Discover IBM Security Expert Essentials:

Build Your Skills and Get Software Support You Can Trust

Peter Santoro
Pieter Ampe
Alaa Ali

sel@us.ibm.com

IBM Security Community

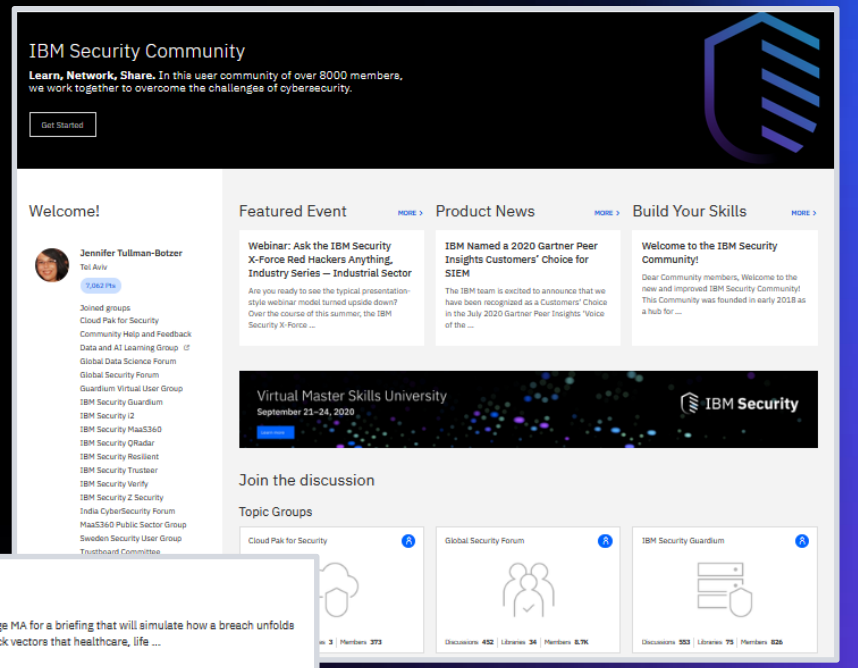
https://ibm.com/community/security

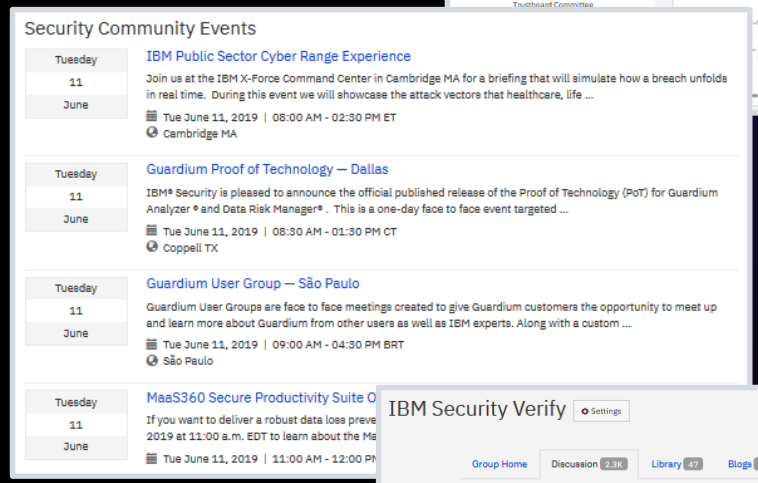
Learn: The indispensable site where users come together to discover the latest product resources and insights — straight from the IBM experts.

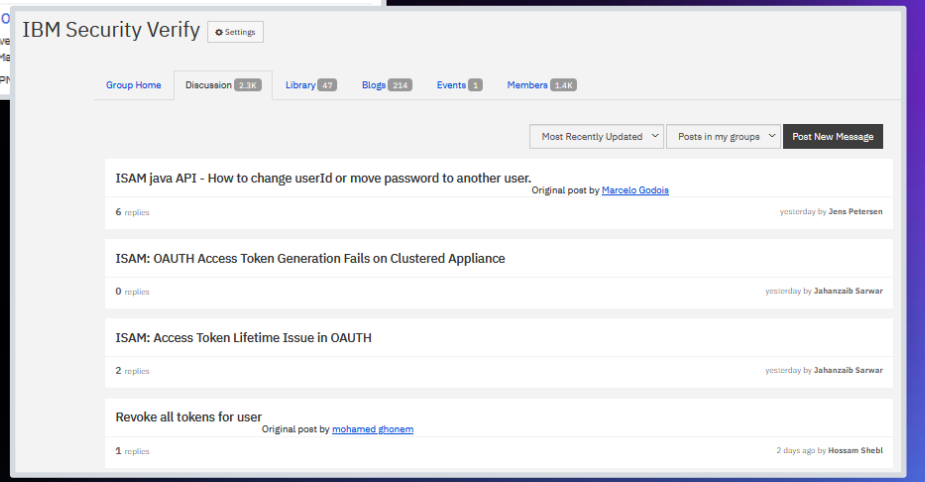
Network: Connecting new IBM clients, veteran product users and the broader security audience through engagement and education.

Share: Giving YOU a platform to discuss shared challenges and solve business problems together.

9500+ Members Strong and Growing Every Day!







Common Security Operations Challenges

Skills shortages

- Global security skills shortage
- Integration with IBM Security Software

Technical obstacles

- Adaption and integration of existing tools with emerging technologies
- Automation of processes

Security policies

- New requirements for securing remote employees and end users
- Secure, rapid development workflows

Who is the Security Expert Labs team?

This worldwide network of software experts can help you deploy, optimize and expand your IBM Security tools and solutions, while also helping your team build your own skills and become self-sufficient.

ADOPT

Security Expert Labs consultants use proven strategies, security best practices and innovative solutions like AI, Watson™ and managed security models to help you adopt a foundation for growth and stability.

EXPAND

We manage over 250 million identities across more than 1,200 global clients. Our expert consultants accelerate the deployment of your IBM Security solutions, matching the size and scale needed to meet your business objectives.

OPTIMIZE

Drawing on our unparalleled software knowledge and support capabilities, we help your team quickly move your projects to completion. We provide the on-going expertise and care to help you stay current with IBM technology to achieve your ROIs.

Whether you need short-term assistance to meet a stated objective, long-term support for ongoing expert access, or personalized enablement with role-based technical training, our team is here to help.

IBM Security Expert Essentials

Delivering the right expertise at the right time.

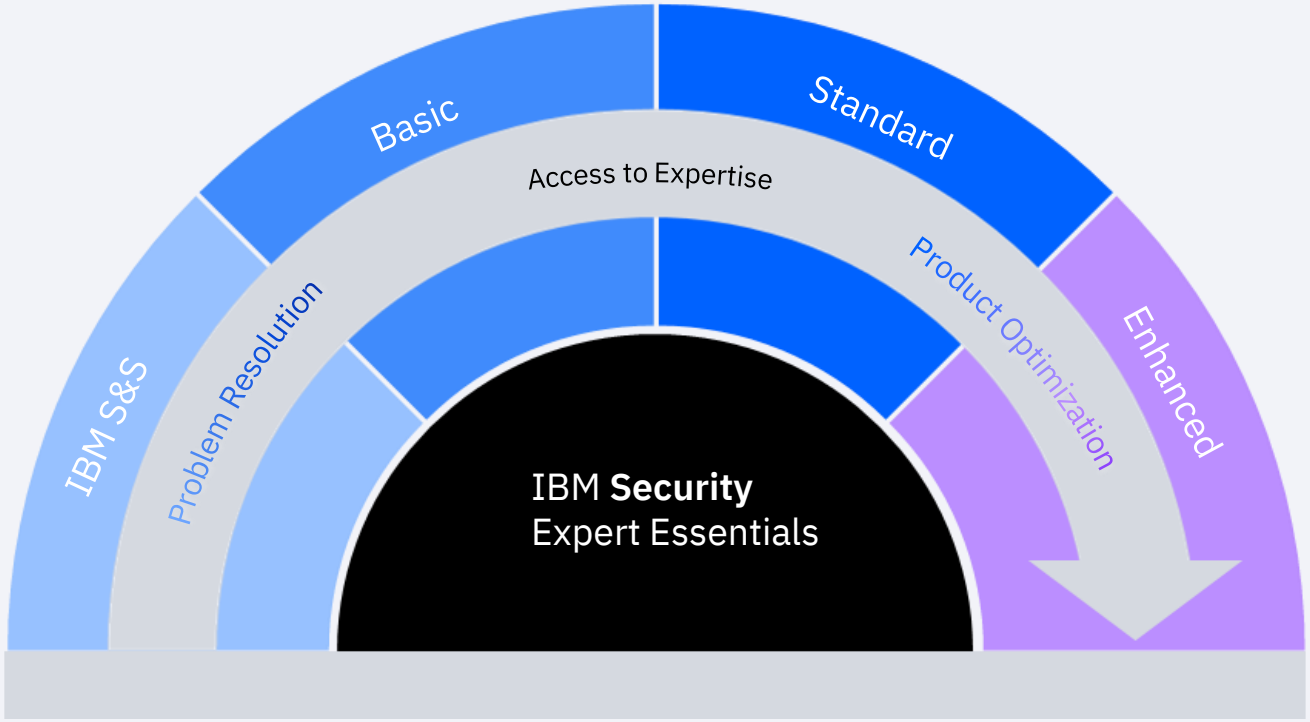
IBM Security Expert Essentials is a tiered, subscription-based bundle of services, available at a fixed annual fee, that provides flexibility based on your skills, project requirements, and business and technical needs.

Technical advice

Customized to help accelerate adoption, improve productivity and experience the full benefit of your IBM Security solutions, while simultaneously building staff expertise.

Ongoing lifecycle services

For reliable continuous security operations, and guidance on evolving best practices across the lifecycle to improve solution capabilities, performance, and stability, and to reduce risk



IBM Security Expert Essentials

What you get with each tier of service

Email

sel@us.ibm.com

for details

Segment	Outcome	Basic	Standard	Enhanced
On Demand Consulting	*Lists of specific offerings and use of consulting weeks that account managers utilize for client-driven requests*	n/a	n/a	**3 weeks** Migration Assessments Staff Augmentation Troubleshooting Optimization and Tuning High-level plan of actions to support your business initiatives
Priority Case Handling	*Account Manager supports named callers and prioritizes product support cases*	n/a	3 customer callers	5 customer callers
Single Point of Contact	*Account Manager responsible for regular checkpoints, product support and orchestrating expert essentials*	n/a		
Solution Review & Assistance Consulting	*Lists of specific offerings and use of consulting weeks that account managers utilize for IBM-driven recommendations.*	n/a	**2 weeks** Performance Tuning Best Practices mentoring Integration Workshops Architecture and Advisement Health checks	**3 weeks** **Includes Standard plus:** Administration as a Service Installation and Configurations Solution Assurance Development Skills Transfer Gaps in Technology Roadmaps Identify risks and recommendations
Trusted Advisor Reviews	*Recurring checkpoints and sessions on various topics delivered for business and technical stakeholders in security solution success*	Product Roadmap Reviews Skills Assessment/ Education Roadmaps Operations Reviews Tech Talks	**Includes Basic plus:** Maturity Model Reviews Value Assessments Upgrade/Migration Planning Dev and operations best practices	**Includes Basic and Standard plus:** Integration use cases Architecture and Deployment tech talks for services providers, enterprise deployments
Personalized Training	*Front-end to Security Learning Academy; roadmaps by role; self paced virtual courses, badging*			
Unlimited Online Expert Q&A	*Access to Portal for deployment questions; routed to subject experts; knowledge transfer*	2 customer resources for Q&A	3 customer resources	5 customer resources

Areas of expertise include:

Data Security
- Guardium Insights
- Guardium Data Protection
- Guardium Appliance Hardware
- Guardium S-TAP for zOS
- Guardium Key Lifecycle Manager
- Guardium Key Lifecycle Manager for z/OS
- Guardium Data Encryption
- Guardium Data Encryption for zOS
- Data Risk Manager

Mobile Security
- MaaS360

Threat Intelligence
- X-Force Exchange Commercial API Standard
- X-Force Exchange Commercial API Enterprise
- Advanced Threat Protection Feed by X-Force

Security Intelligence
- QRadar Appliance Hardware
- QRadar Appliance Hardware (MVS TSS)
- QRadar Log Manager
- QRadar SIEM
- QRadar Applications
- QRadar Forensics
- QRadar Network Insights
- QRadar on Cloud
- QRadar Cloud Apps
- QRadar Advisor with Watson
- QRadar Vulnerability Manager and Risk Manager
- Resilient

Intelligence Analysis and Investigations
- i2 Analyst's Notebook and other i2 software
- i2 Analyst's Notebook Premium
- i2 Analyze
- i2 iBase and i2 Analyst's WorkStation
- i2 Enterprise Insight Analysis
- i2 Connect

Cloud Paks
- Cloud Pak for Security
- Threat Intelligence Insights for Cloud Pak for Security

Identity and Access Management
- Verify Access
- Verify Access Privilege Vault
- Federated Identity Manager
- Identity Governance & Intelligence
- Enterprise Single Sign-on
- Directory Integrator
- Directory Server

IBM Security / © 2020 IBM Corporation

QRadar Offerings

Standard QRadar offerings

Deployment

QRadar Administration as a Service

Health Optimization and Tuning for S, M L Deployments

Onboarding IBM QRadar on Cloud

QRadar Advisor w/Watson Readiness Service

QRadar Migration: ArcSight to QRadar

QRadar Deployment for All-In-One

QRadar Deployment for S, M L Distributed

QRadar on Cloud Deployment for S, M, L Distributed

QRadar Upgrade and Migration for S, M, L Deployments

Deployment Add Ons

Configuration for Disaster Recovery

QRadar Risk Manager and Vulnerability Manager Deployment

QRadar Incident Forensics Deployment

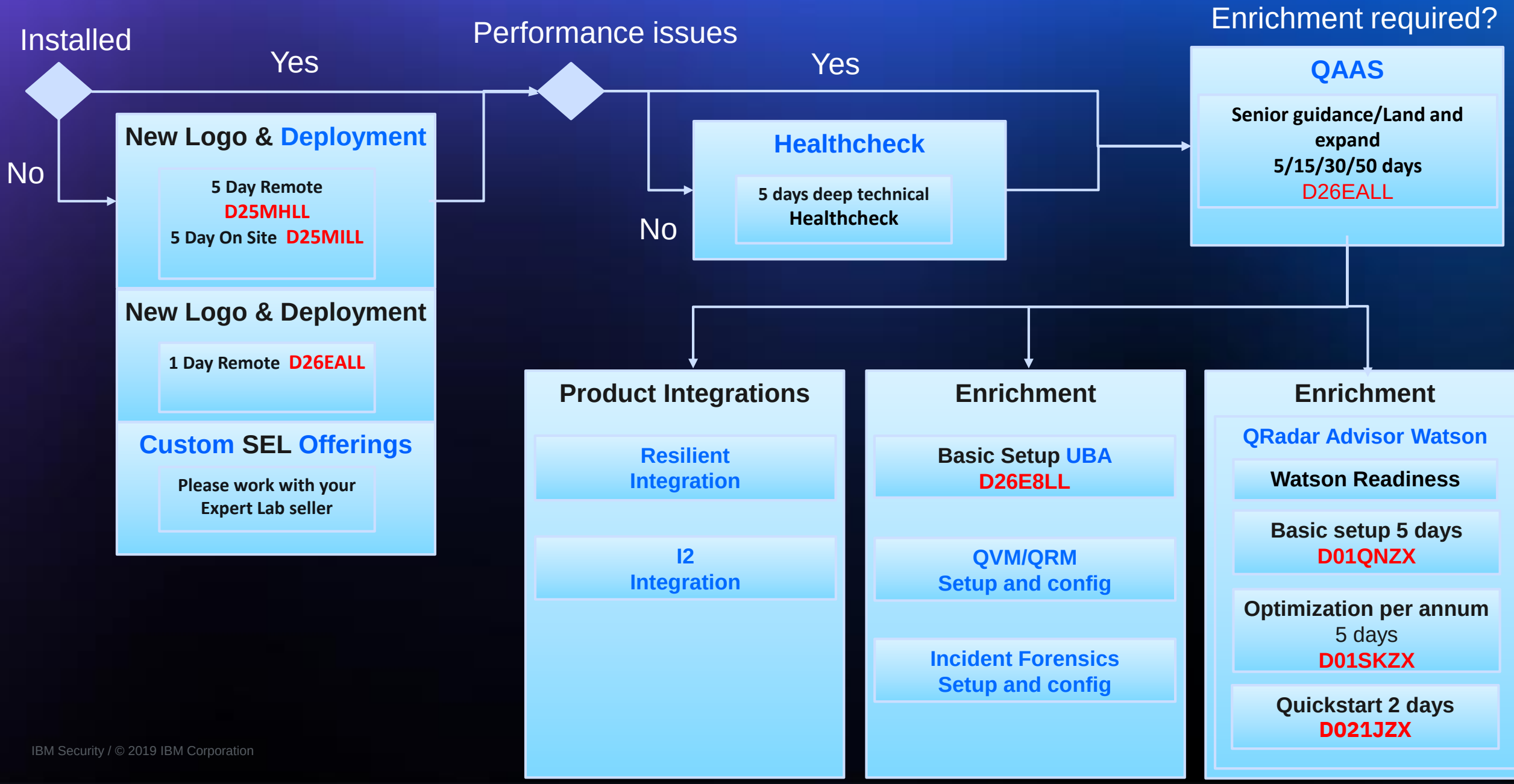
Custom uDSMs

Custom Enablement Workshop

QRadar Basics

Custom Enablement Workshop - QRadar Administration

QRadar

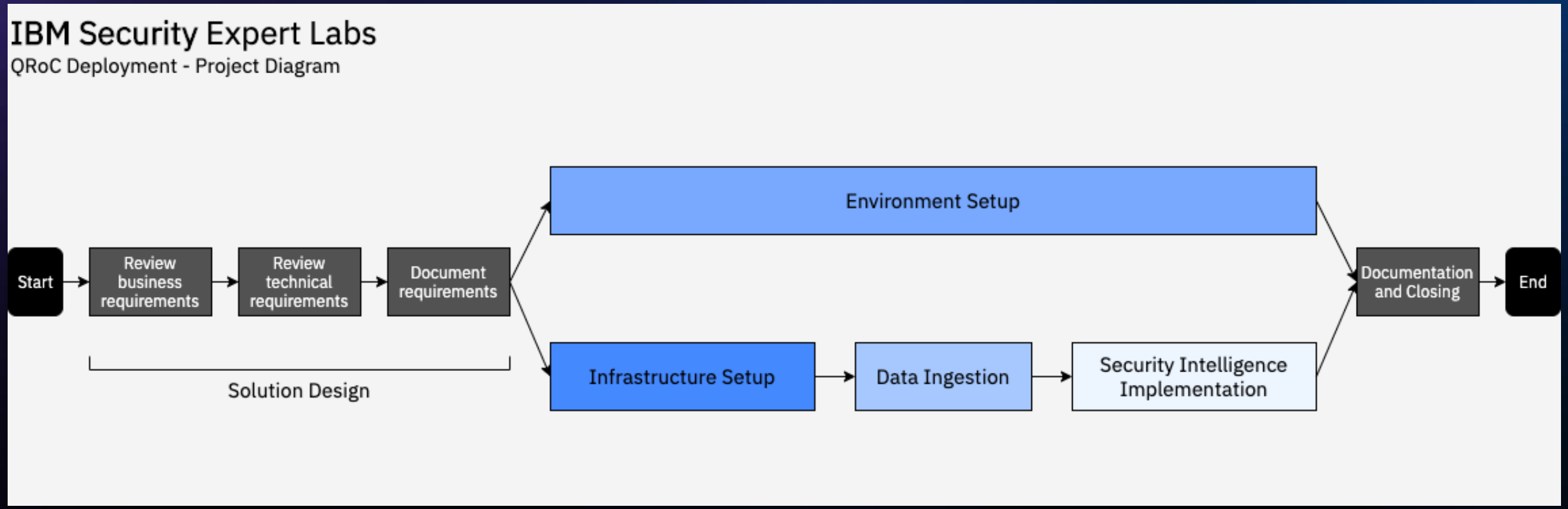


IBM Security / © 2019 IBM Corporation

IBM Security QRadar on Cloud Setup (D003TZX)

- Deploy QRadar on Cloud (QRoC) without worrying about continued large infrastructure maintenance
- Accelerated onboarding of data sources (log sources) into QRoC

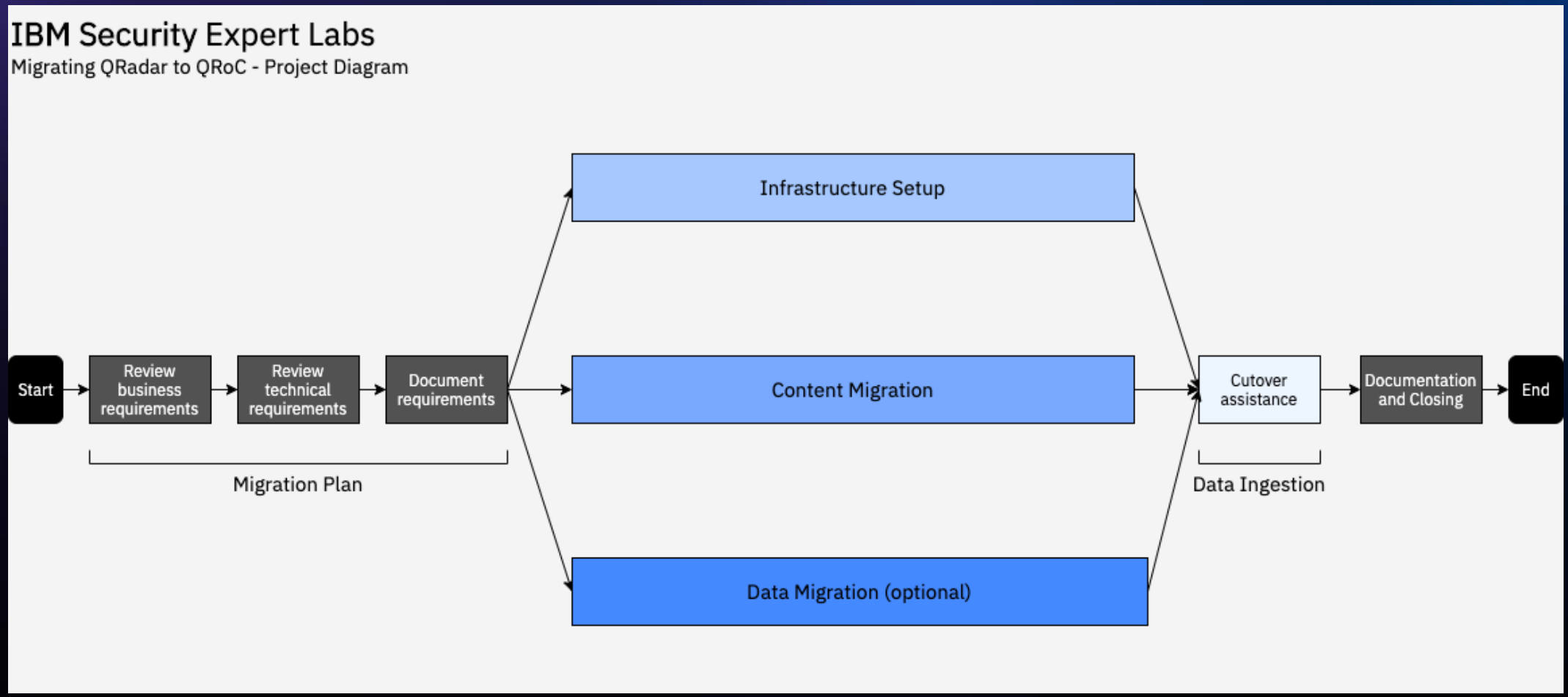
What to expect from this project:



IBM Security QRadar on Cloud Migration (D003TZX)

- Mitigate migration risk by using SIEM consultants to outline a solid migration plan
- Benefit from expertise to provide best practices, tuning, and optimization

What to expect from this project:



IBM Security QRadar on Cloud Custom Parser Setup (D003SZX)

- Ingest logs from a custom device using a supported ingestion mechanism
- Quickly gain visibility into security-relevant logs after custom parser is created

IBM Security QRadar on Cloud 8 Day Remote Optimization Service per annum (D003UZX)

- Senior product guidance on optimization of the use of QRoC:
  - Health check
  - Tuning
  - Optimization
  - Enablement

Large defense corporation

Protecting its cloud environment with QRadar on Cloud, with migration support from Security Expert Labs

Business Challenge:

The client wanted to move their SIEM to the Cloud in order to reduce renewal and operational costs, while maintaining full NIST compliance through customized dashboards. They faced an aggressive timeline and had several custom parsers to migrate.

Solution:

Migrate to **QRadar on Cloud** with the lead of **IBM Security Expert Labs** using an agile approach in a very compressed timeline by providing architectural oversight and recreating close to 340 dashboards and roughly 40 custom parsers. This has opened up future opportunities to utilize QRadar on Cloud's UBA Machine Learning as well as Resilient to automate audit workflows.

Outcome:

- Seamless user transition into QRadar on Cloud
- Continued NIST compliance within imposed hard deadline

Solution Components:

– QRadar on Cloud
– IBM Security Expert Labs

IBM Security

IBM

Medium-sized healthcare institution

The client wanted to migrate to the Cloud while ensuring their deployment remains healthy and follows best practices during the digital transformation process and beyond.

Solutions: QRadar on Cloud and IBM Security Expert Labs

The healthcare organization called on the expertise of the IBM Security Expert Labs team, comprised of solution architects and SIEM consultants, to rapidly migrate their on-prem QRadar to QRoC and to perform several tuning activities for rules and DSMs and to create a new custom DSM.

IBM **Security**

20k EPS

UBA deployed
Custom DSM created
Tuned rules and parsing

How We Can Help You Achieve Success

The team did an analysis of our support cases and found patterns that our Expert Essentials subscription could help with.

IBM went through the QRadar upgrade process with us step by step and ensured that support was even available over the weekend should we face any unexpected challenges.

The monthly case reports we get through our Expert Essentials subscription have proven invaluable in showing us trends in cases and allowing us to act quickly when needed.

We were having some issues installing UBA until the IBM team helped us produce a plan of staged installs and daily metrics.

Our Expert Labs consultant helped us become more proactive in reporting the health of our deployment so we could catch issues before they became real problems.

IBM helped us plan and implement a successful Guardium upgrade of 1200 appliances. Doing this work alone would have taken our team substantially longer.

Connect with us

Request additional info or schedule a consultation:

sel@us.ibm.com

Learn more:

https://ibm.com/security/security-expert-labs