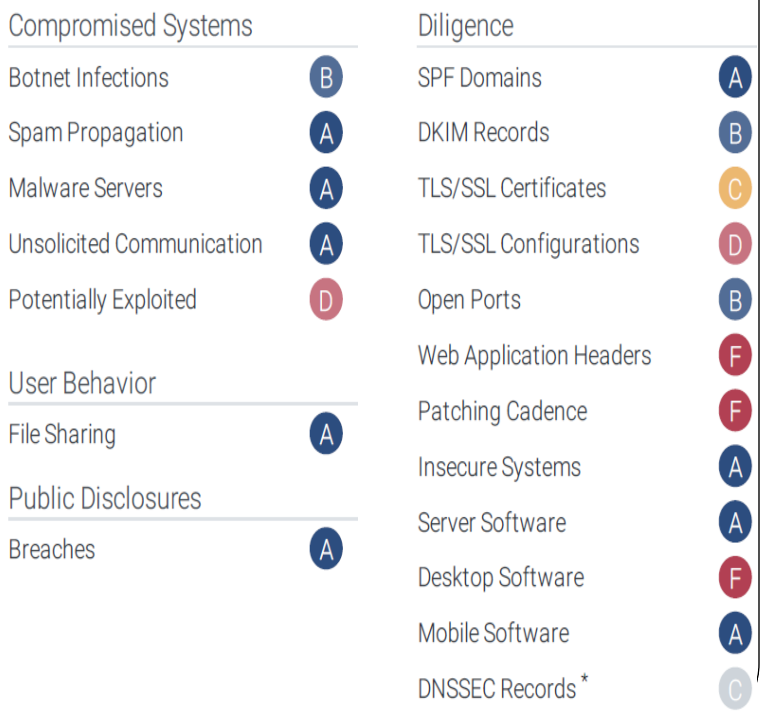
Ref: Bobby Adam
Cyber security analyst
At Bitsight Tech.



GGU's rank in IT security platform is low among all companies

The industry average: 640 to 740 out of 900
overall IT security performance of GGU:
590 to 650 out of 900
There was a decrease in security rate between July 2018 and July 2019

- A In the top 10% of all companies
- B In the top 30% of all companies
- C In the bottom 50% of all companies
- D In the bottom 40% of all companies
- F In the bottom 30% of all companies



Compromised Systems	
Botnet Infections	B
Spam Propagation	A
Malware Servers	A
Unsolicited Communication	A
Potentially Exploited	D

User Behavior	
File Sharing	A

Public Disclosures	
Breaches	A

Diligence	
SPF Domains	A
DKIM Records	B
TLS/SSL Certificates	C
TLS/SSL Configurations	D
Open Ports	B
Web Application Headers	F
Patching Cadence	F
Insecure Systems	A
Server Software	A
Desktop Software	F
Mobile Software	A
DNSSEC Records *	C

Analysis of GGU's infrastructure

- **Family Education Rights and Privacy Act (FERPA)** protects the privacy of student's educational records
- **GGU's contract model of cooperation:** vendors should know that they must accept the penalty if Forensics process at SOC prove that the data breach exploited in their side.
- **Solution:** Golden Gate University should officially negotiate with vendors or third parties to follow and guarantee FERPA privacy requirement and approve GGU's internal or its reperesentive's forensics process.
- **Data storage issue:** despite the obligation made by FERPA to encrypt data at rest or in transit, Golden Gate University does not apply encryption method to store students' information on database which can be considered as the high risk vulnerability.
- **Solution:** deploying encryption method for data at rest

FAMILY EDUCATIONAL RIGHTS & PRIVACY ACT

iKeepSafe

FERPA

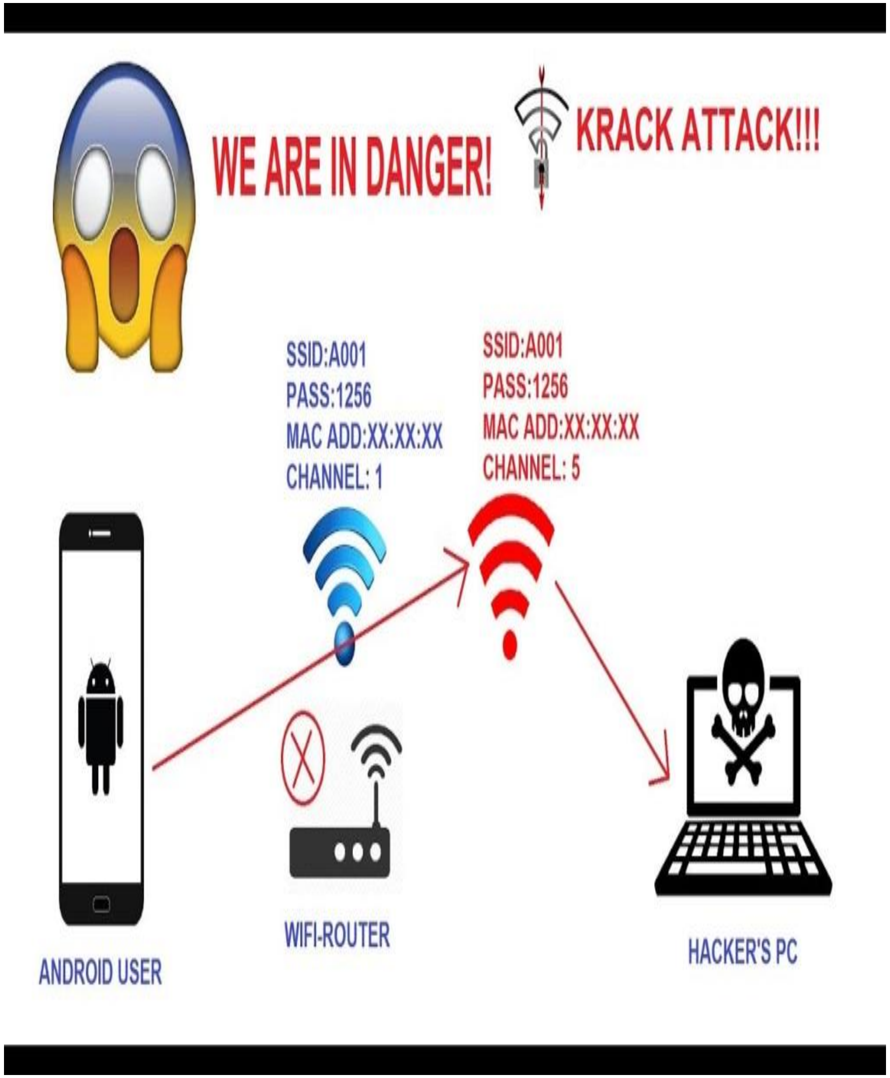
Analysis of GGU's infrastructure

- **WIFI parameters re-use ISSUE:** 4-way handshake protocol deployed in GGU wireless protocol is vulnerable against **Key Reinstallation Attack** (KRACK)

- **How it works?** This attack works based on initiating an all-zero parameter by injecting repetitive IV as an input of encryption algorithm.
- **Solution:** As a solution IBM QRadar can use signal intelligence to detect the Wifi manipulation in the network access to reduce the risk of KRACK attack.
- **Training issue:** School must engaged at least one associate director in learning the technical requirement of FERPA compliance and regulations.
- **Solution:** Online Training courses are

available on:

https://www.knowledgecity.com/



Analysis of GGU's infrastructure

What is a general solution: Security Operating system (SOC)

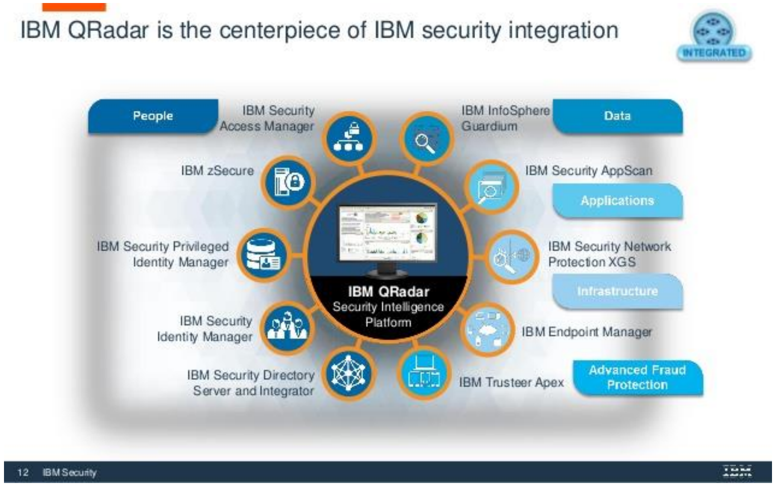
Roles:

- To provide a quick response to the security issues
- To bring insight, statics to the infrastructure
- To automate some repetitive tasks
- To detect suspicious signaling activity out of the bound or with monopolization purpose

IBM QRadar

Different types of deployment:

- On Prem, as a service, Cloud and Hybrid



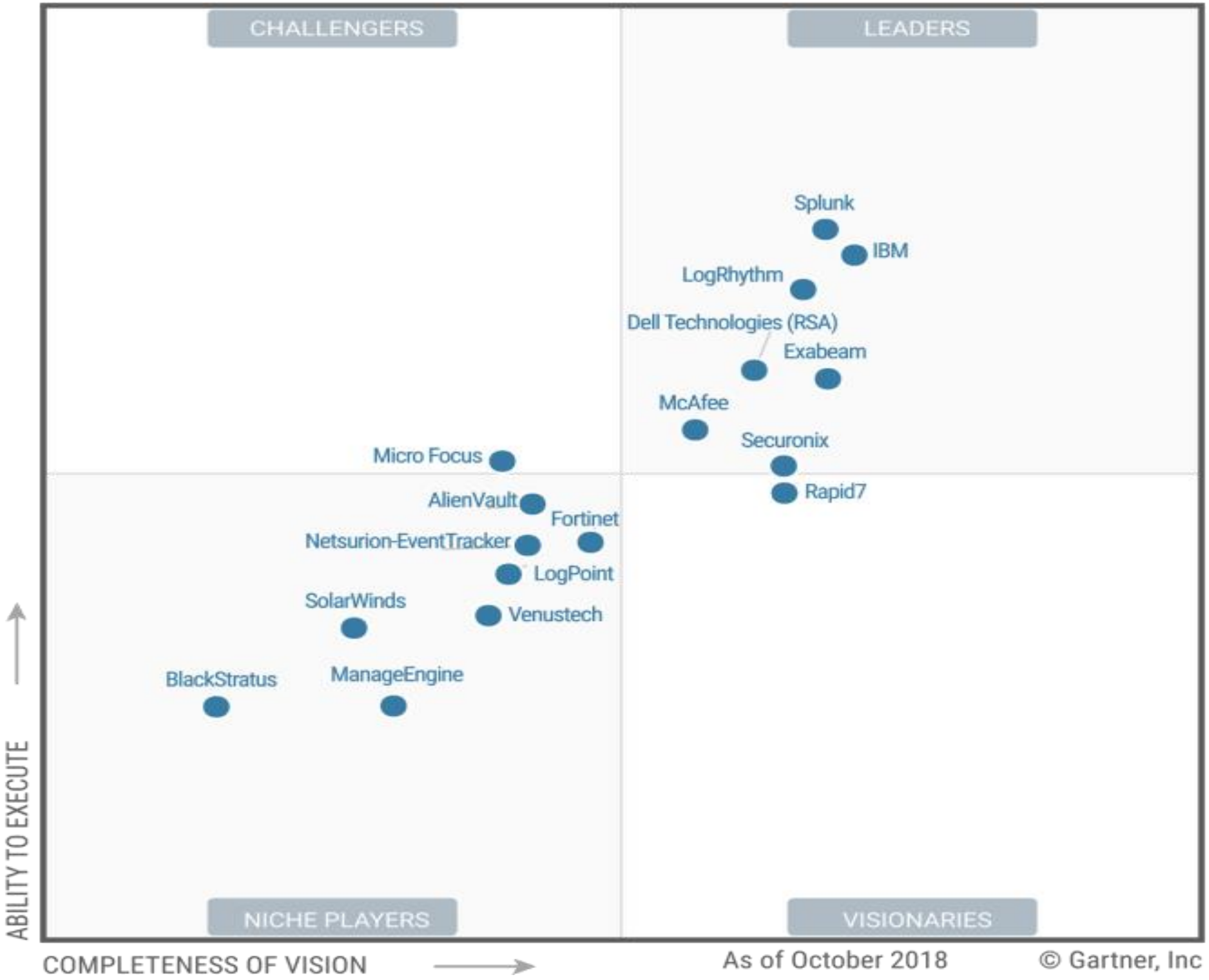
IBM QRadar is the centerpiece of IBM security integration

INTEGRATED
People
IBM Security Access Manager
IBM InfoSphere Guardium
Data
IBM zSecure
IBM Security AppScan
Applications
IBM Security Privileged Identity Manager
IBM Security Network Protection XGS
Infrastructure
IBM QRadar
Security Intelligence Platform
IBM Security Identity Manager
IBM Endpoint Manager
IBM Security Directory Server and Integrator
IBM Trusteer Apex
Advanced Fraud Protection
12 IBM Security
IBM

ALTERNATIVES

Market and Competitor Analysis

- IBM
- Splunk
- LogRhythm



As of October 2018

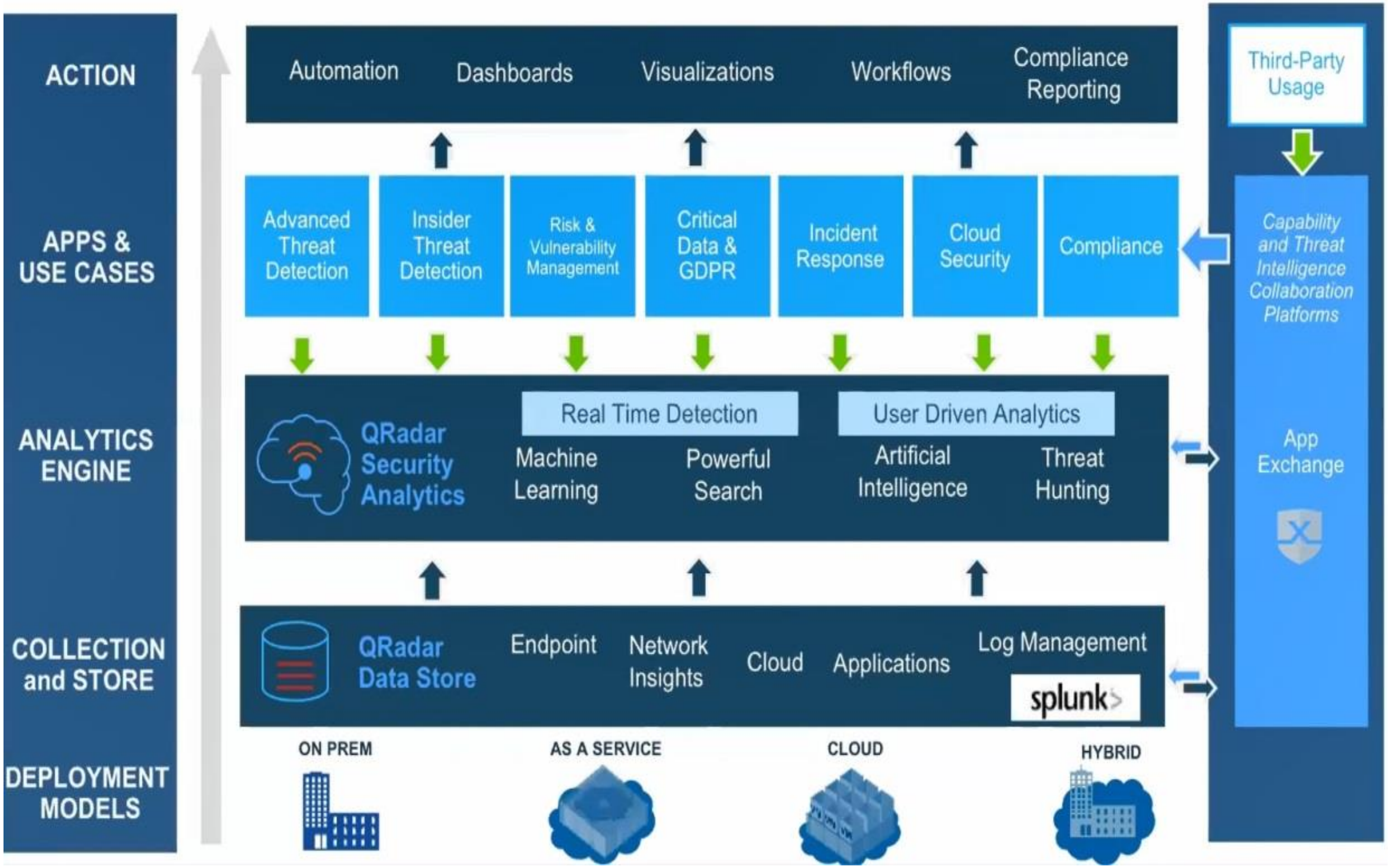
© Gartner, Inc

ALTERNATIVES

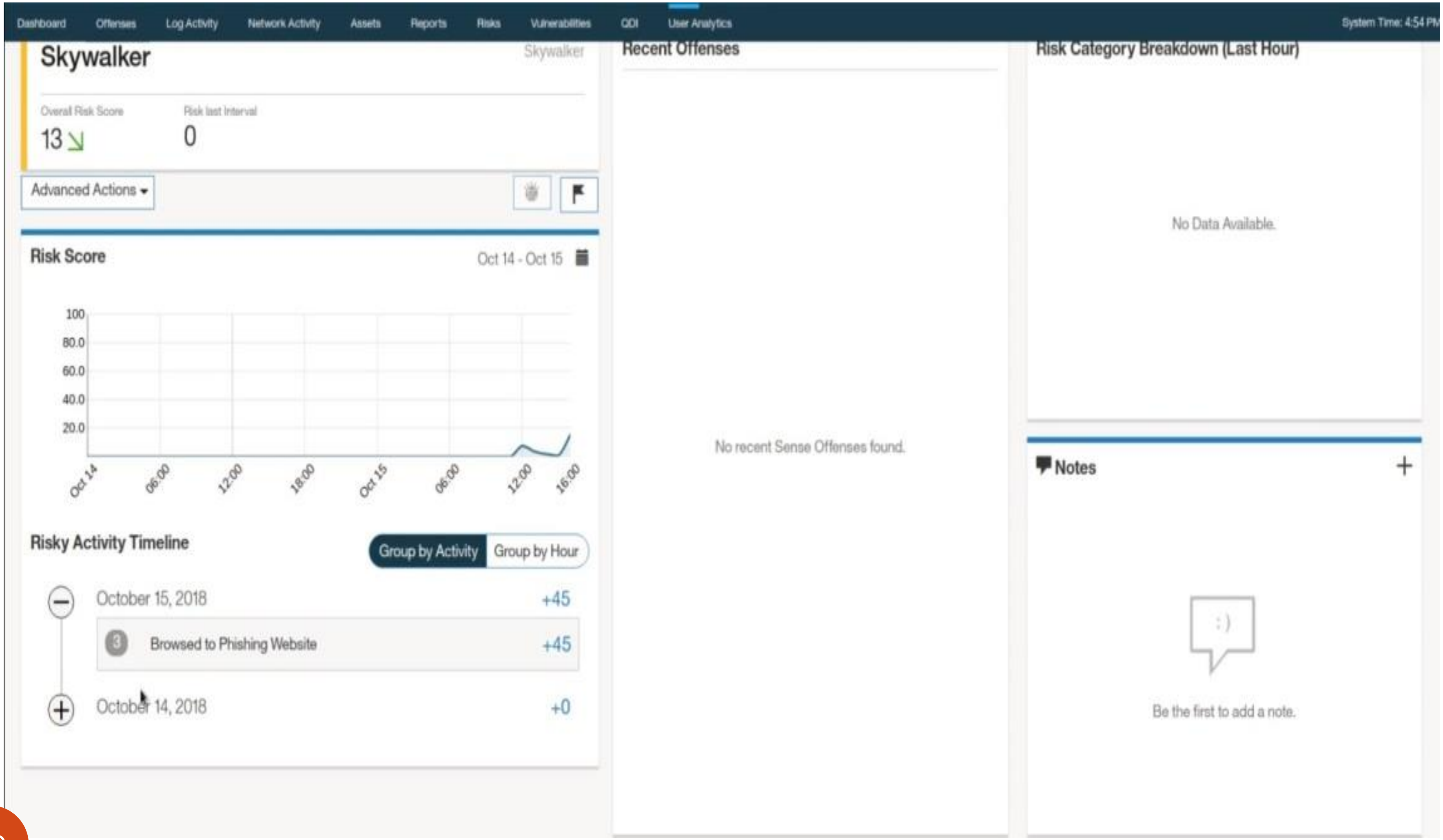
SWOT analysis on Splunk and LogRhythm **Strength**	**Weakness**
● Natural Language Process (NLP) ● Enterprise Security ● User Behavior Analytics ● Compatibility with other environment like SCADA	● Lack of ML and AI technology ● Non-integrated solutions and multiple technologies
Opportunity	**Threat**
● Coopetition model for marketing ● Capability of providing a partially service in cooperation with other vendors' platforms	● Data breach rose by integrity concerns ● repetitive functioning and time wastage in absence of AI and ML

PROPOSED SOLUTIONS

IBM Qradar Organizational Chart and architecture



PROPOSED SOLUTIONS



System Time: 4:54 PM

Skywalker

Skywalker

Overall Risk Score 13

Risk last Interval 0

Risk Score

Oct 14 - Oct 15

Risky Activity Timeline

October 15, 2018 +45

3 Browsed to Phishing Website +45

October 14, 2018 +0

Recent Offenses

No recent Sense Offenses found.

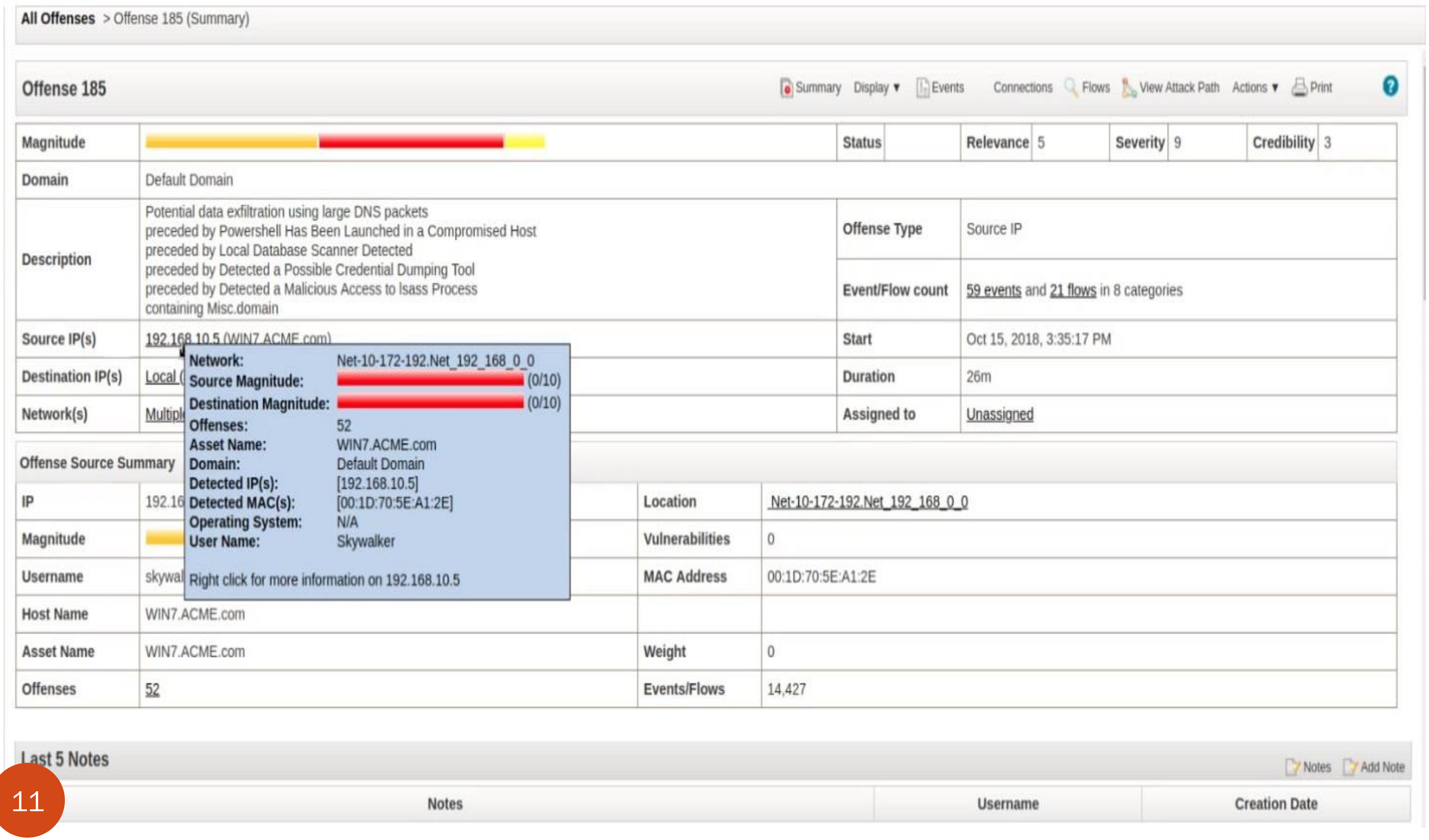
Risk Category Breakdown (Last Hour)

No Data Available.

Notes

Be the first to add a note.

PROPOSED SOLUTIONS



All Offenses > Offense 185 (Summary)

Offense 185

Magnitude		**Status**		**Relevance**	5	**Severity**	9	**Credibility**	3
Domain	Default Domain								
Description	Potential data exfiltration using large DNS packets preceded by Powershell Has Been Launched in a Compromised Host preceded by Local Database Scanner Detected preceded by Detected a Possible Credential Dumping Tool preceded by Detected a Malicious Access to lsass Process containing Misc.domain	**Offense Type**	Source IP						
		Event/Flow count	59 events and 21 flows in 8 categories						
Source IP(s)	192.168.10.5 (WIN7.ACME.com)	**Start**	Oct 15, 2018, 3:35:17 PM						
Destination IP(s)	Local (	**Duration**	26m						
Network(s)	Multipl	**Assigned to**	Unassigned						

Network:	Net-10-172-192.Net_192_168_0_0
Source Magnitude:	(0/10)
Destination Magnitude:	(0/10)
Offenses:	52
Asset Name:	WIN7.ACME.com
Domain:	Default Domain
Detected IP(s):	[192.168.10.5]
Detected MAC(s):	[00:1D:70:5E:A1:2E]
Operating System:	N/A
User Name:	Skywalker

Right click for more information on 192.168.10.5

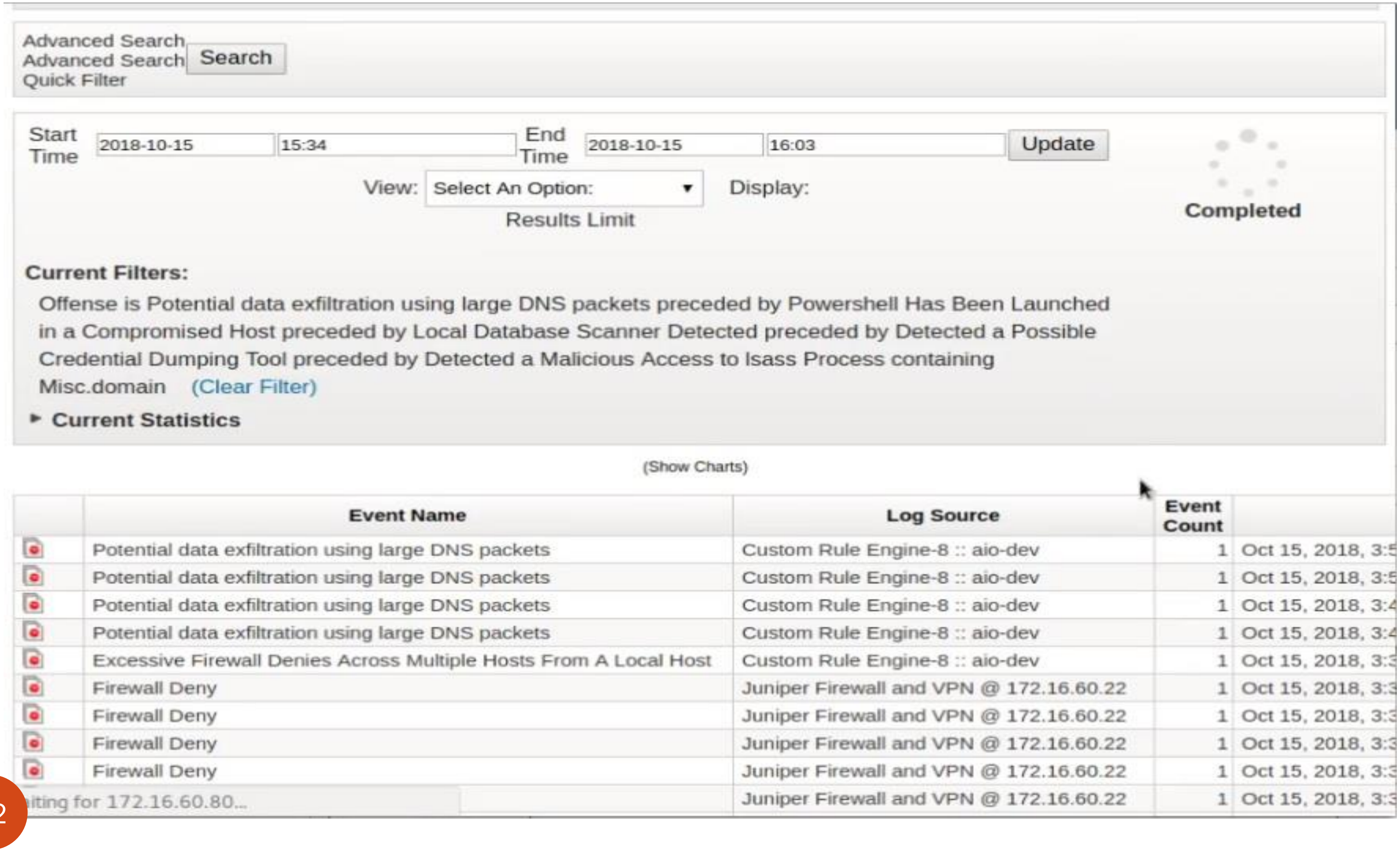
Offense Source Summary

IP	192.16	**Location**	Net-10-172-192.Net_192_168_0_0
Magnitude		**Vulnerabilities**	0
Username	skywal	**MAC Address**	00:1D:70:5E:A1:2E
Host Name	WIN7.ACME.com		
Asset Name	WIN7.ACME.com	**Weight**	0
Offenses	52	**Events/Flows**	14,427

Last 5 Notes

Notes	Username	Creation Date

PROPOSED SOLUTIONS



Start Time 2018-10-15 15:34 End Time 2018-10-15 16:03 Update

View: Select An Option: ▾ Display:

Results Limit

Completed

Current Filters:

Offense is Potential data exfiltration using large DNS packets preceded by Powershell Has Been Launched in a Compromised Host preceded by Local Database Scanner Detected preceded by Detected a Possible Credential Dumping Tool preceded by Detected a Malicious Access to lsass Process containing Misc.domain (Clear Filter)

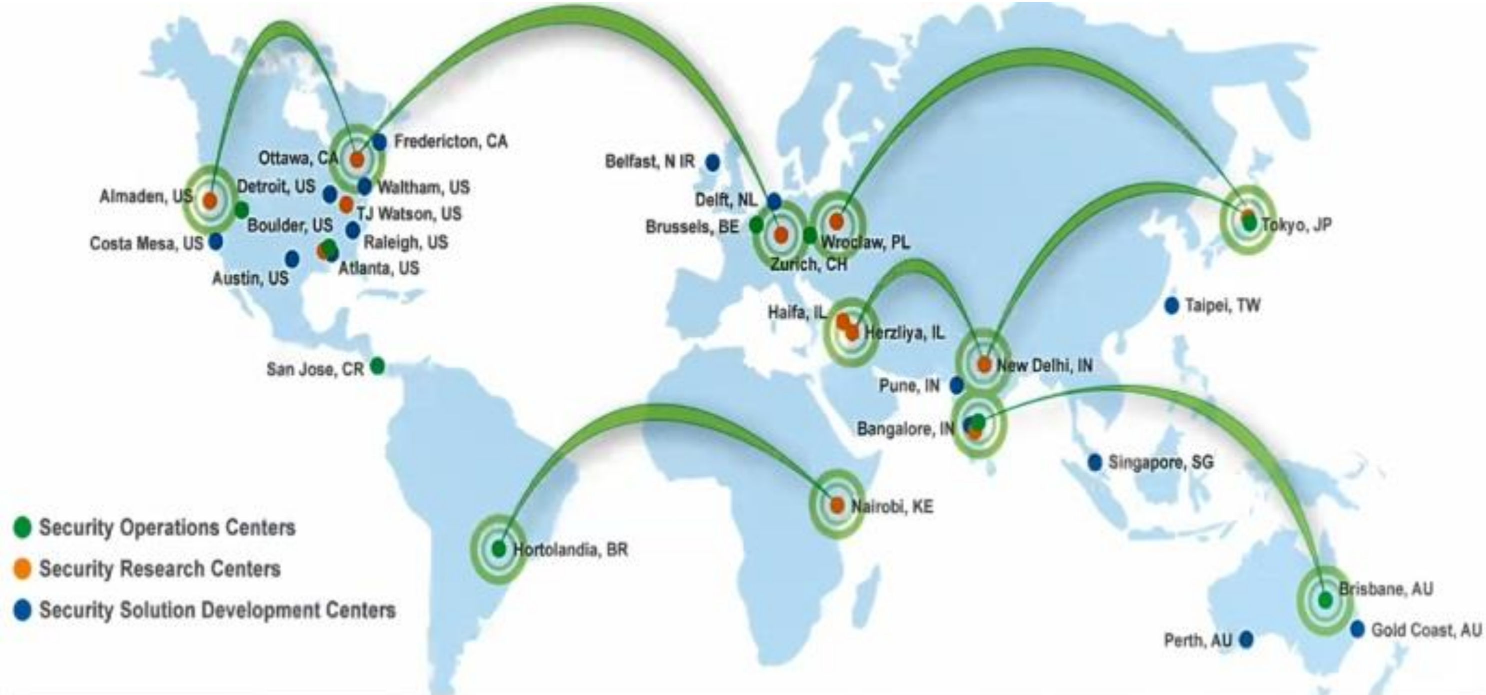
▸ Current Statistics

(Show Charts)

	Event Name	Log Source	Event Count	
	Potential data exfiltration using large DNS packets	Custom Rule Engine-8 :: aio-dev	1	Oct 15, 2018, 3:5
	Potential data exfiltration using large DNS packets	Custom Rule Engine-8 :: aio-dev	1	Oct 15, 2018, 3:5
	Potential data exfiltration using large DNS packets	Custom Rule Engine-8 :: aio-dev	1	Oct 15, 2018, 3:4
	Potential data exfiltration using large DNS packets	Custom Rule Engine-8 :: aio-dev	1	Oct 15, 2018, 3:4
	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: aio-dev	1	Oct 15, 2018, 3:3
	Firewall Deny	Juniper Firewall and VPN @ 172.16.60.22	1	Oct 15, 2018, 3:3
	Firewall Deny	Juniper Firewall and VPN @ 172.16.60.22	1	Oct 15, 2018, 3:3
	Firewall Deny	Juniper Firewall and VPN @ 172.16.60.22	1	Oct 15, 2018, 3:3
	Firewall Deny	Juniper Firewall and VPN @ 172.16.60.22	1	Oct 15, 2018, 3:3
	iting for 172.16.60.80...	Juniper Firewall and VPN @ 172.16.60.22	1	Oct 15, 2018, 3:3

PROPOSED SOLUTIONS

- Marketing and Manufacturing Plans



IBM Security by the Numbers

130 + monitored countries (MSS)

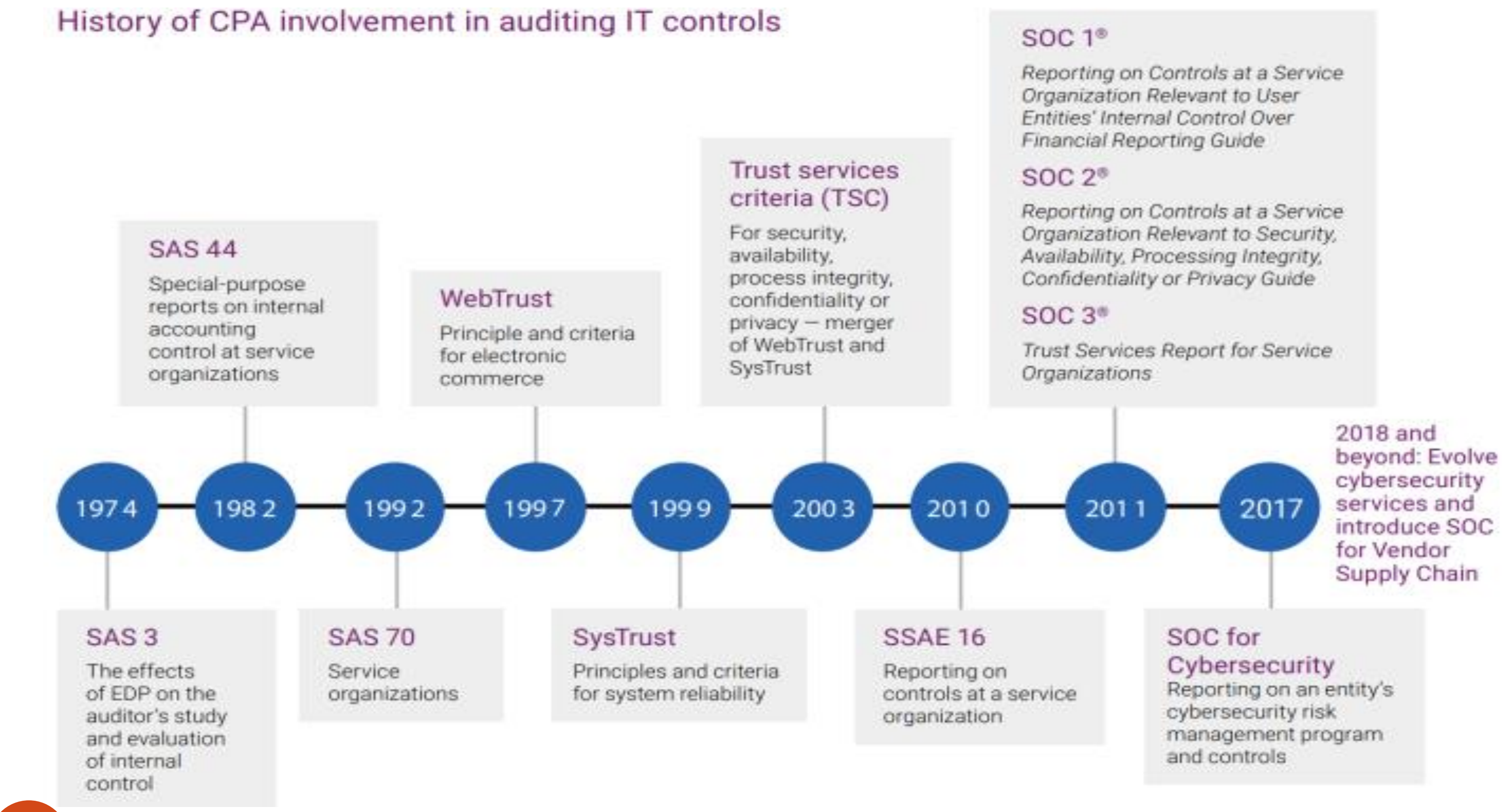
3300 + service delivery experts

270000000 + endpoints protected

35000000000 + events managed per day

PROPOSED SOLUTIONS

IBM QRadar



History of CPA involvement in auditing IT controls

1974

SAS 3

The effects of EDP on the auditor's study and evaluation of internal control

1982

SAS 44

Special-purpose reports on internal accounting control at service organizations

1992

SAS 70

Service organizations

1997

WebTrust

Principle and criteria for electronic commerce

1999

SysTrust

Principles and criteria for system reliability

2003

Trust services criteria (TSC)

For security, availability, process integrity, confidentiality or privacy — merger of WebTrust and SysTrust

2010

SSAE 16

Reporting on controls at a service organization

2011

SOC 1®

Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting Guide

SOC 2®

Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy Guide

SOC 3®

Trust Services Report for Service Organizations

2017

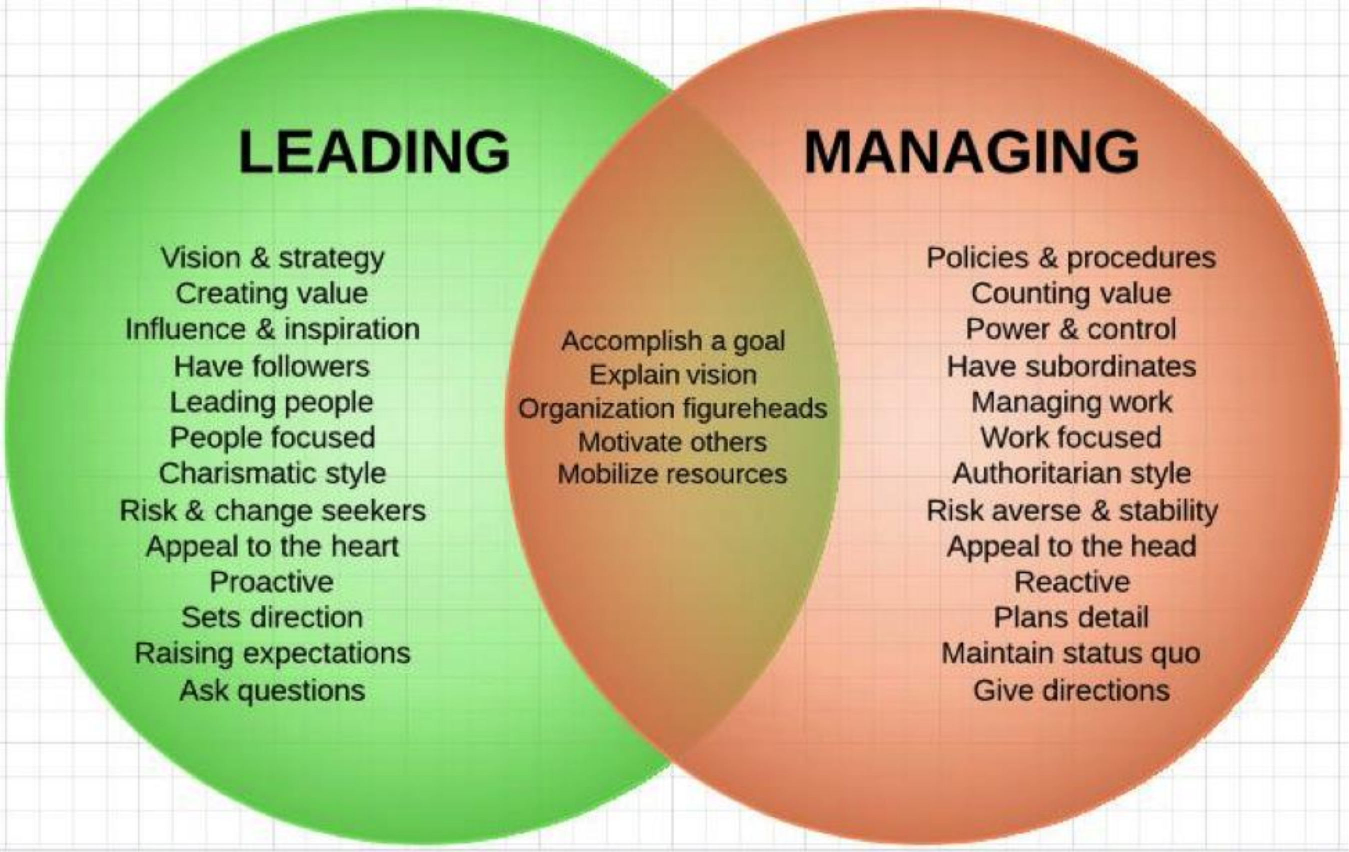
SOC for Cybersecurity

Reporting on an entity's cybersecurity risk management program and controls

2018 and beyond: Evolve cybersecurity services and introduce SOC for Vendor Supply Chain

PROPOSED SOLUTIONS

- **Leadership and Management Styles**



LEADING

Vision & strategy
Creating value
Influence & inspiration
Have followers
Leading people
People focused
Charismatic style
Risk & change seekers
Appeal to the heart
Proactive
Sets direction
Raising expectations
Ask questions

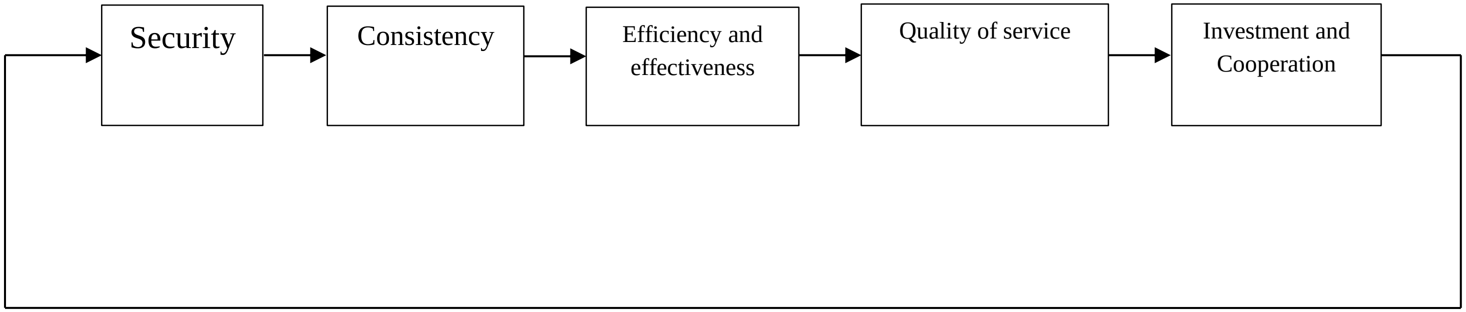
Accomplish a goal
Explain vision
Organization figureheads
Motivate others
Mobilize resources

MANAGING

Policies & procedures
Counting value
Power & control
Have subordinates
Managing work
Work focused
Authoritarian style
Risk averse & stability
Appeal to the head
Reactive
Plans detail
Maintain status quo
Give directions

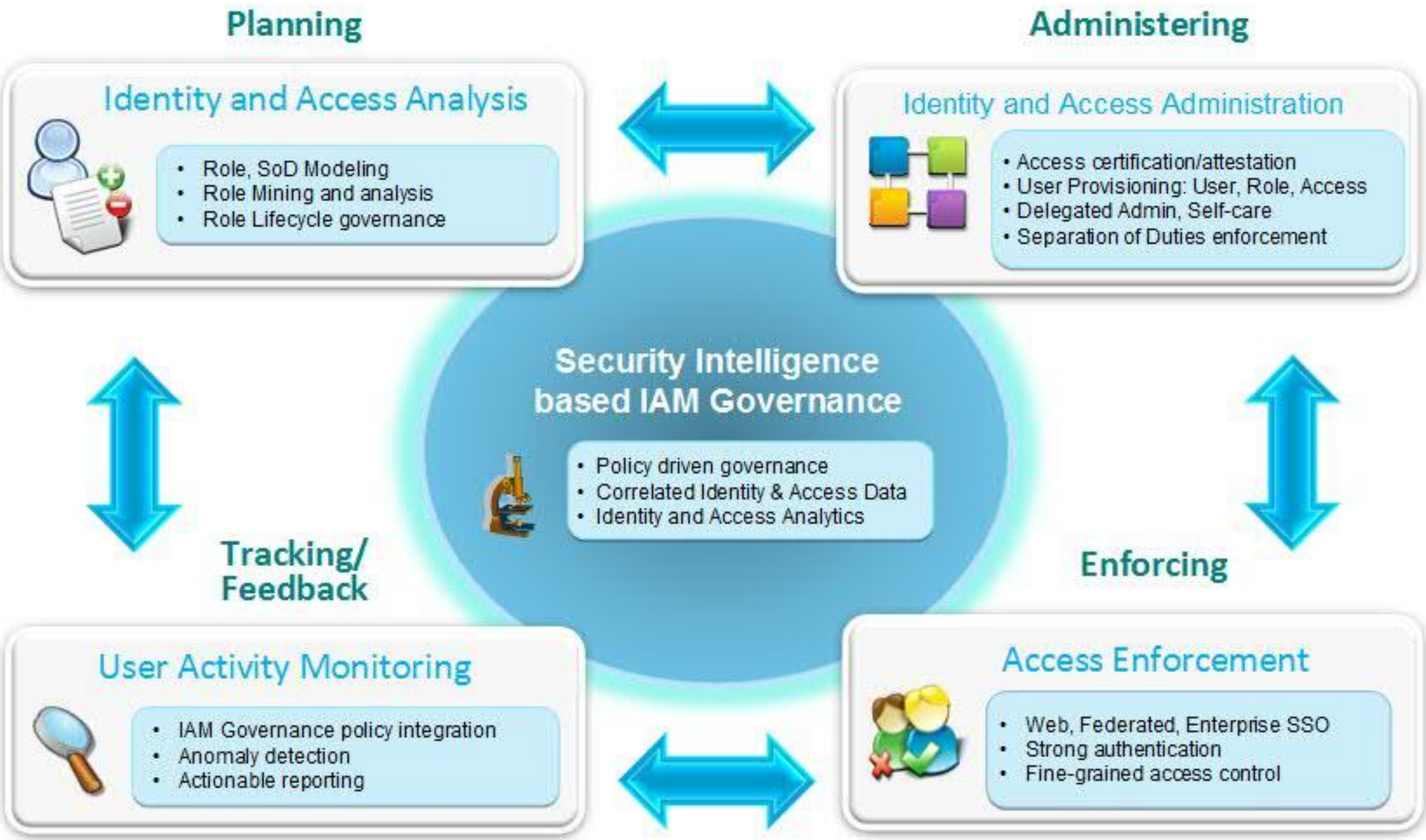
PROPOSED SOLUTIONS

Value Analysis of the Plan



Strength	**Weakness**
• log management • well-designed governance plan • Measurable risk posture • Machine learning and Artificial Intelligence technology to automate course of action • real-time threat scanning and detection • user driven analytics	• multiple technologies in log management (deployed SPLUNK)
Opportunity	**Threat**
• having an integrated platform • stronger metrics for risk posture • Prediction of a wider range of incidents	• Multiple technologies allow anomalies to exploit vulnerabilities • Complex scenarios of data breach

PROPOSED SOLUTIONS



Planning

Identity and Access Analysis

- Role, SoD Modeling
- Role Mining and analysis
- Role Lifecycle governance

Administering

Identity and Access Administration

- Access certification/attestation
- User Provisioning: User, Role, Access
- Delegated Admin, Self-care
- Separation of Duties enforcement

Security Intelligence based IAM Governance

- Policy driven governance
- Correlated Identity & Access Data
- Identity and Access Analytics

Tracking/ Feedback

User Activity Monitoring

- IAM Governance policy integration
- Anomaly detection
- Actionable reporting

Enforcing

Access Enforcement

- Web, Federated, Enterprise SSO
- Strong authentication
- Fine-grained access control

Financial analysis

Competitor's pricing model

SPLUNK

Splunk Light: $75 per month

Splunk Enterprise: $150 per month **Splunk Enterprise:** $83 per GB

Financial analysis

List of Equipment	Start date of configuration/employment	cost per month	Months	Cost per year
IBM QRadar	October 1st	$ 800	12	9600
Splunk log management	October 1st	$ 300	12	3600
CISO	October 1st	$11,200.00	12	134,000.00
Total				147,200.00

List of Equipment	Start date of configuration/employment	cost per month	Months	Cost per year
IBM QRadar	October 1st	$ 800	12	9600
Splunk log management	October 1st	$ 300	12	3600
Training current staff for CISO position and FERPA compliance	October 1st	$2,500.00	4	10,000.00
Total				23,200.00

CONCLUSION

Role of the IBM Qradar as a well-designed SOC platform

- to identify and manage assets
- to bring insight to the infrastructure and network
- to integrate IT security solutions
- to deploy AI and ML technology for task automation

Different types of deployment:

- ON PREM, as a service, Cloud and Hybrid

Market competitors Analysis

- I compere IBM QRadar with other competitors leading SOC market such as SPLUNK and LogRhythm.
- I performed the SWOT analysis

financial analysis

- I provide financial analysis for ON PREM and Cloud-based service.

BIBLIOGRAPHY

- Tips for Creating a Strong Cybersecurity Assessment Report. (n.d.). Retrieved from https://zeltser.com/security-assessment-report-cheat-sheet/

- IBM QRadar vs Splunk: Top SIEM Solutions Compared. (n.d.). Retrieved from https://www.esecurityplanet.com/network-security/ibm-qradar-splunk-siem-solutions-compared.html
- Jose Bravo (2014). QRadar Risk Manager Capability Overview. Retrieved from https://www.youtube.com/watch?v=uzc-9-DaHqE
- Course: How to configure QRadar to ingest Splunk event logs. (n.d.). Retrieved from https://www.securitylearningacademy.com/course/view.php?id=3705

- Developer, I. (2014, July 08). Introduction To QRadar Forensics. Retrieved from https://www.youtube.com/watch?v=7IifzJZs45s

- System management (n.d.). Retrieved from https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/c_qradar_adm_system_mgmt.html

- IBM QRadar Security Intelligence. (n.d.). Retrieved from https://www.ibm.com/security/security-intelligence/qradar?cm_mmc=Search_Google-_-Security_Detect%20threats%20-%20QRadar-_-WW_NA-_-%20qradar_b&cm_mmca1=000000MI&cm_mmca2=10000099&cm_mmca7=1014221&cm_mmca8=aud-334316643045:kwd-295901328379&cm_mmca9=_k_EAIaIQobChMI84K6yPv44gIVAspkCh2ZiA_bEAAYASAAEgKiSPD_BwE_k_&cm_mmca10=345024606176&cm_mmca11=b&gclid=EAIaIQobChMI84K6yPv44gIVAspkCh2ZiA_bEAAYASAAEgKiSPD_BwE

- IBM. (2019). Retrieved from https://en.wikipedia.org/wiki/IBM

- COST OF CYBER CRIME STUDY (2017). Retrieved from

https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

- CPAs: Helping service organizations build trust and transparency. (n.d.). Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-service-organizations-brochure.pdf

- Gartner Chart. (2018). Retrieved from https://www.gartner.com/doc/reprints?id=1-5WGR9UB&ct=181205&st=sb

- LogRhythm vs Splunk: Top SIEM Solutions Compared. (n.d.). Retrieved from https://www.esecurityplanet.com/products/logrhythm-vs-splunk-siem-solutions-compared.html

- FERPA Compliance Training Protects the Privacy of Your Students. (n.d.). Retrieved from https://www.knowledgecity.com/Employee-Training/FERPA-Compliance?gclid=EAIaIQobChMIjtG0zfHQ4wIVCb3sCh0BsgSyEAAYASAAEgIrlfD_BwE/ferpa-thankyou.html
- Key Reinstallation Attack (2017) Retrieved from

https://papers.mathyvanhoef.com/ccs2017.pdf