Simplifying SIEM migration

IBM Security

IBM

Contents

Introduction

You know your data is at risk everywhere—on premises and in the cloud. And if your team is like 70% of security operation centers (SOCs), chances are you rely on a security information and event management (SIEM) software to detect and analyze threats.[1] Given the evolving threat landscape, new environments and data sources, it's critical that your SIEM solution is able to seamlessly monitor across your organization's entire infrastructure, even as your business grows.

If you're reading this ebook, you're probably thinking of migrating to a next-generation SIEM solution and know that a SIEM migration is not a simple task. A successful SIEM migration starts with choosing the right IT service provider that can offer you strong migration expertise.

The IBM Security™ QRadar® platform is a comprehensive SIEM solution that can help you quickly detect and prioritize potential threats to your business. The IBM Security experts have helped dozens of companies migrate their traditional SIEM solutions. IBM has the experience, skills, technology, and resources to give you a smooth migration path.

On average companies take

279 days

to detect and contain a data breach.[2]

Benefits of upgrading to a next-generation SIEM platform

Why QRadar?

Ingests vast amounts of data from on-premises and cloud sources

Offers deep visibility and flow analysis of network traffic and metadata

Includes access to IBM Security X-Force® Threat Intelligence at no additional charge

Applies built-in analytics to accurately detect threats

Enables artificial intelligence (AI)-assisted investigations and incident prioritization

Fosters an ecosystem by providing more than 500 out-of-the-box integrations

Enables deployment on premise or in the cloud using a flexible architecture

Correlates related activities to prioritize incidents

Offers integration of the MITRE ATT&CK framework for threat detection, investigation and response processes

Includes open and customizable behavioral models for profiling users and assets

Eliminates manual tasks by automatically parsing data and normalizing logs

Provides comprehensive and centralized visibility

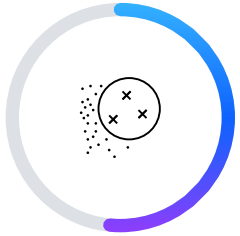
The QRadar platform offers a next-generation SIEM solution to monitor and detect threats across applications, users, containers, endpoints, networks, and cloud environments in real time.

The QRadar SIEM platform is designed to provide security teams with centralized visibility to identify threats and anomalies early in the attack lifecycle. As data is ingested, the solution applies real-time security intelligence and analytics to quickly and accurately detect and prioritize threats. Your SOC team will gain a centralized view into logs, flows, and events across on-premises, software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) environments.

"Using IBM QRadar SIEM is like having eyes in the back of your head. Before, we always felt like we were on the back foot when it came to security, but now we're much more proactive."

Michael Warrer
Chief Information Officer, NRGi

Read the case study →



QRadar increases the ability to accurately detect real attacks by

51%[3]

Features built-in analytics to accurately detect threats

The QRadar solution analyzes threat data to accurately detect known and unknown threats that others miss. Built-in analytics help shorten time to value without requiring data science expertise.

QRadar is designed to correlate activity across the entire network and apply a spectrum of signature-based and behavioral-based detection methods to identify known and unknown threats.

The IBM Security team's decades of expertise in SIEM has been infused directly into QRadar through a vast library of expertly built signature-based rules. The solution uses behavioral modeling for baselining user activity, enabled via integrations with Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory.

QRadar can detect behavioral anomalies and risky behavior that indicates malware takeover of a user account, compromised credentials, or malicious insider activity. Security analysts can quickly identify users with elevated risk scores, and create prioritized watchlists for privileged users, executives, or machine accounts. QRadar enables SOC teams to rapidly scale insider threat programs with custom behavioral detection models via an integrated machine learning (ML) model builder.

IBM Security QRadar SIEM solution

- Real-time correlation and behavioral anomaly detection
- Threat intelligence and vulnerability insight
- Machine learning, service and user profiling

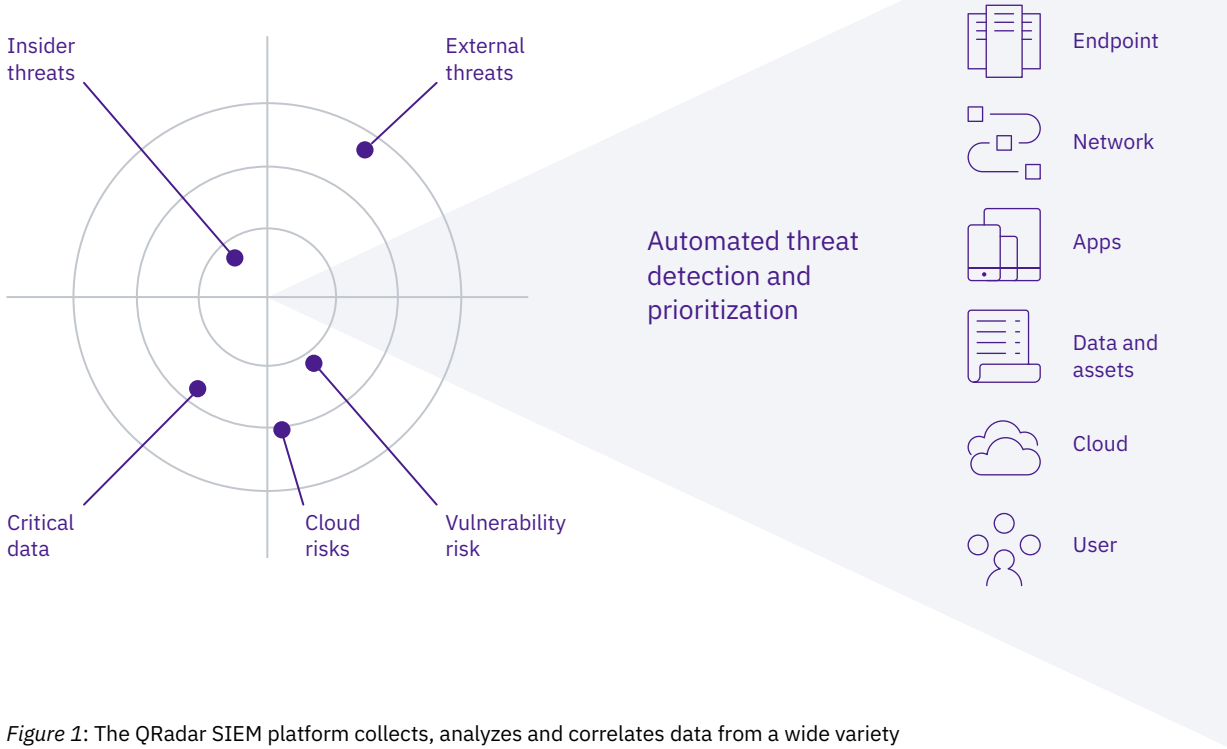


Figure 1: The QRadar SIEM platform collects, analyzes and correlates data from a wide variety of sources to detect and prioritize the most critical threats that require investigation

Features built-in analytics to accurately detect threats

Continued

Additionally, QRadar uses advanced network analysis to sense a change in network traffic, such as the appearance of a new host or abnormal communications between existing hosts. Network analysis gives security analysts a deeper understanding of system, application, and network traffic. QRadar can detect east-west traffic that may indicate lateral movement, identify advanced threats as they traverse the network, and pinpoint attempts at sensitive data exfiltration. Additional network telemetry collected reduces false positives and aids incident responder and threat hunters who can quickly identify affected hosts to begin remediation.

The QRadar platform's analytics engine includes offense chaining, which links related alerts into a single consolidated offense. Offense chaining provides fewer, higher-fidelity alerts and reduces false positives, allowing analysts to triage with confidence. Since all information is available on one screen, it becomes easy for the user to see an overview of related suspicious activity that's been detected. As new events unfold, the IBM QRadar Advisor with WatsonTM app helps prioritize offenses and automatically updates with new data.

.

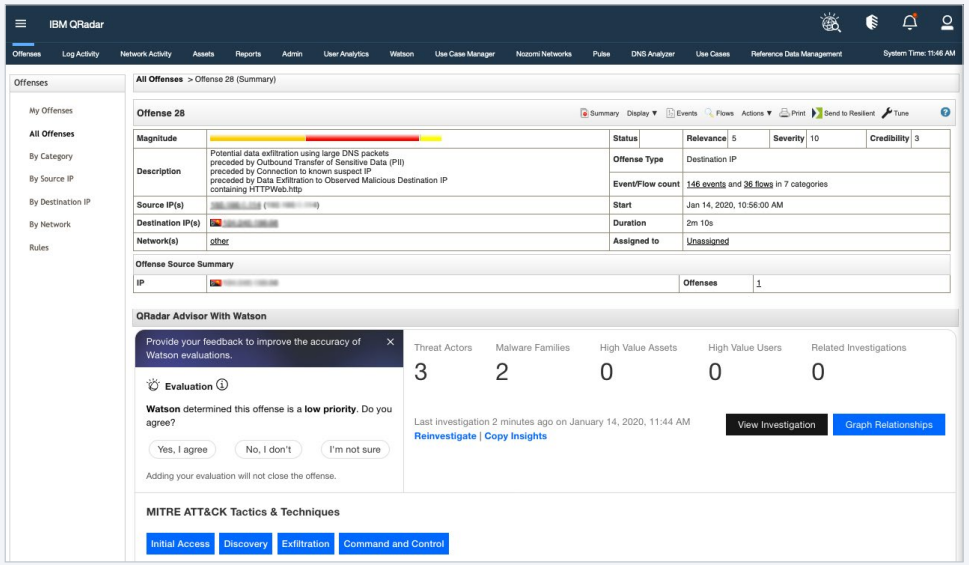


Figure 2: Custom rules and offenses

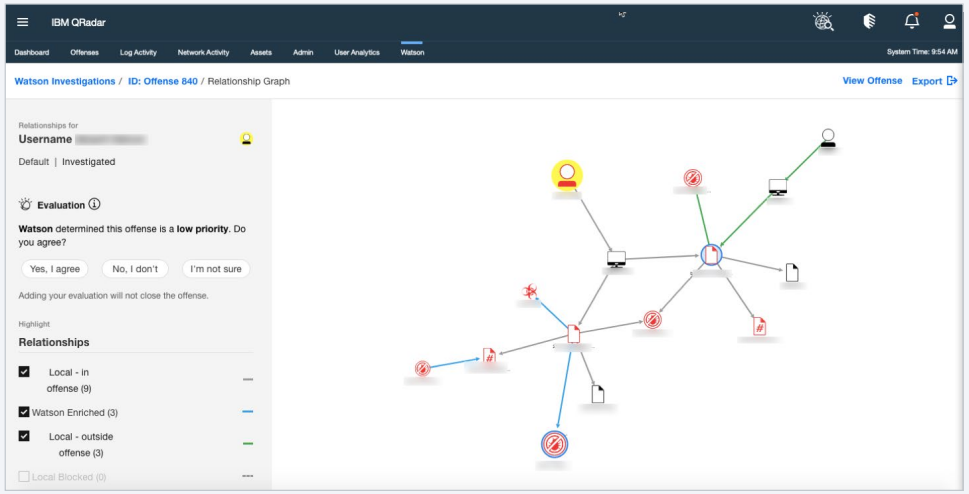


Figure 3: A QRadar Advisor with Watson investigation example

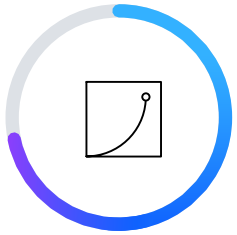
Offers strong out-of-the-box features

The QRadar solution includes more than 500 prebuilt Device Support Modules (DSMs) that provide default setting integrations with commercial off-the-shelf technologies.

Your SOC team can simply point logs to QRadar, and the solution can automatically detect the log source type and apply the correct DSM to parse and normalize the log data. As a result, your organization can get up and running much faster than organizations with alternative solutions. QRadar also offers a DSM Editor with an intuitive graphical user interface (GUI) that's designed to be simple to use and enable security teams to easily define how to parse logs from custom applications.

54%

of respondents say it is very easy to bring logs into QRadar for correlation and analysis.[3]



70%

of respondents say out-of-box QRadar correlation rules are valuable.[3]

Provides flexible architecture on premises or on cloud

The QRadar SIEM solution can be delivered as hardware, software or virtual machines (VMs) for on-premises or IaaS environments. Start with an all-in-one solution or scale up to a highly distributed model across multiple network segments and geographies.

Furthermore, the solution enables integration with cloud services, such as Amazon Web Services (AWS), Microsoft Azure, SalesForce.com, Office 365, and IBM Cloud™, helping analysts better detect and respond to threats regardless of where they occur.

The QRadar platform enables integration with cloud services, including:

- AWS
- Azure
- SalesForce.com
- Office 365
- IBM Cloud™

Uses the MITRE ATT&CK framework

Organizations around the world are adopting the MITRE ATT&CK framework and use it as a foundation for the development of specific threat models and methodologies in the private sector, government, and cybersecurity. MITRE is a nonprofit organization that has developed the model after years of observing how real-world adversary groups operate.

The QRadar SIEM software enables integration with IBM QRadar Advisor with Watson, which automatically maps MITRE ATT&CK tactics and techniques to enrich the incident by providing firsthand information about the tactics and stages of an attack potentially being used by a threat actor. This process significantly reduces investigation time since analysts get an immediate understanding of which tactics are being deployed by bad actors, which, in turn, speeds up response and containment of threats. Shorter dwell times also lower the costs of security breaches.

IBM QRadar Use Case Manager packages the Cyber Adversary Framework Mapping Application to override default mappings and map your custom rules to MITRE ATT&CK tactics and techniques. By gaining the ability to visualize threat coverage across the MITRE ATT&CK framework, security analysts aren't only able to detect threats based on adversary behavior, but they can also proactively identify gaps and areas of inadequate security coverage, view predefined tactic and technique mappings, and add their own custom mappings to improve security coverage.

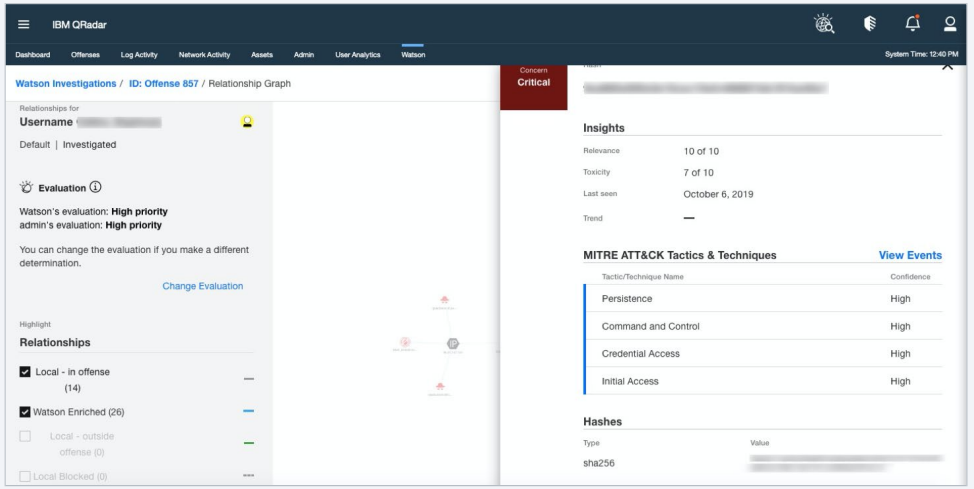


Figure 4: The QRadar Advisor with Watson app automatically maps MITRE ATT&CK tactics and techniques to Custom Rules Engine (CRE).

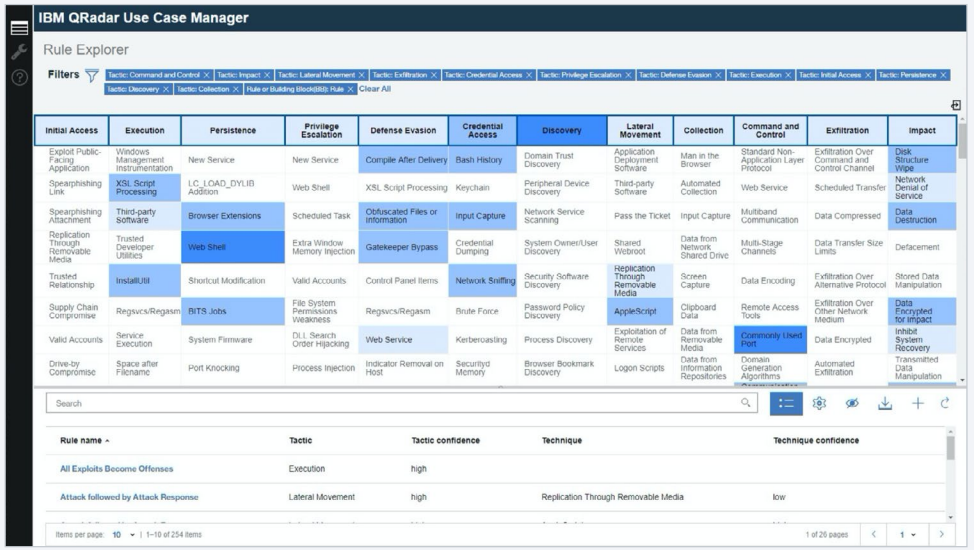


Figure 5: QRadar Use Case Manager

Solves skills gap with AI

IBM QRadar Advisor with Watson helps analysts quickly gain deeper insights into offenses to make more informed decisions. The solution can tap into unstructured data and provide a visual knowledge graph that shows the full scope of the threat in the environment. These enriched insights help reduce the time spent on investigations and empower analysts to make faster and more informed decisions.

Empower your SOC team with QRadar Advisor with Watson →

"IBM QRadar Advisor with Watson is a real breakthrough for us and for our clients. Using Watson, our analysts are able to do things 50 percent faster than those without the Watson solution. By bringing together top-notch expertise from Sogeti and IBM, along with superior innovation, we are helping our clients improve and fortify their cyber security."

Vincent Laurens
Vice President and Cybersecurity Practice Executive, Sogeti Luxembourg

Read the case study →

Addresses compliance requirements

With prebuilt content, rules, and reports, QRadar SIEM provides the transparency and accountability needed to help organizations address industry compliance requirements. The solution provides out-of-the-box compliance packages for General Data Protection Regulation (GDPR), the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), ISO 27001, Payment Card Industry Data Security Standard (PCI DSS), and more. These packages are included with a QRadar SIEM license and available in the IBM Security App Exchange.

Get your organization compliance-ready →

75%
of organizations

say data privacy is a strategic imperative for them. Thanks to regulations like the GDPR, customers are more aware of their privacy rights.[4]

Boosts incident response with security orchestration

QRadar offers a seamless integration with the IBM Resilient Security Orchestration, Automation and Incident Response (SOAR) platform, which enables significant improvements to how your organization responds to cyberattacks by automating and orchestrating people, processes, and technology.

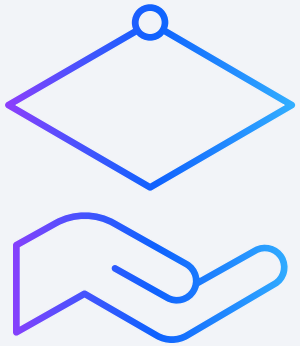
By combining the Resilient SOAR platform with an existing QRadar deployment, your security analysts can shorten the time to incident remediation by quickly and efficiently escalating suspected offenses from QRadar to Resilient, triggering additional automated enrichments and driving full investigation processes. As incidents evolve, all information is synchronized between QRadar and Resilient, helping ensure full data integrity and a continuous feedback loop to improve threat detection accuracy.

Explore IBM Security Resilient →

Helps maximize your security investments with the IBM Security App Exchange

Explore the IBM Security App Exchange and find over 200 validated apps, iintegrations, extensions and content packs from IBM and our partner ecosystem. Learn new use cases and integrations and extend your existing capabilities to better defend your enterprise.

Disocver new apps and extensions to enhance QRadar →



Migration process

There's no doubt that migrating to a next-generation SIEM solution can increase your SOC efficiency, help you better protect your organization, manage incidents, and meet compliance regulations.

Depending on your business requirements, your approach to migration will be different. Similarly, the timeline and milestones for the migration may be different, too. The simplest scenario is when an organization is retiring its traditional SIEM and moving to the IBM QRadar SIEM platform. Another scenario is when company A, which prefers a more modern SIEM platform, acquires company B and retires its old systems and deploys QRadar. In either of these scenarios, migration is the logical choice.

IBM Security recommends a three-step migration process for your organization to move to a next-generation SIEM solution. It's a phased approach that includes planning, migration and optimization processes, with each phase building on the previous one. The IBM Security team, with its decades of experience and best practices, provides the necessary guidance and expertise for each of these steps in the migration journey.

Instant switch to QRadar	**Migration strategy** to QRadar
Stand-up QRadar	
Cut over log sources	Feed from current SIEM to QRadar
Migrate rules, dashboards	
Retire current SIEM, maintain for compliance	Maintain current SIEM for limited reports
Small-medium-large deployment options	Expand insight with native capabilities
Follow-on expert consulting and **three-step migration →**	

Table 1: Two migration strategies

Now, let’s review the three-step migration process:

Assess and plan

Migrate

Optimize

Assess and plan

First things first—know your goals and plan. What are your business challenges? Are you planning the SIEM platform to be on premises, or in a public or hybrid cloud? Whatever may be the deployment model, the IBM QRadar team can work with your organization to launch the project and define requirements.

The deliverable of this planning stage is a QRadar migration plan that describes how QRadar is going to be configured and how the team will migrate existing historical event data if that's in the scope. The plan will also include what use cases, reports, apps, dashboards, and alerts will be implemented in QRadar once it's up and running.

The IBM team will lead your security team through a migration planning workshop or more, as required. This process will include reviewing and capturing business and technical requirements needed for the migration. Lastly, a migration plan will be created. Expertise is needed from both you and the IBM team as part of the review and capturing of requirements.

Here are some of the steps you can expect to work through:

Review the business requirements by assessing:

- Which existing use cases need to be replicated in QRadar
- Additional security intelligence use cases recommended by IBM or desired by the client
- Compliance and auditing reporting needs
- Reporting and dashboard requirements
- Vulnerability management systems
- Integration with incident response and ticketing tools
- Disaster recovery models
- Post-migration SIEM management
- QRadar skills development

Determine the technical requirements, such as:

- Detailed information on log and flow sources, including network hierarchy, device and application information
- Requirements for custom Universal Device Support Modules (uDSMs)
- How to cutover data collection from another SIEM to QRadar
- Network infrastructure considerations, such as firewalls and ports
- User roles and access
- Migration of existing historical event data

Prepare a migration plan that includes:

- Details of the business and technical requirements captured during the requirements gathering sessions
- Design and architectural diagrams
- Procedures required for the migration, including for migration of data and cutting over log sources
- Customization and integration requirements or recommendations, if any

Migrate

During this phase, the IBM specialists will deploy the QRadar solution and migrate data and configuration elements from the third-party SIEM. Tuning will help you isolate results to prioritized offenses so you can focus on what actually needs your attention. The final deliverable of this phase is an IBM QRadar Architecture and Deployment Guide, which will be delivered to the client team after the migration.

This activity includes the following tasks:

- Configure and test the QRadar appliances, VMs, cloud-based appliances or software nodes for this engagement using a detailed deployment checklist.
- Replicate configuration elements from the third-party SIEM to QRadar.
- Perform cutover log collection from the third-party SIEM to QRadar. A detailed procedure for this process will be established in the planning phase.
- Address issues with the ingestion and parsing of data.
- Create custom device support modules to parse log data from log sources not supported by the QRadar open-to-buy (OTB) application.
- Migrate existing historical event data to QRadar, if required.
- Configure data retention and backups.
- Verify event and flow collection from the existing deployment to new appliances.
- Verify deployment health and performance configurations.
- Finally, prepare a detailed QRadar Architecture and Deployment Guide that details all facets of the QRadar deployment.

Optimize

After the migration, rules and analytics will be customized to address the unique needs within your environment. The QRadar team will provide hands-on training and mentoring to enable your team to effectively support your new solution on an ongoing basis. This approach will run at a pace that'll be appropriate for individual customers, whether that's a "big bang" approach or a phased parallel approach.

As you work through these steps, you'll be able to turn off the old system and work on your new SIEM foundation, gradually evolving towards a new operating model. It's not uncommon for the IBM team to decide if any updates should be made to the QRadar Architecture and Deployment Guide.

If you haven't started working on your SIEM migration yet, don't wait any longer. As you can see, a SIEM migration can have significant challenges. However, by adopting a phased and strategic approach, as recommended by IBM Security, you should be able to smoothly transition to steady state.

Ultimately, by migrating to a next-generation SIEM platform, you're setting your organization on the path to success. The SIEM solution can help your security team's ability to proactively identify threats, defend against possible breaches and make your SOC more efficient.

This activity includes the following main steps:

Configure QRadar to support the documented business requirements. This process includes configuring:

- Custom rules and use cases
- Reports, alerts and dashboards
- Threat feeds
- QRadar apps, including, but not limited to, user behavior analytics, QRadar deployment intelligence and pulse.

Perform tuning to reduce white noise and false positives and enhance performance.

Integrate with incident response and ticketing tools.

Provide QRadar skills development to the required client resources.

Transition the steady-state solution to the client SOC team or managed service provider.

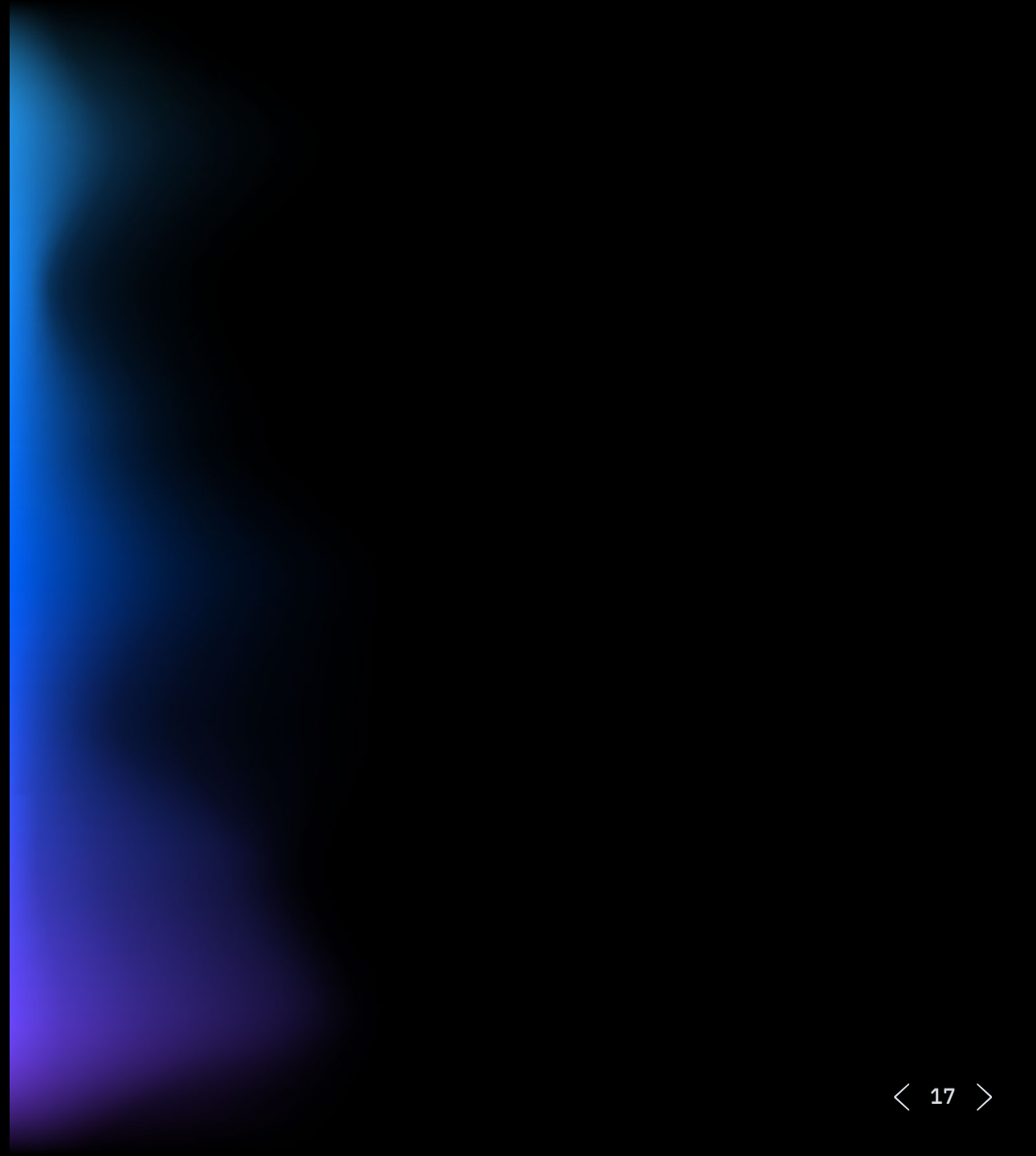
What’s next?

IBM QRadar can help you alleviate the pains caused by outdated solutions and address security issues no matter where you deploy applications—in an on-premises, hybrid, or SaaS model.

From gaining complete visibility into data to quickly detecting potential threats while addressing compliance, QRadar offers out-of-the box analytics, correlation rules and dashboards to help you stay ahead of the SIEM game.

Give your security team the right tools.

Upgrade to a next-generation SIEM platform. →



Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research, provides security intelligence to help organizations holistically protect their infrastructures, data and applications. It offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security, and more.

These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media, and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. IBM provides full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit ibm.com/financing.

To learn more about IBM QRadar Security Intelligence Platform in the cloud, please contact your IBM representative or IBM Business Partner, or visit ibm.com/software/products/en/qradar-on-cloud.

© Copyright IBM Corporation 2020

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2020

IBM, the IBM logo, ibm.com, IBM Cloud, IBM Security, QRadar, Watson, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Azure, and Office 365 are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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.

1 Jon Oltsik. "Big Changes Are Coming to Security Analytics and Operations." *Dark Reading*, December 11, 2019. www.darkreading.com/cloud/big-changes-are-coming-to-security-analytics-and-operations/a/d-id/1336565

2 "Cost of a Data Breach Report highlights." *IBM*. ibm.com/security/data-breach

3 "QRadar Security Intelligence Client Study." *Ponemon Institute*, December 2018. ibm.com/downloads/cas/M9YRMAKZ

4 "Data Privacy Is The New Strategic Priority." Forrester Opportunity Snapshot: A custom study commissioned by IBM, July 2019. ibm.com/account/reg/us-en/signup?formid=urx-39964

WGW03245-USEN-01