```
WEBVTT

00:01.033 --> 00:05.433
In this QRadar architecture video,
I will explain what this product is comprised of,

00:05.433 --> 00:09.500
its different components and how it should
be deployed in your network environment.

00:10.433 --> 00:13.500
Understanding the architecture of the IBM
QRadar

00:13.533 --> 00:16.533
ecosystem is viable
for everyone in IT security

00:16.666 --> 00:20.233
who is concerned with solutions
in the overall security immune system.

00:20.700 --> 00:23.866
By learning how the central Security
Intelligence components

00:23.900 --> 00:28.533
are designed to take in and process log
events and flow data, you will be better

00:28.566 --> 00:31.533
equipped to holistically work
as a Security Analyst.

00:32.933 --> 00:36.033
We will begin by talking
about the challenges security teams

00:36.066 --> 00:40.233
currently have when facing the complexity
of modern IT architectures

00:40.366 --> 00:45.100
and how IBM solves this by streamlining
the workflow of the Security Analyst.

00:46.300 --> 00:50.900
We will then look at the functional
architecture level of QRadar and explain
```

00:50.933 --> 00:55.333
how it was designed as a modular security
intelligence solution from the ground up.

00:56.233 --> 01:00.933
Then, we will look at the extensibility
of this modular design and deployment pattern,

01:01.066 --> 01:04.833
followed by a close examination
of the component architecture

01:04.866 --> 01:08.533
so that you can understand
how data is ingested and processed.

01:09.433 --> 01:12.733
When you later examine bits
and pieces of a larger security

01:12.766 --> 01:16.233
incident investigation,
this architectural understanding

01:16.266 --> 01:20.433
can substantially enhance your capability
for a detailed and fast analysis.

01:23.333 --> 01:25.566
So let's
begin by introducing the challenges

01:25.633 --> 01:28.866
and talking about the deployment
architecture that addresses them.

01:31.433 --> 01:34.266
As organizations' architectures
have recently evolved

01:34.300 --> 01:38.966
and adapted rapidly to include
an increasing number of remote endpoints

01:39.033 --> 01:44.033
accessing cloud and SaaS services,
data is becoming more and more federated.

01:44.266 --> 01:48.166
This situation is leading

```
to threat vectors increasing exponentially

01:48.233 --> 01:52.566
because the networks have extended beyond
the traditional boundaries, which poses

01:52.633 --> 01:56.533
a greater risk due to the increasing
complexity of advanced threats.

01:57.233 --> 02:00.666
Driven by these changes,
security teams have incorporated

02:00.700 --> 02:03.666
more and more technologies
to keep track of the threats.

02:04.266 --> 02:08.266
However, data and security tools are often
siloed and disjointed,

02:08.633 --> 02:10.566
making it difficult for security teams

02:10.566 --> 02:13.333
to fully understand incidents
in a timely manner.

02:14.366 --> 02:19.033
This compartmentalization of tools leads
to increased manual work, pivoting from

02:19.066 --> 02:22.966
one system to the next checking incidents
and integrating tasks manually.

02:23.766 --> 02:27.133
Due to the manual nature
and lack of consolidation of incidents

02:27.166 --> 02:30.500
from different tools,
security analysts are often missing

02:30.533 --> 02:34.033
the big picture and are not able to detect
complex attacks.

02:34.066 --> 02:35.700
```

```
In addition, too many alerts

02:35.700 --> 02:39.500
introduce noise that can obfuscate
real threats, resulting in analysts

02:39.533 --> 02:43.300
being overloaded most of the time,
detecting and triaging attacks,

02:43.433 --> 02:46.366
when they should rather be responding
to them in a timely manner.

02:46.733 --> 02:50.066
With this increased volume of threats
and the additional challenge

02:50.100 --> 02:52.700
of unexperienced team members
in most cases,

02:52.933 --> 02:55.966
security teams often
feel overwhelmed and burnt out.

02:56.366 --> 02:59.700
How can an organization
conceptually approach these challenges?

03:02.333 --> 03:03.700
To address these challenges,

03:03.733 --> 03:07.833
you want to focus on three main goals
by modernizing the threat detection

03:07.866 --> 03:10.433
and response principles
in your organization.

03:10.933 --> 03:12.066
Although security tools

03:12.066 --> 03:15.533
continue to be numerous
and spread through your IT infrastructure,

03:15.900 --> 03:19.733
they can be better leveraged to reduce
```

or even eliminate silos.

03:20.466 --> 03:23.333
In addition,
you want to establish a common workflow

03:23.366 --> 03:27.866
for threat hunting investigation and alert
response, which no longer requires

03:27.900 --> 03:30.166
your security analysts
to pivot between tools.

03:31.300 --> 03:35.166
Ultimately, such an improved workflow
can help connect tools

03:35.233 --> 03:39.433
to gain more visibility and reduce
workloads on the security analysts.

03:40.466 --> 03:43.300
Finally,
most of the workload can be alleviated

03:43.333 --> 03:48.100
by automating both repetitive and complex
tasks, such as bringing together

03:48.133 --> 03:52.666
data from a variety of sources,
triaging incidents and analyzing them.

03:53.900 --> 03:58.466
Let's take a moment and depict this dilemma
from the viewpoint of the security analysts.

04:01.266 --> 04:04.800
To address the challenges for the
security analysts discussed so far,

04:05.366 --> 04:11.533
IBM wants to achieve a simplified and streamlined workflow
that focuses on automating investigation

04:11.533 --> 04:16.700
and response actions to reduce manual efforts
and avoid pivoting between security tools.

```
04:17.600 --> 04:22.333
This solution leverages detection and response
workflows across all security tools

04:22.333 --> 04:25.066
by gathering their insights into a single workflow.

04:25.700 --> 04:29.900
The greatest advantages of this
is that you can integrate all your security tools,

04:29.900 --> 04:33.833
regardless of vendor,
and reduce risk and time to close incidents.

04:34.500 --> 04:38.566
This solution is called
the Unified Analyst Experience (UAX),

04:38.633 --> 04:42.233
which is part of the overall IBM Security QRadar Suite.

04:44.266 --> 04:48.600
To streamline the workflow of a security analyst
at the same time as reducing risk,

04:48.600 --> 04:51.400
IBM Security offers the QRadar Suite.

04:52.033 --> 04:56.866
This offering contains a set of components
for your organization that helps you integrate

04:56.866 --> 05:01.133
both IBM and third-party detection
and response tools into a single console.

05:01.700 --> 05:06.533
The QRadar Suite provides
many automatization tools utilizing its AI capability

05:06.533 --> 05:13.000
to help your analysts to act against real threats, minimize their
impact, and secure your assets.

05:13.100 --> 05:16.733
The overall QRadar
Suite offering is comprised of the following pillars:

05:18.200 --> 05:20.833
```

ASM (Attack Surface Management):

```
05:20.900 --> 05:24.800
It is important to begin by understanding
your potential attack surface.

05:24.800 --> 05:29.400
An ASM solution continuously identifies
external facing assets

05:29.400 --> 05:33.700
that are visible to attackers and prioritizes
high-risk exposures.

05:34.333 --> 05:39.866
Attack Surface Management helps organizations test their defenses and
incident response teams

05:39.866 --> 05:41.466
from the attackers’ perspective.

05:41.500 --> 05:46.133
It is based on the principle of continuous improvement,
learning and adapting

05:46.133 --> 05:49.966
with every new target discovered and each new attack runbook
developed.

05:50.433 --> 05:52.933
The IBM solution here is Randori.

05:54.533 --> 06:00.733
EDR (Endpoint Detection and Response): detects and stops
evasion attempts and advanced persistent threats,

06:00.733 --> 06:06.100
such as ransomware, at the endpoint in near-real time
with intelligent automation and AI,

06:06.333 --> 06:10.400
attack visualization storyboards,
and automated alert management.

06:10.666 --> 06:13.433
It can do this both online or offline.

06:13.433 --> 06:18.033
The IBM solution here is QRadar EDR,
formerly known as ReaQta.
```

```
06:20.100 --> 06:23.600
Log Insights: a cost-effective tool that helps you gain

06:23.600 --> 06:29.600
complete visibility with cloud scale log
ingestion, rapid search, powerful visualization

06:29.600 --> 06:34.933
and federated threat hunting and collaboration
without the need of a real-time correlation of logs,

06:35.200 --> 06:39.433
nor the overhead of a fully equipped threat detection
and response tool.

06:39.433 --> 06:42.966
The IBM solution here is QRadar Log Insights.

06:43.666 --> 06:47.700
SIEM (Security information and event management):

06:47.800 --> 06:50.766
aggregates log data and network traffic information

06:50.766 --> 06:55.600
from different sources in your network
or cloud infrastructure and correlates it

06:55.633 --> 07:01.166
to raise security alerts in near real-time
by using preconfigured or customized rules.

07:01.800 --> 07:05.000
With the aid of advanced insights
from machine learning capabilities,

07:05.200 --> 07:07.800
it can provide insights into suspicious activity.

07:07.800 --> 07:14.400
Also, an SIEM provides long-term storage of data
for greater correlation and compliance requirements,

07:14.400 --> 07:18.433
being able to generate timely reports
on any type of activity.

07:19.300 --> 07:22.533
It provides native user behavior analytics (UBA),
```

07:22.633 --> 07:27.533
hundreds of pre-built integrations
and use cases, and built-in MITRE ATT&CK mapping.

07:28.066 --> 07:33.333
The IBM solution here is QRadar SIEM with its variety of applications
and add-ons.

07:35.133 --> 07:38.466
SOAR (Security Orchestration, Automation and Response):

07:39.133 --> 07:43.866
automates the investigation of security incidents,
following the MITRE ATT&CK framework,

07:44.000 --> 07:49.400
to determine their criticality, escalation
procedures, and assigning ownership to resolve them.

07:50.000 --> 07:54.900
A SOAR solution helps solve incidents
and, therefore, block or remediate attackers faster.

07:55.233 --> 07:59.300
It also helps align teams and accelerate response
and recovery times.

07:59.733 --> 08:02.900
The IBM solution here is QRadar SOAR.

08:02.900 --> 08:07.666
Because organizations do not usually use
all security tools from the same vendor,

08:07.900 --> 08:13.000
the QRadar Suite takes an open approach
with Federated Access to give you flexibility.

08:13.866 --> 08:19.333
The QRadar Suite provides a strong ecosystem of integrations across
Threat Detection and Response,

08:19.333 --> 08:21.166
including third-party solutions.

08:21.733 --> 08:25.600
This can deliver significant time savings and value
from day one,

08:25.600 --> 08:31.833
because you can access and query data at its source location, and only
consolidate and import when necessary.

08:33.000 --> 08:40.366
Putting these pillars together, the QRadar Suite was architected
around a single, Unified Analyst Experience (UAX)

08:40.566 --> 08:44.400
that unifies capabilities across Security solutions
including EDR,

08:44.633 --> 08:48.233
log management, SIEM, and SOAR, as well as context

08:48.233 --> 08:52.033
and workflows across IBM QRadar and third-party solutions.

08:53.200 --> 08:58.866
It includes automated investigations, root cause analytics mitigation
recommendations,

08:58.866 --> 09:06.466
an AI driven alert disposition analysis that intelligently prioritizes
alerts and learns from analyst feedback,

09:06.466 --> 09:13.866
and federated search and investigation that enables analysts to
leverage data and insights from all their security tools.

09:14.366 --> 09:16.233
No matter where you are starting from,

09:16.233 --> 09:21.000
you can enhance your SOC maturity and capabilities with the QRadar
suite of products

09:21.000 --> 09:24.233
by adding what you need, when you need it, for added value.

09:24.766 --> 09:28.766
This results in accelerated threat detection
and response capabilities

09:28.766 --> 09:33.100
that you can gain with the integration
of multiple QRadar products over time.

09:33.800 --> 09:38.166
X-Force Threat Intelligence and Expertise

```
is inherent to all QRadar products,

09:38.166 --> 09:42.200
where it helps you gain accurate insights quickly by streamlining your
SOC

09:42.200 --> 09:45.000
with automated and intelligent detection and response.

09:45.700 --> 09:49.266
The QRadar Suite gives you complete visibility
into your entire environment.

09:50.766 --> 09:53.866
It collects data from endpoints, network devices,

09:54.100 --> 09:56.966
cloud environments, and even other data lakes,

09:56.966 --> 10:00.133
and it applies advanced analytics with alert consolidation

10:00.133 --> 10:03.766
and risk prioritization to highlight
your most critical threats.

10:04.600 --> 10:09.633
You can make quick and informed decisions
with attack visualization storyboards and leverage

10:09.633 --> 10:13.933
automated alert management and advanced continuous
learning AI capabilities.

10:14.566 --> 10:18.600
In addition, QRadar
Suite capabilities can automatically investigate

10:18.600 --> 10:23.066
threats with multi-stage analysis
to accurately triage incidents faster.

10:23.833 --> 10:27.366
The IBM global threat intelligence with
automated threat hunting

10:27.366 --> 10:31.300
provides deep search capabilities
so you can proactively hunt threats.
```

```
10:31.300 --> 10:33.433
With the help of AI and automation,

10:33.433 --> 10:38.866
you can bridge the skills gap by automating artifact
correlation, investigation,

10:38.866 --> 10:43.766
and case prioritization even before someone
begins investigating an open case.

10:43.833 --> 10:49.066
For the remainder of this course,
we will focus on the QRadar SIEM architecture details.

10:51.566 --> 10:53.466
QRadar SIEM use cases

10:53.500 --> 10:57.600
include Advanced Threat Detection
as well as Insider Threat Detection

10:57.666 --> 11:01.333
using the User Behavior
Analytics app (UBA).

11:01.366 --> 11:07.200
QRadar SIEM can help you better analyze
risk across your QRadar SIEM deployment

11:07.200 --> 11:10.700
and manage vulnerabilities
for all your deployed IT assets.

11:11.900 --> 11:15.133
QRadar SIEM can assist you
with your compliance posture

11:15.300 --> 11:18.400
by supporting many standardized reports
and guidelines.

11:20.000 --> 11:23.533
Cloud Security assets
can be tied into your QRadar SIEM

11:23.566 --> 11:27.200
deployment just as any other on-premises
infrastructure.
```

```
11:27.766 --> 11:32.400
Finally, QRadar SIEM can be integrated
with Incident Response systems.

11:33.600 --> 11:38.466
You can add content packs and additional
applications (from either IBM or third parties)

11:38.466 --> 11:42.466
to enhance QRadar from the IBM Security App Exchange.

11:43.933 --> 11:48.266
The QRadar Analytics engine,
including User Behavior Analytics,

11:48.266 --> 11:53.166
uses machine learning and provides real-time
detection and user-driven analytics.

11:54.100 --> 11:57.766
Powerful search capabilities
can be enhanced by using artificial

11:57.800 --> 12:02.333
intelligence for your investigations
based on the QRadar Advisor with Watson.

12:03.333 --> 12:06.566
QRadar SIEM
allows unlimited and tamper-proof

12:06.600 --> 12:08.966
logging from a wide variety of sources.

12:10.566 --> 12:13.766
You can deploy QRadar SIEM
in a variety of ways:

12:14.200 --> 12:19.000
on premises, as a service, in the cloud,
and in a hybrid deployment.

12:19.900 --> 12:24.266
In addition, QRadar SIEM can be used in
multi-tenant environments,

12:24.300 --> 12:28.100
allowing Managed Security Service
Providers (MSSPs)
```

12:28.133 --> 12:31.966
or multidivisional organizations
to provide security services

12:32.000 --> 12:36.366
to multiple client organizations
from a single, shared, QRadar deployment.

12:37.166 --> 12:39.266
For example, as an MSSP,

12:39.300 --> 12:43.466
you might host 20 clients
on a single instance of QRadar SIEM,

12:43.600 --> 12:47.333
where each client manages
approximately 1000 employees.

12:47.733 --> 12:51.900
You don't have to deploy unique QRadar
SIEM instances for each customer.

12:52.600 --> 12:55.900
For this course,
we focus on a QRadar SIEM deployment

12:55.933 --> 12:58.766
that revolves around a single customer
environment.

12:59.366 --> 13:01.733
Let's explore
the various deployment models.

13:03.466 --> 13:07.100
No matter how many
QRadar SIEM applications are leveraged,

13:07.166 --> 13:09.833
or how many appliances constitute
a deployment,

13:10.166 --> 13:13.800
all capabilities are leveraged
through a single, web-based console,

13:13.966 --> 13:17.633
with all the associated benefits
that a common interface delivers

```
13:17.766 --> 13:22.266
in terms of speed of operation,
transference of skills, ease of adoption,

13:22.433 --> 13:24.466
and a universal learning curve.

13:25.833 --> 13:29.766
Among the benefits you will learn later,
you will notice that the console provides

13:29.800 --> 13:34.033
full visibility and actionable insight
to protect against advanced threats.

13:34.966 --> 13:39.200
It also adds network flow capture
and analysis for deep application insight,

13:39.466 --> 13:44.066
it employs sophisticated
correlation of events, flows, assets,

13:44.100 --> 13:49.366
topologies, vulnerabilities, and external
data to identify and prioritize threats;

13:50.200 --> 13:54.266
it contains workflow management to fully
track threats and ensure resolution,

13:54.566 --> 13:58.200
and it uses a scalable
hardware, software and virtual appliance

13:58.233 --> 14:02.800
architecture, including cloud integrations
to support the largest deployments.

14:04.066 --> 14:09.166
The QRadar SIEM Console is the central interface
for all analyst-related tasks.

14:09.900 --> 14:12.033
As a QRadar SIEM analyst,

14:12.033 --> 14:15.900
you can switch from log events
to network flows to risk and compliance
```

```
14:15.966 --> 14:19.966
policy reports and prioritized lists
of network-wide vulnerabilities

14:20.200 --> 14:23.966
and perform analysis of incidents
after an offense has been raised.

14:25.166 --> 14:27.800
This allows an organization
to reduce the time before

14:27.833 --> 14:31.233
an initial breach is detected
and avoid the actual exploit.

14:32.633 --> 14:35.400
The Console provides
numerous tabs that allow insight

14:35.433 --> 14:38.766
into different views
of the collected and correlated data.

14:39.666 --> 14:43.166
This is the Dashboard tab,
which allows an organization to define

14:43.200 --> 14:46.266
many different views
into the collected and processed data.

14:47.233 --> 14:50.666
QRadar SIEM
provides a set of predefined dashboards

14:50.833 --> 14:53.300
but you can create and maintain your own.

14:53.366 --> 14:55.866
You can do the following with each different tab:

14:56.200 --> 15:00.500
Use the Offenses tab to view all the offenses
that occur in your IT environment.

15:00.833 --> 15:03.633
You can investigate offenses, source
and destination,
```

15:03.666 --> 15:06.666
IP addresses, network
behaviors, and anomalies.

15:07.433 --> 15:10.266
The Log Activity tab displays
event information

15:10.300 --> 15:14.566
as records from a log source,
such as a firewall or router device.

15:15.233 --> 15:19.433
Here, you can specifically investigate
event data and monitor log activity.

15:20.200 --> 15:24.100
The Network Activity tab displays
information about network communication.

15:24.433 --> 15:25.833
You can investigate the flows

15:25.833 --> 15:29.566
that are captured by QRadar SIEM
in real time and monitor

15:29.600 --> 15:33.300
the network activity
by using configurable time-series charts,

15:33.433 --> 15:36.866
but only if the content capture option
is enabled in your installation.

15:37.366 --> 15:41.600
This is a feature in QRadar SIEM that
allows the collection of network flows.

15:42.400 --> 15:47.166
Next, in the Assets tab, you can search
and view the assets in your IT environment.

15:47.700 --> 15:51.600
QRadar SIEM automatically discovers
and creates asset profiles

15:51.766 --> 15:55.300
by using passive flow data

```
and vulnerability data.

15:55.733 --> 16:00.866
Asset profiles store a multitude of information
for each known asset in your network,

16:00.866 --> 16:03.900
including running services and vulnerability information.

16:04.366 --> 16:08.700
Asset profile information can be used
for correlation purposes, where it helps

16:08.766 --> 16:12.833
to reduce false positives and provide
more details for investigations.

16:13.700 --> 16:18.600
The asset profiles are also very important
when you manage IT vulnerabilities.

16:18.866 --> 16:22.366
You can even tune false positives
directly from the Asset tab.

16:23.366 --> 16:26.566
Next to the assets,
you can use the Reports tab to create,

16:26.666 --> 16:30.233
distribute, and manage reports for QRadar
SIEM data.

16:30.700 --> 16:34.766
There are different kinds,
such as compliance, device, executive,

16:34.800 --> 16:38.766
and network reports; which are available
in pre-installed templates.

16:39.466 --> 16:44.833
You can also create customized reports
and there are various formats available for exporting them.

16:45.233 --> 16:48.233
Continuing,
we have the Vulnerability and Risk tabs,

16:48.400 --> 16:52.866
```

which can only be accessed
if you deploy a QRadar Vulnerability Manager

16:52.866 --> 16:55.266
and Risk Manager license
in your environment.

16:55.900 --> 17:00.100
QRadar Vulnerability Manager can ingest
and manage vulnerability data

17:00.166 --> 17:03.833
from third party vulnerability scanners,
which is then available

17:03.866 --> 17:08.100
for more detailed threat investigations
as well as vulnerability reporting.

17:08.166 --> 17:13.566
QRadar Risk Manager monitors device
configurations, simulating changes to your

17:13.600 --> 17:18.500
network environment, and prioritizes
risks and vulnerabilities in your network.

17:19.400 --> 17:22.266
Additionally,
there's the Admin menu, which provides

17:22.300 --> 17:26.000
all tools to manage and maintain
the QRadar SIEM deployment.

17:26.500 --> 17:29.400
Analysts typically
do not have access to these tools.

17:30.166 --> 17:34.800
Finally, the Security icon takes you
to the QRadar Assistant App menu,

17:34.900 --> 17:38.233
where you can manage your app and content
extension inventory,

17:38.500 --> 17:41.266
view app and content
extension recommendations,

```
17:41.466 --> 17:45.433
and get links to useful information
to maintain your QRadar SIEM

17:45.466 --> 17:48.600
deployment up to date, healthy,
and running smoothly.

17:49.366 --> 17:53.500
After you add additional capabilities
to your QRadar SIEM deployment,

17:53.600 --> 17:58.400
such as Incident Forensics, User Behavior
Analytics, Use Case Manager or third

17:58.433 --> 18:02.966
party apps, they will be accessible
via their own tabs here in the Console.

18:05.400 --> 18:06.466
QRadar SIEM

18:06.466 --> 18:10.400
can analyze large amounts of data
and uses context to transform it

18:10.433 --> 18:13.633
into useful, actionable information
as is shown here.

18:14.366 --> 18:17.233
This is what you can see
as a security analyst when you begin

18:17.266 --> 18:21.466
to investigate an offense record
that was triggered by a correlation rule.

18:22.633 --> 18:26.666
You can quickly investigate the who, what,
and where behind an offense;

18:27.000 --> 18:30.266
determine if it is a legitimate threat
or a false positive;

18:30.500 --> 18:33.366
and find out details
```

about the evidence of the attack.

18:34.300 --> 18:38.766
QRadar SIEM provides strong event
management and analysis capabilities

18:38.966 --> 18:43.566
and is very effective in detecting threats
because it can leverage a broad range

18:43.600 --> 18:48.366
of data, analyze it, and apply context
from an extensive range of sources.

18:49.300 --> 18:54.066
This helps to reduce false positives,
report on actual exploits, and show

18:54.100 --> 18:57.800
what kind of activity is taking place
within your IT environment.

18:58.433 --> 19:01.400
This can result in faster
threat detection and response

19:01.433 --> 19:06.000
because QRadar SIEM continuously monitors
data sources across the

19:06.033 --> 19:10.400
IT infrastructure, leveraging the context
in which systems are operating.

19:11.400 --> 19:12.600
That context includes

19:12.600 --> 19:17.200
security and network device logs,
vulnerabilities, configuration data,

19:17.400 --> 19:21.266
network traffic telemetry,
cloud environment log source data,

19:21.600 --> 19:26.600
application events and activities, user
identities, asset information,

19:26.900 --> 19:29.366

```
geolocation and application content.

19:30.500 --> 19:33.200
This activity generates
a staggering amount of data,

19:33.366 --> 19:38.400
which makes the automation in QRadar SIEM
very important, because it can correlate

19:38.433 --> 19:42.566
this large amount of data down
to a small number of actionable offenses.

19:43.200 --> 19:47.366
And with this broad amount of data,
it detects equally broad types of threats.

19:48.000 --> 19:52.466
QRadar SIEM leverages this data
to establish a very specific context

19:52.500 --> 19:56.900
around each potential area of concern
and uses sophisticated analytics

19:56.966 --> 20:00.033
to accurately detect
more and different types of threats.

20:00.600 --> 20:01.466
For example,

20:01.500 --> 20:05.833
a potential exploit of a web server
reported by an intrusion detection system

20:06.000 --> 20:11.200
can be validated by unusual outbound
network activity detected by QRadar SIEM.

20:11.233 --> 20:15.866
QRadar SIEM uses intelligence, automation
and analytics

20:16.100 --> 20:18.700
to provide
actionable security information,

20:18.766 --> 20:23.066
```

including the number of targets
involved in a threat, who was responsible,

20:23.166 --> 20:28.066
what kind of attack occurred, where it is
located, whether it was successful,

20:28.466 --> 20:32.033
vulnerabilities, evidence
for forensics and so on.

20:33.633 --> 20:36.700
In addition to the conventional QRadar
console UI,

20:37.066 --> 20:42.800
starting with v7.4, QRadar
SIEM includes the Analyst Workflow app,

20:42.900 --> 20:45.466
which provides a modern experience
for analysts.

20:46.200 --> 20:50.466
The app's UI is based on the IBM Design
methodology principles,

20:50.500 --> 20:54.000
which aim for a more intuitive
and concise user experience.

20:54.466 --> 20:58.233
These IBM Design principles are applied
to many IBM products.

20:59.200 --> 21:04.000
The Analyst Workflow app provides new
methods for filtering offenses and events,

21:04.400 --> 21:08.833
and graphical representations of offenses
by magnitude, assignee and type.

21:09.833 --> 21:12.266
It provides an improved workflow
for offenses,

21:12.300 --> 21:15.900
which enables a more intuitive method
to investigate an offense

21:15.966 --> 21:19.566
to determine the root cause of an issue
and work to resolve it.

21:20.166 --> 21:25.100
You can use a built-in query builder
to create AQL queries by using examples

21:25.166 --> 21:30.033
and saved or shared searches, or by typing
plain text into the search field.

21:30.700 --> 21:33.466
The latter
method provides a type-ahead experience

21:33.500 --> 21:38.266
to make searching for common
indicators of compromise (IOC) easy

21:38.300 --> 21:41.800
and customizable
by using the AQL query language.

21:42.400 --> 21:44.633
You can filter offenses in various ways.

21:46.600 --> 21:47.233
We just saw

21:47.233 --> 21:50.300
what a typical security
analyst can see after QRadar

21:50.400 --> 21:54.400
SIEM has analyzed large amounts of data
and contextual information

21:54.433 --> 21:58.233
to transform this data
into useful, actionable information.

21:59.266 --> 22:00.033
It is important

22:00.033 --> 22:03.966
to understand the functional context
and where all this data is coming from.

22:05.033 --> 22:07.433
First, there is point in time.

22:07.466 --> 22:12.466
Everything that QRadar SIEM investigates
is based on an exact point in time.

22:12.800 --> 22:15.866
This timestamp
allows QRadar SIEM to correlate

22:16.000 --> 22:19.766
the most complex relationships
between disparate log sources

22:19.800 --> 22:23.166
and network flows
to present them as one connected offense.

22:23.966 --> 22:25.966
Second, there are the offending users.

22:26.400 --> 22:29.833
QRadar extracts user information
wherever possible,

22:29.866 --> 22:33.300
allowing an analyst to further investigate
individual users.

22:33.833 --> 22:37.600
It also uses this information
for user behavioral analytics.

22:38.066 --> 22:39.766
Next, there are the origins.

22:39.800 --> 22:43.700
This represents the starting point
for all QRadar SIEM correlation

22:43.766 --> 22:46.300
activity and is captured as an IP address.

22:47.100 --> 22:51.666
Similarly, the targets represent
the final point for all QRadar SIEM

22:51.700 --> 22:55.466
correlation activity, and those are also

captured as an IP address.

22:55.800 --> 22:59.500
QRadar SIEM maintains
a centralized asset database

22:59.566 --> 23:03.633
that is used to record
a variety of details for each asset

23:03.666 --> 23:07.366
that has been discovered
and they can be discovered in two ways:

23:07.833 --> 23:11.666
actively, by using third-party
vulnerability scans that can be managed

23:11.700 --> 23:16.300
with QRadar Vulnerability Manager,
or passively through network flows.

23:16.366 --> 23:20.800
Asset data can also be imported
by using other enterprise

23:20.833 --> 23:22.700
tools for asset management.

23:22.766 --> 23:25.600
Details of these assets
can include IP address,

23:25.866 --> 23:30.100
hostname, active applications
and services, as well as vulnerabilities.

23:31.166 --> 23:32.366
Speaking of which,

23:32.400 --> 23:36.233
QRadar SIEM maintains
a list of vulnerabilities for each asset.

23:36.966 --> 23:39.800
These can be discovered
by using third-party vulnerability

23:39.833 --> 23:43.666
management solutions and managed by QRadar

Vulnerability Manager.

23:43.700 --> 23:48.766
Asset related vulnerabilities are used
for QRadar correlations and analytics,

23:48.900 --> 23:53.166
and they can influence several factors
throughout the offense management process.

23:54.400 --> 23:56.600
Then there are the known threats.

23:56.633 --> 23:59.700
QRadar SIEM
can connect to external threat feeds

23:59.866 --> 24:02.100
such as the IBM X-Force Exchange.

24:03.100 --> 24:06.766
This threat information
can also be used for QRadar SIEM

24:06.800 --> 24:10.766
correlations and analytics to influence
the incident management process.

24:11.566 --> 24:15.700
There is also something called Behavioral
and network threat analytics.

24:15.766 --> 24:19.300
Utilizing some of the above-mentioned data
in combination

24:19.366 --> 24:24.366
with other enterprise-wide collected
information, QRadar SIEM can analyze

24:24.400 --> 24:28.766
user or network traffic behavior to alert
whenever abnormal activity

24:28.800 --> 24:30.633
has been detected.

24:30.666 --> 24:33.566
And finally,
after all this data has been correlated,

24:33.600 --> 24:37.600
it is presented to the analysts
in the QRadar SIEM console.

24:38.166 --> 24:40.766
If a particularly important threat
is discovered,

24:41.000 --> 24:44.900
an analyst must investigate it
with utmost urgency.

24:44.966 --> 24:50.233
To support this task, QRadar SIEM now
provides Cognitive Analytics.

24:50.866 --> 24:54.233
This capability augments
security analyst's ability

24:54.266 --> 24:57.233
to identify and understand
sophisticated threats

24:57.433 --> 25:01.033
by tapping into unstructured data
such as blogs, websites,

25:01.066 --> 25:05.366
and research papers; and correlating it
with local security offenses.

25:07.000 --> 25:08.466
Now, while the

25:08.500 --> 25:11.033
log events are critical,
they can leave gaps in visibility.

25:11.466 --> 25:16.200
This is because, when attackers compromise
an IT system, they first try to turn off

25:16.400 --> 25:20.000
logging or manipulate local log files
to obfuscate their tracks.

25:20.666 --> 25:23.466
Traditional SIEMs are blind at this point.

25:23.866 --> 25:26.500
However, no
attacker can disable the network

25:26.766 --> 25:28.866
or they cut themselves off as well.

25:28.900 --> 25:33.900
Network Flow Analytics in QRadar allows
deep packet inspection for OSI Layer 7

25:33.966 --> 25:38.566
flow data, which can contain very helpful
information for advanced forensics.

25:39.300 --> 25:42.300
Network flow information
helps to detect communication

25:42.366 --> 25:46.300
flow anomalies, zero-day attacks
that have no signature yet,

25:46.600 --> 25:49.900
and provides visibility into all attacker
communications.

25:50.666 --> 25:53.666
Using passive monitoring, flow
analytics builds up

25:53.700 --> 25:56.033
an asset database and profiles
your assets.

25:56.833 --> 26:00.266
For example, an IT system
that has responded to a connection

26:00.300 --> 26:04.066
on port 53 UDP is obviously a DNS server.

26:04.600 --> 26:07.866
Another IT system
that has accepted connections on ports

26:07.900 --> 26:11.366
139 or 445 TCP is a Windows Server.

```
26:11.966 --> 26:14.566
Adding
application detection can confirm this

26:14.766 --> 26:18.600
not only at a port level,
but the application data level as well.

26:19.233 --> 26:22.466
Lastly, this feature provides
you with better network visibility

26:22.633 --> 26:25.066
and thus helps
you resolve traffic problems.

26:25.833 --> 26:29.566
Besides this native flow
analytics capability that QRadar offers,

26:29.900 --> 26:34.566
there is also the QRadar Network Threat
Analytics app that continuously monitors

26:34.600 --> 26:38.400
the flow records in your network
to identify anomalous traffic.

26:39.233 --> 26:42.800
The dashboard provides
visualizations to show which flow records

26:42.833 --> 26:46.600
deviate the most from other flow records
that are typically observed

26:46.633 --> 26:48.100
on your network.

26:48.233 --> 26:51.100
The visualizations
can help you quickly identify

26:51.233 --> 26:52.666
which flows might indicate

26:52.666 --> 26:56.766
suspicious behavior on your network
and prioritize your investigations.
```

26:58.833 --> 27:05.200
Now, let's talk about three very important characteristics
of the QRadar SIEM Extensible Functional Architecture.

27:06.700 --> 27:09.766
This functional architecture
is extensible by design.

27:10.266 --> 27:14.233
This means that the framework allows you
to add additional functionalities

27:14.266 --> 27:17.433
as needed in an organization.

27:17.466 --> 27:20.066
First,
let's talk about cognitive analytics.

27:21.000 --> 27:25.300
Security analysts today are more
and more overwhelmed by the amount of data

27:25.366 --> 27:29.500
that requires investigation,
and by the mounting time pressure to act.

27:30.033 --> 27:32.700
The more data
that there is, the more difficult

27:32.766 --> 27:35.466
and the longer
it takes to analyze security risks.

27:36.233 --> 27:38.866
One way to provide
cognitive analytics to QRadar

27:38.900 --> 27:42.166
SIEM is by analyzing the user's behavior.

27:42.900 --> 27:47.766
The QRadar User Behavior Analytics app
uses existing data in your QRadar

27:47.900 --> 27:51.100
SIEM to generate
new insights around users.

```
27:51.600 --> 27:55.866
It helps you determine the risk profiles
of these users inside your network

27:55.900 --> 27:59.366
and to act when the app alerts you
to threatening behavior.

28:00.066 --> 28:02.833
Not only you can determine
the risk profile of users,

28:03.200 --> 28:05.866
but with the addition of Machine Learning,
you can gain

28:05.900 --> 28:09.800
additional insights into user behavior
with predictive modeling.

28:10.400 --> 28:14.066
Machine Learning can help your system gain
insights into the expected

28:14.100 --> 28:17.600
behavior of the users in your network
and generate offenses

28:17.633 --> 28:21.266
based on any observed deviation
from established baselines.

28:22.166 --> 28:25.166
And machine learning
is not only present in the UBA app,

28:25.433 --> 28:29.766
but it also plays a major role in how
the Network Threat Analytics app works.

28:30.366 --> 28:33.633
This app continuously monitors
the flow records in your network

28:33.666 --> 28:36.766
to show which of these deviate
the most from other records

28:36.800 --> 28:38.800
that are typically observed
```

on your network.

28:38.833 --> 28:40.633
Alerting on anormalous traffic

28:40.666 --> 28:43.666
and, thus, helping
you prioritize your investigations.

28:44.466 --> 28:46.200
Cognitive analytics

28:46.233 --> 28:49.300
augments your analysts knowledge
and insights with QRadar Advisor

28:49.366 --> 28:53.100
with Watson to speed up analysis
with visuals, query,

28:53.166 --> 28:58.700
and auto-discovery across the platform
where you can inspect events, flows, users

28:58.800 --> 29:02.833
and more by tapping into unstructured data
and correlating it with

29:02.866 --> 29:04.200
local security offenses.

29:06.033 --> 29:09.066
"Digital everything"
means that technology's number one

29:09.100 --> 29:12.366
job in business
now is handling and responding to data.

29:13.200 --> 29:16.200
Cognitive capabilities are being applied
to security

29:16.233 --> 29:19.433
to establish a relationship
between machines and humans.

29:19.800 --> 29:23.666
The role of technology
can now change from enabler to advisor.

29:24.200 --> 29:28.166
We are ushering in this new era
of cognitive security to outthink

29:28.200 --> 29:32.966
and outpace threats with security
that understands reasons and learns.

29:33.566 --> 29:37.200
IBM Watson enables fast
and accurate analysis of security

29:37.233 --> 29:39.766
threats,
saving precious time and resources.

29:40.433 --> 29:43.033
This empowers
the analyst to perform faster

29:43.066 --> 29:46.166
investigations
and clear their backlog more easily.

29:46.700 --> 29:48.366
It will also help to increase

29:48.366 --> 29:51.766
the investigative skills
for individual analysts over time.

29:52.200 --> 29:56.233
With the help of IBM Watson, security
analysts will be able to spend

29:56.266 --> 30:01.066
less time on the mundane tasks of manual
and time-consuming threat analysis,

30:01.266 --> 30:02.700
and more time being human.

30:03.833 --> 30:05.966
Then there's the Open Ecosystem.

30:06.233 --> 30:10.300
The IBM Security App Exchange
provides access to apps from leading

```
30:10.366 --> 30:15.266
security partners and offers integrations
with many third party security products.

30:16.033 --> 30:21.633
QRadar SIEM provides open APIs to allow
for custom integrations and applications,

30:21.666 --> 30:25.166
which can be found at the IBM Security
App Exchange.

30:25.700 --> 30:28.433
As you may know,
today's attackers shared tools.

30:28.833 --> 30:32.066
They collaborate in creating malware
that is difficult to discover.

30:32.633 --> 30:36.600
On the defensive side, organizations
must deal with many siloed

30:36.633 --> 30:40.000
security solutions
from an equally large number of vendors.

30:40.566 --> 30:43.766
It is estimated that an average
organization can have up to

30:43.800 --> 30:46.500
85 security products from 40 vendors.

30:47.000 --> 30:47.833
With this mix,

30:47.866 --> 30:51.433
it is difficult to link the products
together so they can support each other.

30:51.966 --> 30:56.500
To fill this gap, IBM has introduced
the IBM Security App Exchange.

30:57.200 --> 31:00.833
The exchange is a marketplace
for the security community to create
```

31:00.866 --> 31:04.766
and share applications that integrate
with IBM's security solutions.

31:05.200 --> 31:08.033
The first offering
in which customers, business partners,

31:08.066 --> 31:12.300
and other developers can build
custom apps is QRadar SIEM.

31:13.200 --> 31:16.400
Releasing APIs and software
development kits for QRadar

31:16.433 --> 31:19.966
SIEM fosters the integration
with third-party technologies.

31:20.566 --> 31:23.033
This provides organizations
with better visibility

31:23.066 --> 31:27.700
into more types of data and offers new
automated search and reporting functions

31:27.766 --> 31:31.800
that can help security specialists
focus on the most pressing threats.

31:32.633 --> 31:36.600
Now, the IBM Security App
Exchange has a few customized apps

31:36.800 --> 31:40.666
that extend security analytics into areas
like user behavior,

31:40.900 --> 31:43.566
endpoint data, and incident visualization.

31:44.400 --> 31:45.500
Before releasing an app.

31:45.500 --> 31:49.033
IBM Security tests every application
very closely

31:49.066 --> 31:52.233
to ensure the integrity
of these community contributions.

31:53.066 --> 31:57.166
The app exchange categorizes
its apps by the type of service

31:57.200 --> 32:01.166
such as cloud, compliance, endpoints,
data, identity,

32:01.200 --> 32:05.566
malware, mobile, threat detection, system
management, and many more.

32:06.000 --> 32:10.033
You can filter by the content type,
so if you want to focus on applications,

32:10.066 --> 32:14.100
assets, connectors, dashboard
improvements, custom rules, content

32:14.166 --> 32:18.233
extensions, log sources, saved searches,
scripts,

32:18.566 --> 32:21.766
workflows, among others;
you can easily do that as well.

32:22.100 --> 32:23.200
You can even filter

32:23.200 --> 32:27.166
content on the App Exchange
based on the MITRE ATT&CK tactic types.

32:27.500 --> 32:30.566
Also, the App Exchange offers
the opportunity to produce

32:30.600 --> 32:38.366
apps for additional IBM security products such as Cloud Pak for
Security, SOAR, Gardium and MaaS360.

32:39.866 --> 32:43.266
Lastly, we have the Deep Threat Intelligence
and Analysis feature.

32:44.000 --> 32:48.500
You can further extend the QRadar SIEM
functionality with threat intelligence

32:48.566 --> 32:52.100
data and analytics functions from the IBM
X-Force Exchange,

32:52.266 --> 32:55.433
which is powered by IBM's X-Force
Research Team.

32:56.066 --> 33:01.300
All this data can be shared
with a collaborative portal using STIX/TAXII standards.

33:01.766 --> 33:05.500
According to the United Nations Office
on Drugs and Crime,

33:05.633 --> 33:12.166
up to 80% of cybercrime acts are estimated to originate
in some form of organized activity.

33:12.600 --> 33:16.200
One element that the offenders have
mastered is collaboration.

33:16.566 --> 33:20.000
They share tools to ensure
that their attacks can be successful.

33:20.466 --> 33:25.433
Not only that, but they share vulnerability,
targeting and countermeasure information.

33:25.700 --> 33:28.800
Collaboration is a force multiplier
for the hacking community.

33:29.400 --> 33:32.900
Furthermore, organizations
have been using threat intelligence

33:32.966 --> 33:36.833
to stay side by side of threats,
but these efforts are limited.

33:37.633 --> 33:40.000

```
To succeed requires much more information

33:40.100 --> 33:43.666
shared among security professionals,
researchers, and practitioners.

33:44.100 --> 33:48.466
Luckily, IBM has built a collaboration
platform called the X-Force Exchange

33:48.666 --> 33:51.966
to facilitate the collaboration
that will allow organizations

33:52.000 --> 33:55.000
to have a much greater
understanding of threats and actors.

33:55.666 --> 34:00.433
The IBM X-Force Exchange is a cloud-based
threat intelligence sharing platform

34:00.566 --> 34:05.366
that enables users to rapidly research
the latest global security threats,

34:05.400 --> 34:09.066
aggregate actionable intelligence,
consult with experts,

34:09.100 --> 34:11.266
and collaborate with peers.

34:11.300 --> 34:14.700
It provides timely,
curated threat intelligence insights,

34:14.766 --> 34:17.566
which adds context to machine-generated
data.

34:18.100 --> 34:21.600
The platform facilitates
making connections with industry peers

34:21.766 --> 34:24.866
to validate findings
and research threat indicators.

34:25.633 --> 34:29.233
```

Leveraging the open and powerful
infrastructure of the cloud,

34:29.233 --> 34:35.366
users can collaborate and tap into over 700 TB
of information from multiple data sources.

34:36.300 --> 34:38.866
This includes one of the largest
and most complete

34:38.900 --> 34:42.366
catalogs of vulnerabilities
in the world, threat Information

34:42.400 --> 34:46.200
based on more than 15 billion monitored
security events per day,

34:46.566 --> 34:51.500
and malware threat intelligence
from a network of 270 million endpoints.

34:51.900 --> 34:56.833
This threat information is based on over
25 billion web pages and images

34:56.866 --> 35:01.100
and deep intelligence on more than 8
million spam and phishing attacks.

35:01.900 --> 35:06.966
To leverage all this X-Force Intelligence
into your QRadar SIEM system, the QRadar

35:07.300 --> 35:08.266
Threat Intelligence

35:08.266 --> 35:12.166
app pulls in threat intelligence
feeds from the X-Force Exchange.

35:12.700 --> 35:16.000
You can then analyze these feeds
for potential global

35:16.033 --> 35:18.966
threats and attacks and plan remediation
actions.

35:19.600 --> 35:22.633
With this, you can create custom rules
for correlation,

35:22.666 --> 35:26.466
searching, and reporting
based on these indicators of compromise.

35:29.433 --> 35:34.700
QRadar SIEM is a modular architecture
that provides real time visibility of your

35:35.000 --> 35:38.833
IT infrastructure so that you can detect
and prioritize threats.

35:39.500 --> 35:44.333
Depending on your log and flow collection
quantities, your functional requirements,

35:44.633 --> 35:48.366
data storage estimations, high
availability and disaster

35:48.400 --> 35:52.233
recovery requirements,
organizational network topology

35:52.400 --> 35:55.600
and your analysis needs,
you can scale your QRadar

35:55.633 --> 35:59.500
SIEM deployment to a larger
and more complex structure as needed,

35:59.700 --> 36:03.533
or you can choose to distribute
it between local and remote environments.

36:04.700 --> 36:07.933
Let's see the different deployment options
that are available to you.

36:09.333 --> 36:14.233
Any QRadar SIEM deployment model
includes access to threat indicators

36:14.300 --> 36:18.400
from the X-Force Exchange and extensions

and apps from the App Exchange;

36:18.633 --> 36:21.766
plus all the functionalities discussed
so far in this course.

36:23.700 --> 36:26.366
The first option is to have
an on-premises installation.

36:27.533 --> 36:31.433
This on-premises installation involves
hardware and software that is installed

36:31.500 --> 36:35.233
at your organization's locations,
and includes the following features,

36:35.433 --> 36:40.733
which can reside in a single or multiple
physical appliances: The user interface,

36:40.766 --> 36:45.200
where all the setup, configurations,
management, and analysis take place.

36:45.766 --> 36:48.800
Event collection
from local and remote log sources.

36:49.966 --> 36:55.900
Normalization of raw log source events to
format them to be used by QRadar SIEM.

36:56.333 --> 36:59.366
Flow collection from SPAN ports or network TAPs;

36:59.366 --> 37:02.766
or from external flow-based
data sources, such as Netflow,

37:03.100 --> 37:06.166
J-Flow, and sFlow directly from routers
in your network.

37:07.500 --> 37:09.500
Event and flow processing.

37:09.533 --> 37:12.800
Execution of the actions

defined for rule responses.

37:13.333 --> 37:14.900
Event and flow storage.

37:14.933 --> 37:16.933
And App hosting.

37:17.700 --> 37:21.500
You can purchase QRadar SIEM
hardware appliances from IBM,

37:21.733 --> 37:25.366
you can also install QRadar
SIEM on virtual appliances,

37:25.566 --> 37:29.000
or you can install QRadar
SIEM software on your own hardware.

37:29.533 --> 37:33.033
All of this can be deployed
in a single location or around the world,

37:33.533 --> 37:37.000
which allows you to collect data
no matter where it is located.

37:37.966 --> 37:41.233
QRadar SIEM
can also be deployed in a cloud space,

37:41.300 --> 37:45.533
such as IBM Cloud,
Amazon Web Services, and Microsoft Azure.

37:45.933 --> 37:48.733
Being your own cloud environment,
you are responsible

37:48.766 --> 37:51.900
for deploying and maintaining
the QRadar SIEM instance.

37:52.033 --> 37:56.033
The QRadar SIEM instance
resides in the cloud, and it collects data

37:56.100 --> 37:59.100
directly from data sources

that reside in the cloud as well.

38:00.833 --> 38:02.700
Then, in a hybrid deployment,

38:02.700 --> 38:06.333
you have both a cloud infrastructure
and an on-premises installation.

38:06.733 --> 38:10.533
In this first example, your main hardware,
including the Console, resides

38:10.566 --> 38:12.200
on your premises.

38:12.233 --> 38:15.433
This hardware that you install on
your premises collects data

38:15.500 --> 38:18.700
from data sources in your network.

38:18.733 --> 38:21.133
In addition,
you place a separate collector

38:21.166 --> 38:24.966
in the cloud, which collects data
from sources that reside in that cloud,

38:25.166 --> 38:29.166
and then sends it to your on-premises
processor for processing and storage.

38:30.633 --> 38:31.300
In this second

38:31.300 --> 38:35.900
example, the QRadar SIEM primary
infrastructure is deployed in the cloud

38:35.933 --> 38:39.433
and you collect and process data
directly from cloud collectors.

38:40.200 --> 38:45.533
In addition, you also collect remotely from
one or many on-premises installations.

38:45.800 --> 38:50.200
Here, an organization has the primary
infrastructure in an AWS Cloud.

38:51.166 --> 38:56.433
You can also collect data from a QRadar
Event Processor hosted in another cloud.

38:58.500 --> 39:04.600
As an alternative to your responsibility over the deployment and
management of your QRadar SIEM instance,

39:05.233 --> 39:11.966
QRadar on Cloud (QRoC) can deliver a highly resilient QRadar
SIEM environment from a managed cloud infrastructure.

39:12.900 --> 39:16.066
Like a traditional on-premises QRadar SIEM deployment,

39:16.066 --> 39:19.800
QRoC provides a Console
and can consist of multiple collectors

39:19.800 --> 39:23.300
and processors that send
your security data through data gateways

39:23.500 --> 39:26.200
or Disconnected log collectors if necessary.

39:26.633 --> 39:31.133
Data is encrypted in transit and at rest,
which ensures full confidentiality.

39:32.000 --> 39:37.666
This environment is served from either an IBM Cloud or AWS QRadar
space.

39:38.200 --> 39:43.200
This solution is offered as a single-tenant implementation on bare
metal servers or Virtual Machines,

39:43.333 --> 39:48.233
depending on your organization’s capacity
requirements, measured in events per second.

39:49.466 --> 39:55.800
QRoC includes advanced threat detection, as well as all the other
functionalities of an on-premises deployment.

39:56.166 --> 40:01.200
It allows for elastic upgrades when needed,
resulting in rapid time to value.

40:01.666 --> 40:06.166
Built-in resiliency and fault tolerance
are standard capabilities in QRoC.

40:06.233 --> 40:10.600
You have access to configurable security operations center and
management dashboards.

40:11.033 --> 40:16.900
It offers a global point-of-presence coverage, and multitenant mode is
supported for service providers.

40:17.000 --> 40:20.566
The dedicated IBM DevOps
team is responsible for maintaining,

40:20.566 --> 40:24.766
upgrading, patching, and monitoring
the health of the system 24x7.

40:24.766 --> 40:28.633
QRadar on Cloud is priced by events
per second and retention.

40:29.066 --> 40:31.433
You will learn more about
that later in this video.

40:32.566 --> 40:36.000
Now that we covered the different options
for deployments you can have,

40:36.233 --> 40:39.300
let's look at how to choose the appliances
for your deployment,

40:39.533 --> 40:44.366
plus the different strategies available
to increase the resilience of your deployment.

40:44.600 --> 40:47.300
For hardware appliances
that you can purchase from IBM,

40:47.433 --> 40:50.633
you can identify them

by a four digit code as shown here.

40:51.900 --> 40:55.533
The first two digits of a QRadar SIEM appliance
refer to the role.

40:56.500 --> 41:02.766
For example, 31 is an All-In-One
or Console appliance, 16 is an Event Processor,

41:02.766 --> 41:06.100
while 15 is an Event Collector,
and 14 is a Data Node.

41:06.700 --> 41:09.900
The second two digits
refer to the hardware designation.

41:10.600 --> 41:21.900
So, a 3129 appliance is a Lenovo All-In-One server model
x3650 M5 BD with a 128 GB RAM and 48 TB storage.

41:22.433 --> 41:26.300
There are also a few legacy codes,
some of which are already discontinued.

41:28.333 --> 41:30.500
As explained earlier, in general terms,

41:30.733 --> 41:34.800
QRadar SIEM collects event log and network
flow information, processes

41:34.833 --> 41:39.100
that information so that you can use it
for your threat management efforts

41:39.100 --> 41:42.166
and displays
that information on a central Console.

41:42.400 --> 41:44.900
An All-in-One appliance performs
all these tasks.

41:45.200 --> 41:48.366
As your requirements grow,
you can add individual appliances

41:48.400 --> 41:51.433

that collect and process
event log and network flow information.

41:51.766 --> 41:55.766
Your All-in-One appliance then becomes
the single Console in your network.

41:55.933 --> 42:00.366
QRadar users log into the Console to view
and process all QRadar SIEM Information.

42:00.833 --> 42:04.800
Perhaps your organization uses an
All-in-One QRadar appliance today,

42:05.033 --> 42:07.300
but you can have a satellite office in another country.

42:07.333 --> 42:11.000
If you want to start collecting network
data in that office, you must install

42:11.033 --> 42:14.366
a Flow Collector there
to send the data to your central Console.

42:14.700 --> 42:19.033
Until that point, the data from the Flow Collector is
processed at your Console appliance.

42:19.100 --> 42:24.066
However, if over time you find that
you must perform investigations on the satellite office,

42:24.200 --> 42:27.400
then you need to install a Flow Processor
there to make searches faster.

42:27.966 --> 42:33.100
You still log into the Console to view the QRadar
SIEM information for your company.

42:33.133 --> 42:36.133
As your company grows, or your threat
management requirements change,

42:36.166 --> 42:40.166
you can then add Event Processors
and Collectors to focus on event logs,

42:40.200 --> 42:43.633
Data Nodes to store more data,
or deploy an App Host to use

42:43.700 --> 42:47.000
additional QRadar apps without affecting
your Console's performance.

42:49.400 --> 42:52.533
The High Availability feature allows you
to build redundancy

42:52.566 --> 42:55.766
into your deployment
to defend against hardware failures.

42:56.633 --> 42:58.300
In a High Availability cluster,

42:58.333 --> 43:02.433
you add a second, backup
appliance to any QRadar SIEM managed host,

43:02.633 --> 43:06.500
such as a Console, Collector, Processor,
and the QRadar App Host.

43:06.966 --> 43:12.566
These are called primary and secondary nodes and,
ideally, they should have identical hardware.

43:12.833 --> 43:18.400
QRadar SIEM syncs data and configurations between these appliances,
which creates a perfect copy.

43:18.600 --> 43:20.300
If the hardware fails,

43:20.466 --> 43:24.533
which is detected by a delayed or stopped heartbeat pingt est,

43:24.533 --> 43:30.433
QRadar SIEM automatically fails over to the backup
hardware to minimize gaps in your data collection.

43:30.600 --> 43:36.633
When a failover is detected, the surviving
appliance assumes control of a VIP (Virtual IP)

43:36.633 --> 43:38.733

```
that is shared between the two nodes in the cluster.

43:39.200 --> 43:41.900
Failover usually takes between 3 and 10 minutes,

43:41.900 --> 43:44.566
depending on the hardware
class and function in the deployment.

43:45.300 --> 43:47.600
For example, Consoles
take the longest to fail over

43:47.700 --> 43:49.833
since there are more services to restart.

43:50.266 --> 43:53.366
For more information about High
Availability, see Deployment, resilience

43:53.400 --> 43:57.233
and high availability for QRadar
in the Security Learning Academy.

43:58.566 --> 44:00.733
In addition to High Availability,

44:00.766 --> 44:04.166
QRadar offers
a disaster recovery (DR) option,

44:04.200 --> 44:07.700
which is a key aspect
to the resilience of a QRadar deployment

44:07.733 --> 44:11.233
because it allows for redundancy
at the Data Center level

44:11.500 --> 44:16.100
in the event of a catastrophic failure
of all appliances in one site.

44:17.200 --> 44:21.400
It is comprised of a primary side and a secondary, or DR, site.

44:22.333 --> 44:27.200
When the primary site fails, the second one takes over
and event and flow data is forwarded.
```

44:27.466 --> 44:29.633
This can be done in near real time.

44:29.900 --> 44:33.766
When setting up disaster recovery,
keep in mind the following considerations:

44:34.200 --> 44:37.533
First, the Disaster Recovery site
can be located near

44:37.566 --> 44:42.033
or far the primary site, provided enough
bandwidth exists for the data transfer.

44:42.700 --> 44:47.033
Second, the disaster recovery site
is its own QRadar SIEM deployment

44:47.200 --> 44:50.766
so that it cannot be affected
by any problem on the primary site.

44:51.566 --> 44:54.000
Additionally,
there are a variety of solutions

44:54.033 --> 44:56.800
that can be deployed
in the field for disaster recovery,

44:57.133 --> 45:01.400
including redundant Console-only
configurations, event and flow forwarding

45:01.433 --> 45:04.700
based solutions,
and even full event distribution

45:04.733 --> 45:07.700
to two deployments
(often termed "dual home").

45:08.133 --> 45:12.500
These solutions vary greatly in terms
of complexity, cost and effectiveness.

45:12.733 --> 45:18.400
Most organizations rely on flexible customization,
usually offered by IBM Professional Services,

45:18.433 --> 45:21.833
in the setup and configuration
of their disaster recovery solution.

45:22.300 --> 45:24.366
For more information
about Disaster Recovery,

45:24.566 --> 45:28.100
see QRadar Disaster Recovery
on the Security Learning Academy.

45:30.600 --> 45:34.233
Let's now take a look at the licensing model for QRadar SIEM.

45:37.933 --> 45:40.933
QRadar is based on a role-based
licensing model.

45:41.533 --> 45:44.366
When you install or add
an appliance to your deployment,

45:44.533 --> 45:48.300
you select a role for that appliance,
which configures the following settings:

45:49.100 --> 45:52.333
It establishes the role that
the appliance plays within the deployment.

45:52.833 --> 45:55.700
It enables or disables
features unique to that role.

45:56.300 --> 45:59.100
And it sets license
value limits on some appliances

45:59.133 --> 46:03.033
to ensure optimal performance
based on the hardware: This hardware check

46:03.100 --> 46:06.400
ensures that an adequate configuration
for the role is established.

46:07.200 --> 46:11.166
It also includes a 35-day trial license

for full functionality.

46:11.433 --> 46:15.166
At the end of this period, the user must
apply a permanent license key.

46:15.600 --> 46:19.100
Once the role is established,
it cannot be changed without reinstalling

46:19.133 --> 46:21.766
the software and walking through
the setup process again.

46:25.500 --> 46:27.333
As a QRadar SIEM user,

46:27.366 --> 46:31.533
you contact IBM for license keys
according to your capacity requirements,

46:31.733 --> 46:34.566
or if you want to add a QRadar
Vulnerability Manager,

46:34.800 --> 46:39.000
QRadar Risk Manager, or QRadar Incident
Forensics to your deployment.

46:39.366 --> 46:42.833
The license keys must be applied
to your QRadar SIEM deployment

46:42.900 --> 46:46.433
using the License Management
app in the Admin console.

46:48.300 --> 46:53.200
QRadar applies the following licensing metrics: Events
Per Second (EPS).

46:53.233 --> 46:56.800
Controlled by the license key, this limits
the number of events

46:56.833 --> 47:00.600
that can be collected, normalized,
and correlated in real time.

47:00.833 --> 47:04.500

Any events that are sent to QRadar
SIEM outside of the licensed

47:04.533 --> 47:08.366
limit are queued in a buffer and processed
when activity slows.

47:08.533 --> 47:10.433
This is called "burst handling".

47:10.500 --> 47:12.500
Flows per Minute (FPM).

47:13.066 --> 47:15.500
Like EPS,
this is controlled by the license key

47:15.633 --> 47:20.333
and limits the number of flow records
QRadar SIEM can process in real time.

47:20.333 --> 47:23.233
Burst handling is applied in a similar way to EPS.

47:24.033 --> 47:26.300
Vulnerability Manager Scannable Assets.

47:26.800 --> 47:32.000
This sets the number of assets your Vulnerability
Manager license allows you to manage.

47:32.033 --> 47:35.733
The base license includes 256 manageable assets.

47:36.333 --> 47:39.600
To manage additional assets,
license upgrades are required.

47:40.133 --> 47:42.366
And Risk Manager Configuration Sources.

47:42.800 --> 47:47.700
This is the number of devices that Risk
Manager can gather a configuration data from.

47:47.733 --> 47:49.333
To enable this functionality,

47:49.366 --> 47:53.133
the Risk Management module

needs to run on a dedicated appliance.

47:53.466 --> 47:57.366
The base license includes up to 50
standard configuration sources.

47:59.600 --> 48:03.233
To finish this section, let's expand
the concept of burst handling.

48:03.533 --> 48:05.633
In the examples depicted here,

48:05.633 --> 48:15.200
a corporate network has a QRadar 1828 Event/Flow Processor appliance
that is rated for 5000 EPS and 100,000 FPM.

48:15.633 --> 48:21.433
Typically, this appliance sees on average
4,000 EPS and 70,000 FPM.

48:21.966 --> 48:24.966
Every morning, between 8:00 and 10:00 AM,
the corporate network

48:25.000 --> 48:29.900
experiences an event and flow spike
due to users logging in, accessing network

48:29.933 --> 48:33.700
resources, collecting email,
and other normal activities.

48:34.133 --> 48:37.266
During this interval, which peaks around 9:00 AM,

48:37.266 --> 48:42.766
the appliance sees an event spike at 6,000 EPS and 120,000 FPM.

48:43.133 --> 48:47.233
The appliance realizes the excessive
events, generates a notification,

48:47.300 --> 48:51.933
and the excess data is pushed
to a temporary queue, or overflow buffer.

48:52.166 --> 48:55.433
Every collector has an overflow buffer
of 5 GB.

48:56.033 --> 48:59.800
Events and flows inside the buffer
are processed first in the next cycle.

49:00.500 --> 49:07.566
As system notification is generated to alert the QRadar SIEM
administrator that an appliance has exceeded its license limit.

49:08.333 --> 49:15.866
If you consistently see these messages in your QRadar SIEM Console, it
may be time to reevaluate your current license limits.

49:17.966 --> 49:20.833
We've seen
so far how QRadar SIEM's functionalities

49:20.900 --> 49:25.033
can be distributed in multiple appliances
according to their functionality

49:25.100 --> 49:28.500
and depending on the characteristics
of your network infrastructure.

49:28.966 --> 49:33.633
In the next video, we will look in more detail
the architecture of each QRadar component.