IBM Security

IBM Security Portfolio

Ankit Jain

IBM Security

ajain126@in.ibm.com

IBM

IBM has the world's broadest and deepest security portfolio

IBM QRadar by the numbers

6K+	customers	IBM Qradar has been replacing existing SIEM deployments across the world
300+	applications	Unique capability to build custom application on Qradar platform. Cognitive Analysis App – 1st and only Solution presently
10+	threat intelligence sources (STIX / TAXII, X-Force, Threatstream, Recorded Future, FireEye, RiskIQ, Threat Connect, Custom)	Unparalled capability – and the subscription is free.
1,664	unique report (e.g., Compliance, Configuration and Change Management, Executive, Log Source, Network Management, Security, Usage Monitoring, Virtual Infrastructure, Vulnerability Management)	Largest library of reports, including Vulnerability Management reports
632	correlation rules / building blocks	Unique usecase library – allows customers to choose the usecases
500+	supported devices, systems, applications and cloud services	
20	third-party vulnerability scanners (e.g., Qualys, Rapid7, Tenable, Tripwire, AppScan, …)	Inbuilt Vulnerability and Configuration Check …
5	flow sources (NetFlow, J-Flow, sFlow, vFlow, and QFlow)	Does not need separate infrastructure to deliver Network Intelligence
1.5M+	EPS implementations	Massive Scalability , with High Availability and Disaster Recovery capability
< 5	month average to fully implement	Automated Discovery of assets, health check applications etc.

QRadar

Security Intelligence Platform

IBM Security

QRadar Product Portfolio

Area of Focus

Security Intelligence platform that enables security optimization through advanced threat detection, meet compliance and policy demands and eliminating data silos

Portfolio Overview

QRadar Log Manager

- Turnkey log management for SMB and Enterprises
- Upgradeable to enterprise SIEM

QRadar SIEM

- Integrated log, flow, threat, compliance mgmt
- Asset profiling and flow analytics
- Offense management and workflow

X-Force IP Reputation Feeds

Network Activity Collection & Prevention (QFlow) and Network Insights (QNI), Network analytics, behavior and anomaly detection

- Layer 7 application monitoring
- Real-time network packet analysis

QRadar Vulnerability Manager, including Risk Management

- Integrated Network Scanning & Workflow
- Risk Management to prioritize vulnerabilities
- Predictive threat modeling & simulation
- Scalable configuration monitoring and audit
- Advanced threat and impact analysis

QRadar Incident Forensics & Packet Capture

- Reconstruct raw network packets to original format
- Determine root cause of security incidents and help prevent recurrences

Reduce costs, increase visibility with an integrated platform

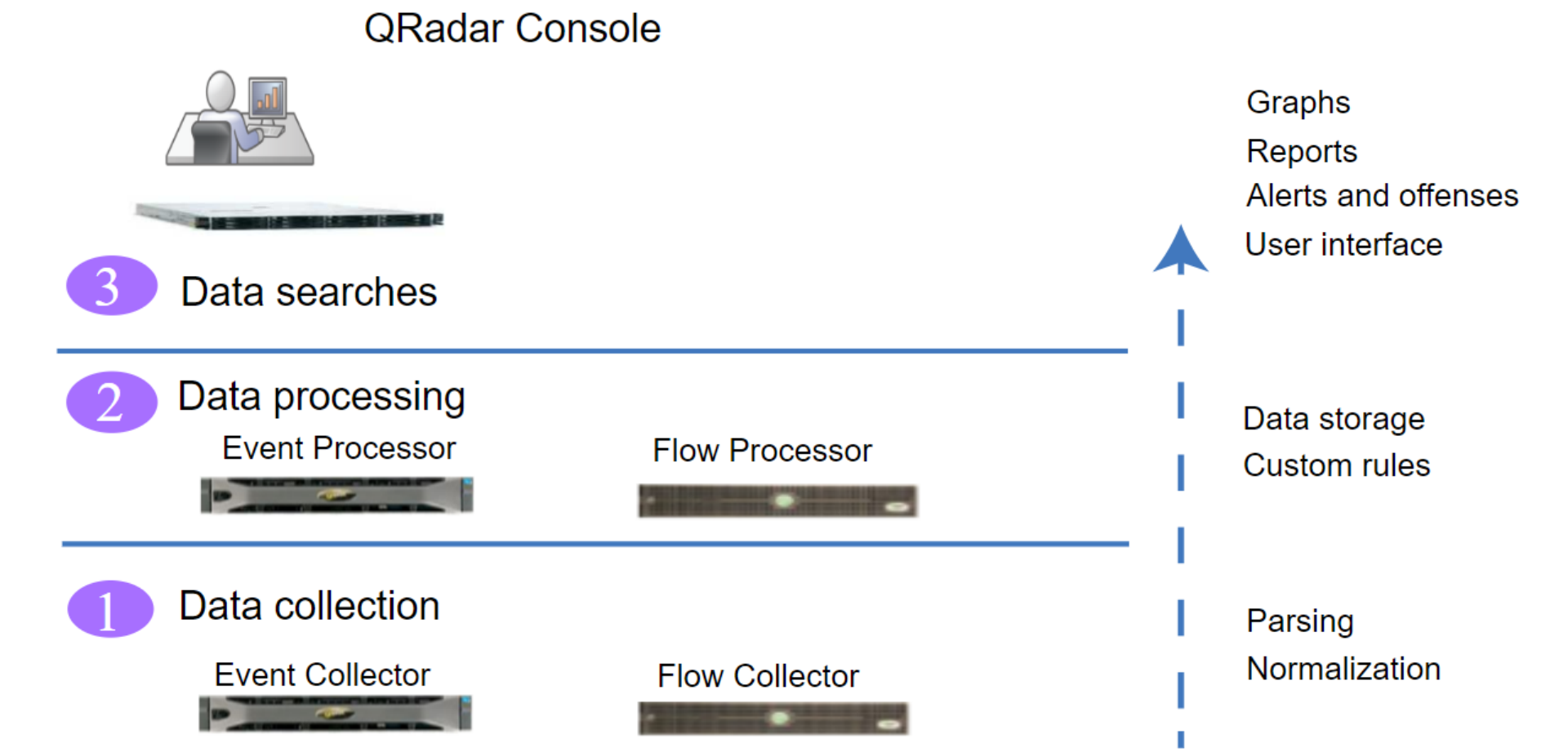
	Traditional SIEM *7 products from 7 vendors*
Flows	ARBOR NETWORKS, Lancope, riverbed Think fast.
Packets	EMC² RSA, SOLERA NETWORKS
Vulnerabilities	QUALYS, RAPID7, tenable network security
Configurations	algosec FIREMON, skybox security, tufin, REDSEAL NETWORKS
Logs	loglogic, splunk>
Events	hp ArcSight, McAfee, EMC² RSA
Response	Remedy, JIRA, servicenow
UBA	exabeam, SECURONIX

IBM Security Intelligence and Analytics

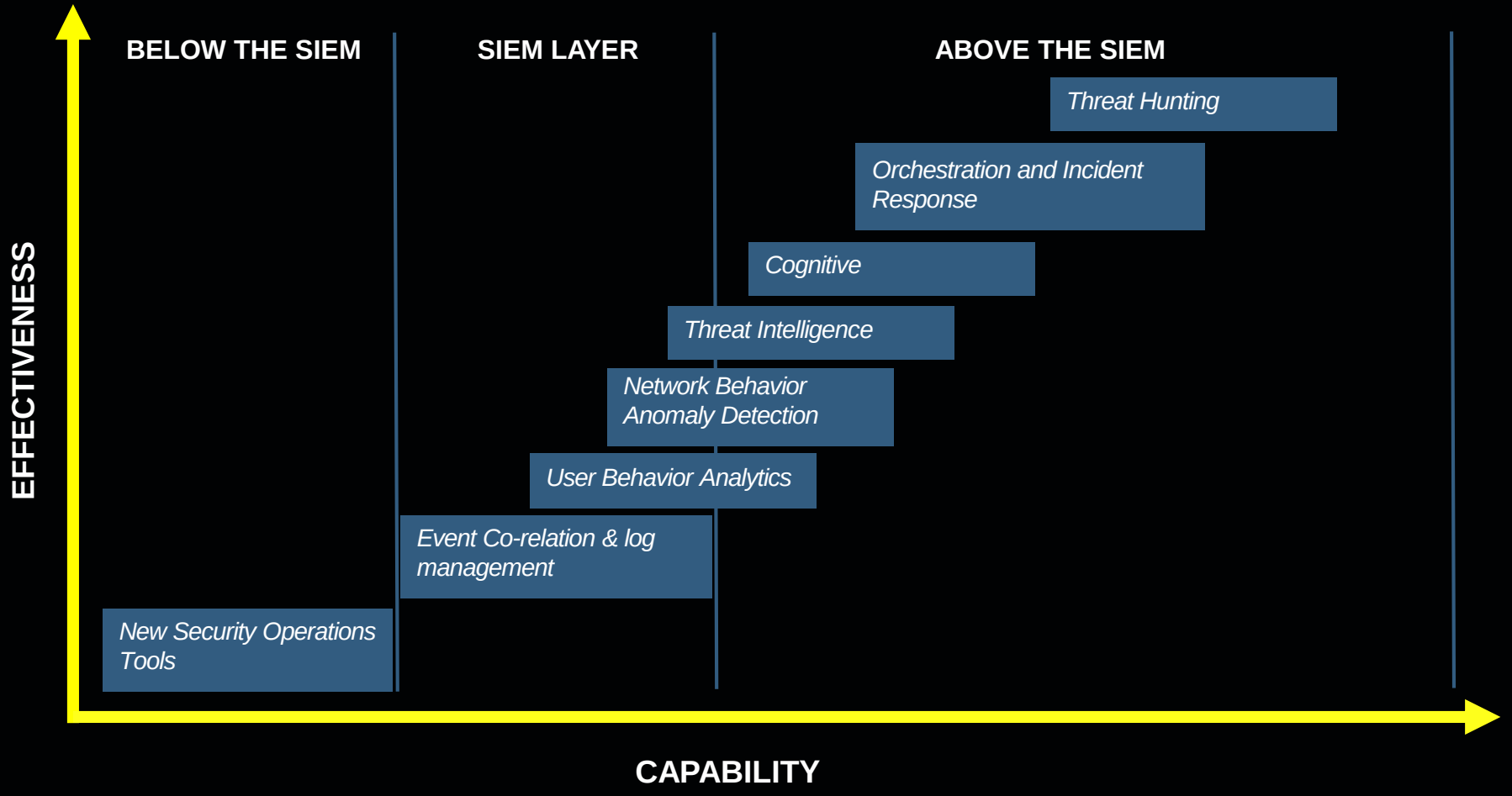
An integrated, unified architecture in a single web-based console

IBM Security QRadar Security Intelligence Platform

QRadar Architecture



The Detailed Roadmap to STOP THREATS



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM