Guardium Virtual User Group

May 23 2023

Leila Johannesen
Guardium Community Advocate

IBM **Security**

Agenda

News & events

Support update

Discussion: New use case capabilities in Guardium Data Protection

Announcements

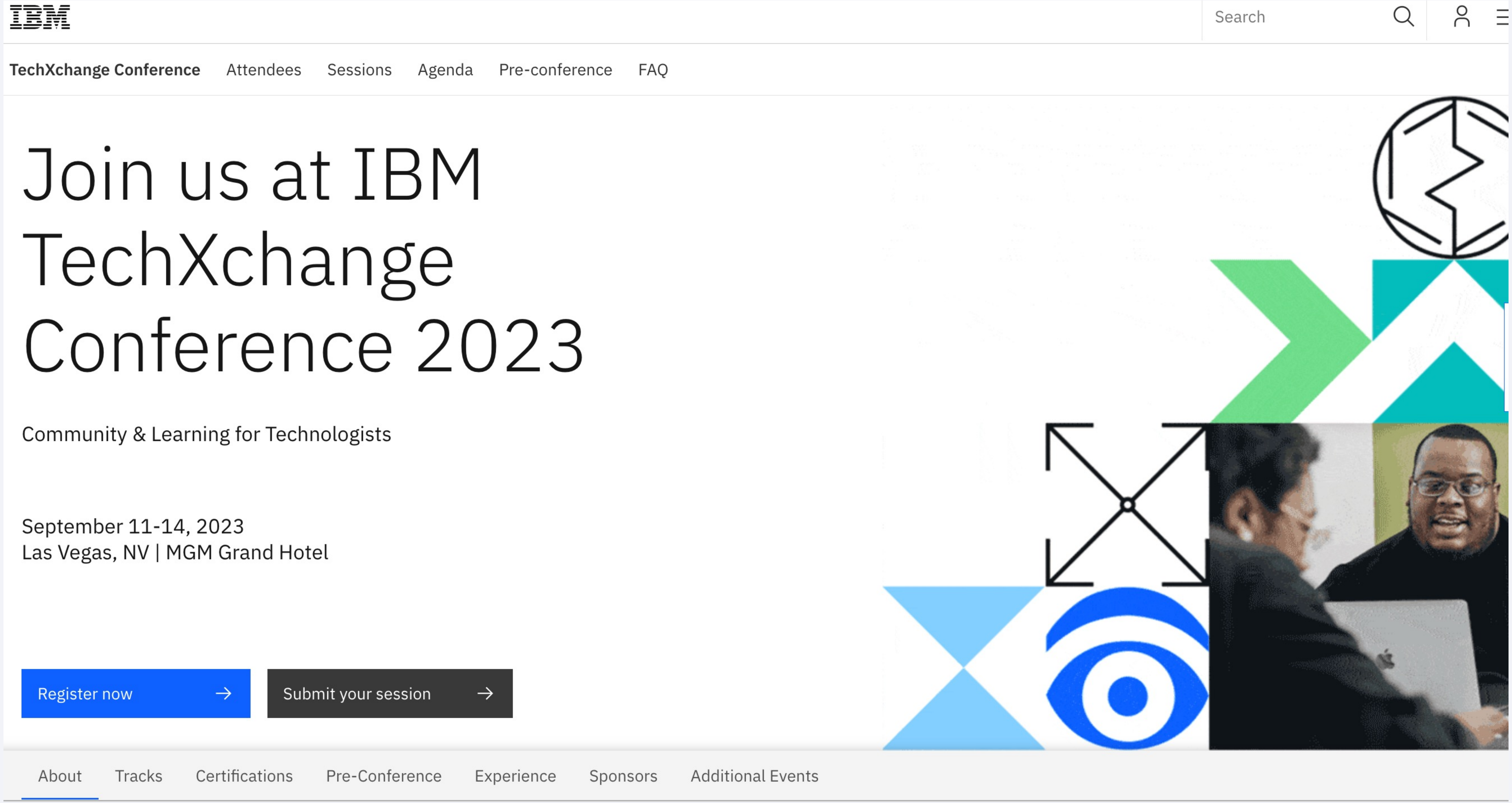
IBM Security Guardium Insights SaaS **eGA May 31 and**

Think 2023 on demand keynotes https://www.ibm.com/events/think/

IBM TechXchange conference **Sept 11-14**

We’ll be hosting a CAB at this event!

https://www.ibm.com/community/ibm-techxchange-conference/



Join us at IBM TechXchange Conference 2023

Community & Learning for Technologists

September 11-14, 2023
Las Vegas, NV | MGM Grand Hotel

You're invited

IBM Security Super User Groups!

Join us for **Super User Groups** created to connect and discuss all things IBM Security Identity and Access Management, Data Security, and Threat Management with other product users as well as IBM experts. We will host individual product user groups for current as well as future customers. In each session, IBM experts will highlight best practices and showcase product demos, while current customers are invited to share feedback on their product experience.

Upcoming events in NA:

Washington, DC – June 7th: https://ibm.biz/RSUG-DC

And more events happening in all geo's! Keep an eye on the IBM Security Community for more: https://ibm.biz/Guardium_Community

Agenda

- Keynote session
- Cyber Range Experience
- What's new in Digital Trust and Threat Management
- Product roadmaps
- Cloud architecture
- Roundtables
- Customer use cases
- Breakout sessions
- Hands on demos
- Networking opportunities
- And more!

Questions? Reach out to carriero@us.ibm.com

Analytics Webinars

June 15 **Guardium Risk Spotter**

Risk Spotter is part of Guardium Data Protection. It uses AI to identify risks across your entire system. Come to learn more about what Risk Spotter can do for you. If you are using already Risk Spotter, join us to ask any questions you have or give us feedback.

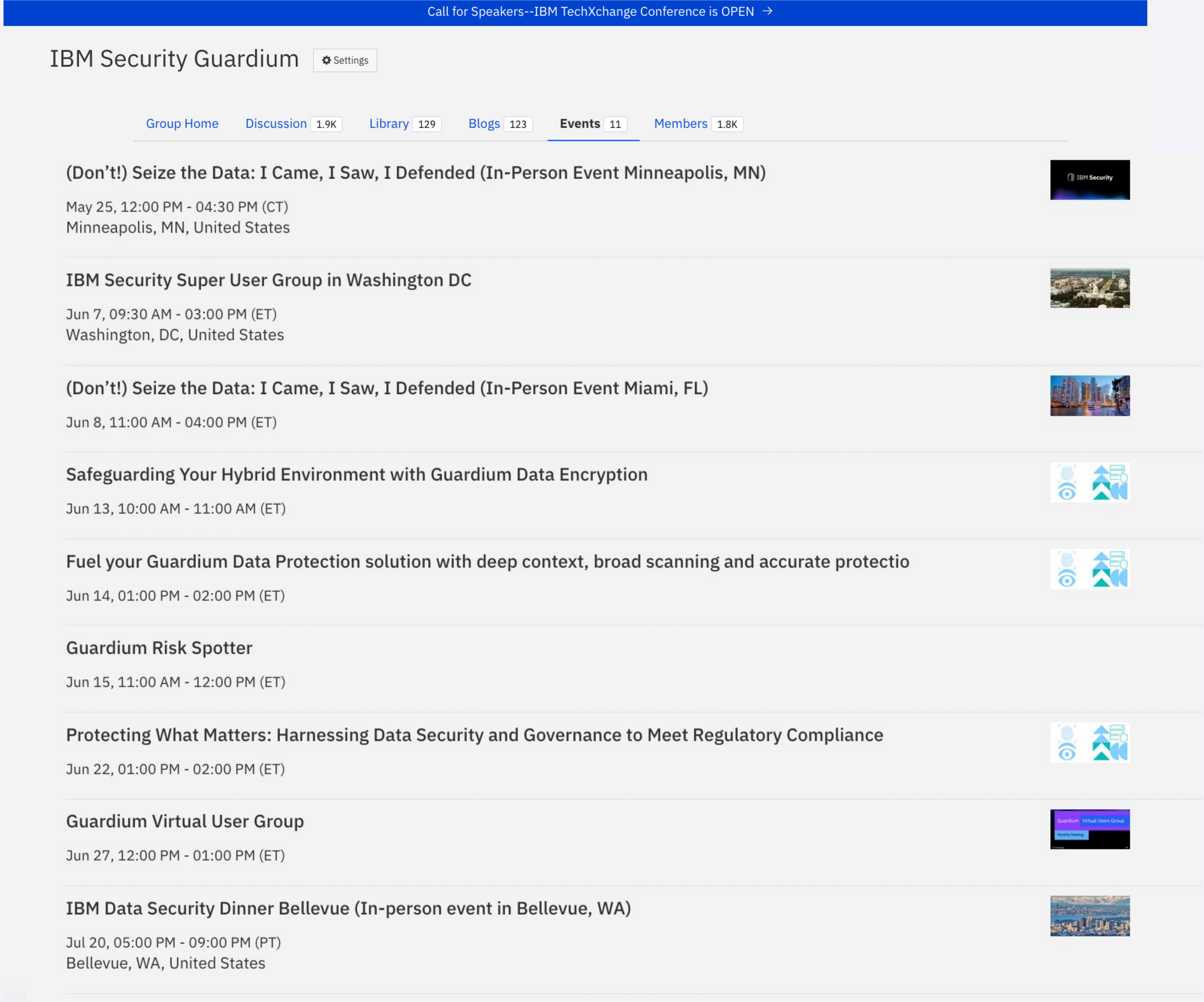
Register here

In May we held a webinar on **Active Threat Analytics**. The slides are in the Community, here.

The replay is being made into a course on the Security Learning Academy.

Events

https://ibm.biz/GuardiumEvents



IBM Security Guardium

(Don't!) Seize the Data: I Came, I Saw, I Defended (In-Person Event Minneapolis, MN)
May 25, 12:00 PM - 04:30 PM (CT)
Minneapolis, MN, United States

IBM Security Super User Group in Washington DC
Jun 7, 09:30 AM - 03:00 PM (ET)
Washington, DC, United States

(Don't!) Seize the Data: I Came, I Saw, I Defended (In-Person Event Miami, FL)
Jun 8, 11:00 AM - 04:00 PM (ET)

Safeguarding Your Hybrid Environment with Guardium Data Encryption
Jun 13, 10:00 AM - 11:00 AM (ET)

Fuel your Guardium Data Protection solution with deep context, broad scanning and accurate protectio
Jun 14, 01:00 PM - 02:00 PM (ET)

Guardium Risk Spotter
Jun 15, 11:00 AM - 12:00 PM (ET)

Protecting What Matters: Harnessing Data Security and Governance to Meet Regulatory Compliance
Jun 22, 01:00 PM - 02:00 PM (ET)

Guardium Virtual User Group
Jun 27, 12:00 PM - 01:00 PM (ET)

IBM Data Security Dinner Bellevue (In-person event in Bellevue, WA)
Jul 20, 05:00 PM - 09:00 PM (PT)
Bellevue, WA, United States

IBM Security Guardium Data Protection V12
Beta Program

Timeframe: June through July

Interested in participating?
Please contact: leilaj@us.ibm.com

Some key enhancements in GDP V12:

- Simplified audit process user experience
- Optimized data classification process workflow
- Ease of use improvements for administration and operation – visibility into patching across MUs, improved load balancing and traffic detection at cluster level
- Currency support for FAM – Solaris support
- Vulnerability Assessment enhancements, including certified support for ServiceNow ‘event management module’
- and more

Support Update

-

Lisette Contreras
Guardium Support

IBM **Security**

V11 Notable Releases

Appliance Updates

- **V11.x: Updated Health Check**: SqlGuard_11.0p9997_Health_Check_2023-04-20
- **DPS patch:** Guardium_11.0_DPS-Update_Q2-2023_Database-Protection-Knowledgebase-Subscription

Agent Updates

- **V11.4**:

GIM V11.4.1.3_r114322 (RedHat 6/7/8, Suse, Ubuntu, zLinux, Solaris, HP-UX, Debian, AIX)
STAP V11.4.1.3 r114322 (RedHat 6/7/8, Suse, Ubuntu, zLinux, Solaris, HP-UX, Debian, AIX)
GIM and STAP 11.3.0.394 (Windows)

KTAP Updates

- **V11.4**:
  RedHat 6: New KTAP module: Guardium_KTAP_11.4_rhel-6-linux-x86-64_r112810_2023-04-29
  RedHat 8: New KTAP module: Guardium_KTAP_11.4_rhel-8-linux-x86-64_r112810_2023-04-30
- **V11.5**:
  Ubuntu: Guardium_KTAP_11.5_ubuntu-20-linux-x86-64_r113723_2023-05-01

V10.x Notable Releases

Appliance Updates

- **V10.x:**
  DPS patch: Guardium_10.0_DPS-Update_Q2-2023_Database-Protection-Knowledgebase-Subscription_
- **V10.5:**
  Bundle: SqlGuard_10.0p560_May-03-2023_

Agent Updates

No new agents released in May as of 05/22/2023.

KTAP Bundles

No new KTA modules released in May as of 05/22/2023.

Flash Alerts and Vulnerability Fixes

Link to latest FLASH Alerts, alerts and bulletins:
https://www.ibm.com/systems/support/myview/subscription/css.wss/view/P14fda7f6ab1

No new FLASH alerts released in April as of 05/22/2023.

Flash Alerts and Vulnerability Fixes (cont)

SECURITY VULNERABILITIES:

No new Security Bulletins released in May as of 05/22/2023.

Discussion

General Resources

IBM Security Guardium User Resources

Learn

Free learning

- Guardium Educational Resources - Handy list of links to videos and courses organized by topic.
- Security Learning Academy - Technical training for IBM Security products, including many courses on Guardium.
- Guardium TechBook – Video presentations on key topics that provide a foundation for Guardium.

Other Training

- Guardium Data Protection Administrator Foundations Badge - Two ways to take the administrator course and get a badge.
- Guardium Data Protection Foundations course - Training administered through third party.

Community

Guardium User Community

- Join the Guardium User Community to participate in online discussions, view libraries, blogs & events.

Virtual User Group meetings

- Monthly meetings for customers on all things Guardium. Contact leilaj@us.ibm.com to be added.

Regional User Group meetings

- Face-to-face user groups held in different regions across the US and world on Guardium. May be held virtually. Sessions listed in events.

Super User Group meetings

- New this year: Virtual user groups on various security topics. Sessions listed in events.

For more information on the Regional or Super User groups, contact carriero@us.ibm.com

Use

Product Documentation

- IBM Security Guardium Data Protection
- IBM Security Guardium Insights

Support

- Support website: Open a case
- Supported platforms and requirements for GDP V11.5
- Search for supported platforms by version
- Find correct K-TAP version
- Subscribe to MyNotifications

Request an Enhancement

- Guardium Ideas Portal: Add an Idea

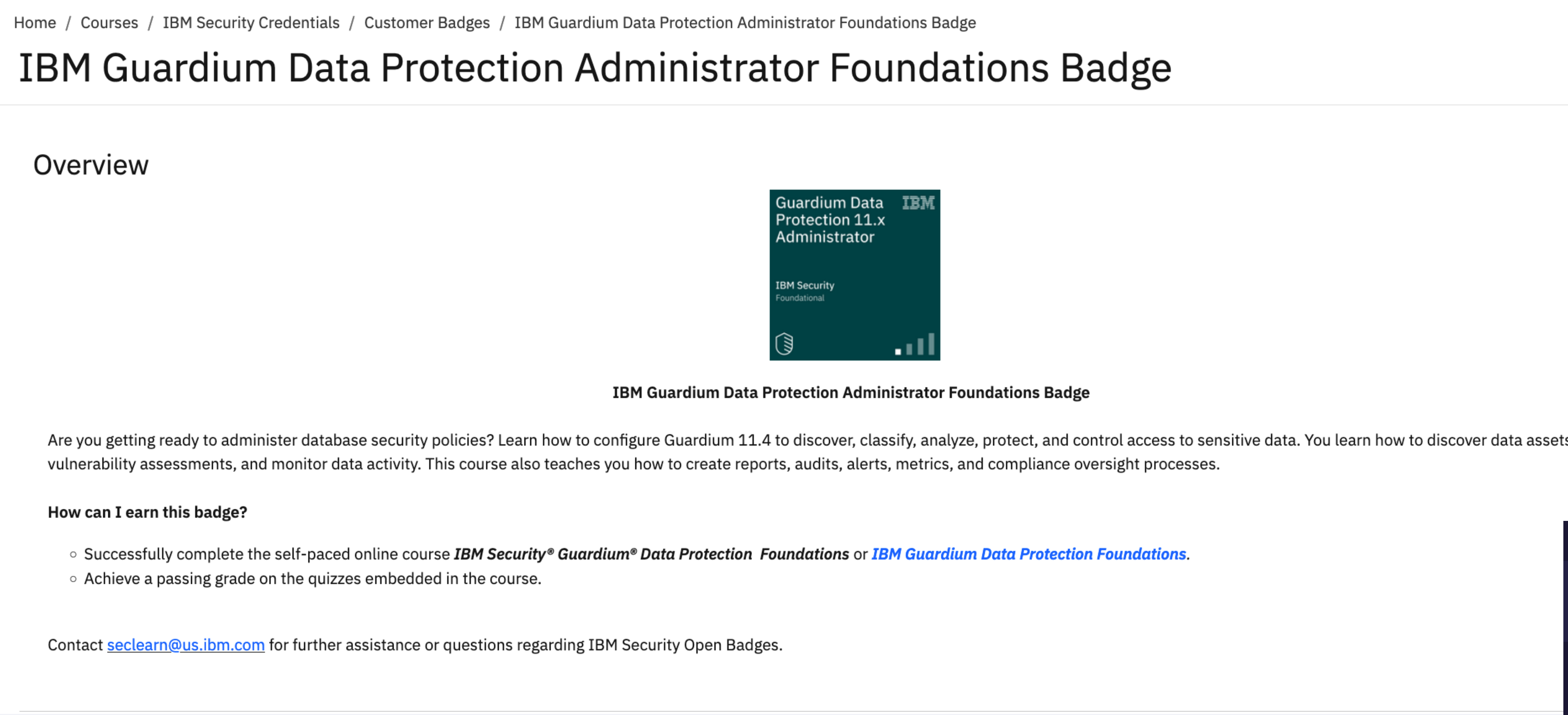
Guardium Value Assessment – A two or three hour no-charge workshop to assess your Guardium environment and make sure you are getting maximum value. Ask your IBM Rep for more information & scheduling.

Updated 2/9/23

All underlined bullets are hyperlinks

IBM **Security**

Guardium Data Protection Administrator Foundations Badge



Home / Courses / IBM Security Credentials / Customer Badges / IBM Guardium Data Protection Administrator Foundations Badge

IBM Guardium Data Protection Administrator Foundations Badge

Overview

IBM Guardium Data Protection Administrator Foundations Badge

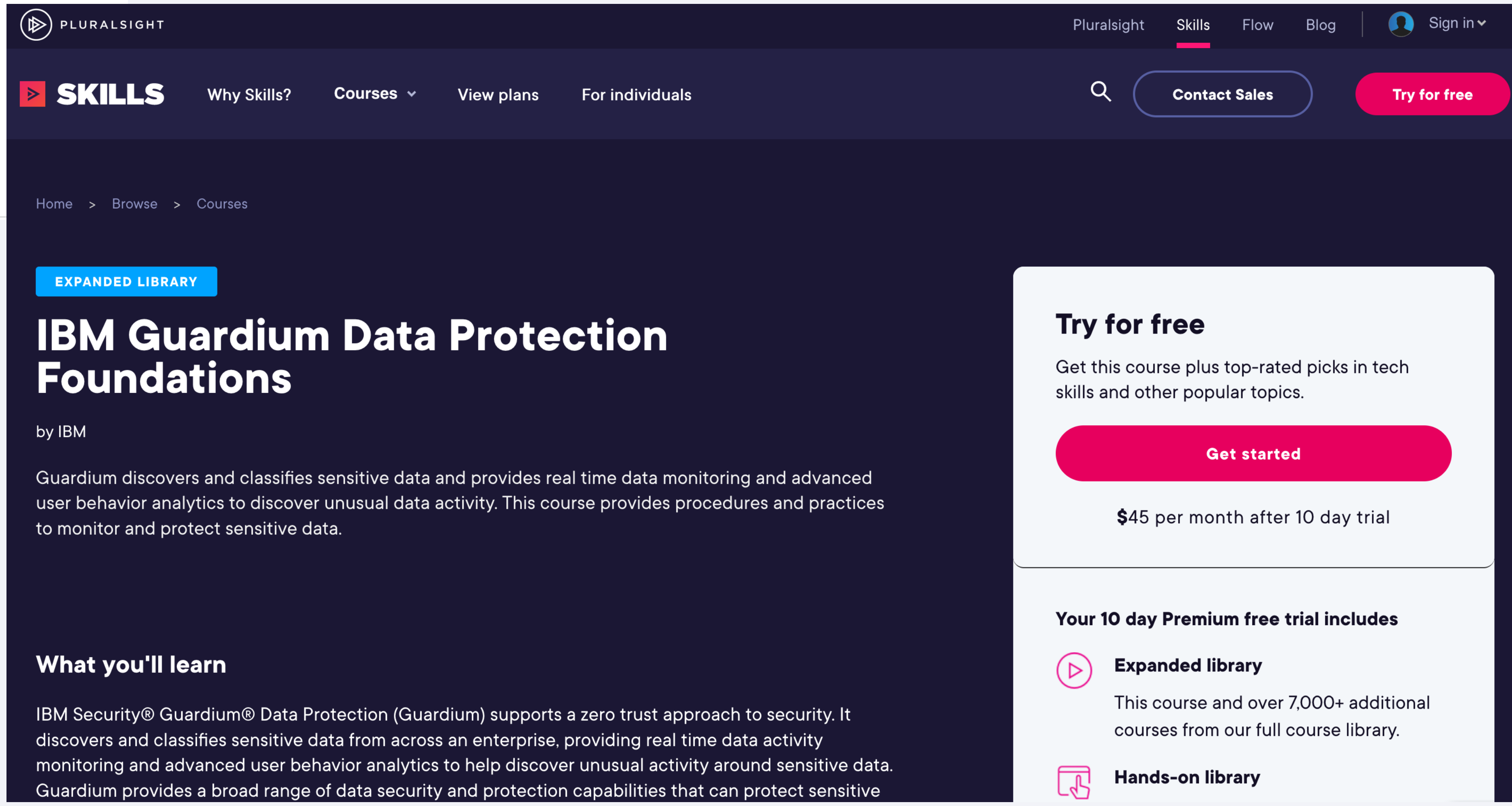
Are you getting ready to administer database security policies? Learn how to configure Guardium 11.4 to discover, classify, analyze, protect, and control access to sensitive data. You learn how to discover data assets, perform vulnerability assessments, and monitor data activity. This course also teaches you how to create reports, audits, alerts, metrics, and compliance oversight processes.

How can I earn this badge?

- Successfully complete the self-paced online course ***IBM Security® Guardium® Data Protection Foundations*** or ***IBM Guardium Data Protection Foundations***.
- Achieve a passing grade on the quizzes embedded in the course.

Contact seclearn@us.ibm.com for further assistance or questions regarding IBM Security Open Badges.

https://www.securitylearningacademy.com/course/view.php?id=6877



Home > Browse > Courses

EXPANDED LIBRARY

IBM Guardium Data Protection Foundations

by IBM

Guardium discovers and classifies sensitive data and provides real time data monitoring and advanced user behavior analytics to discover unusual data activity. This course provides procedures and practices to monitor and protect sensitive data.

What you'll learn

IBM Security® Guardium® Data Protection (Guardium) supports a zero trust approach to security. It discovers and classifies sensitive data from across an enterprise, providing real time data activity monitoring and advanced user behavior analytics to help discover unusual activity around sensitive data. Guardium provides a broad range of data security and protection capabilities that can protect sensitive

Try for free

Get this course plus top-rated picks in tech skills and other popular topics.

Get started

$45 per month after 10 day trial

Your 10 day Premium free trial includes

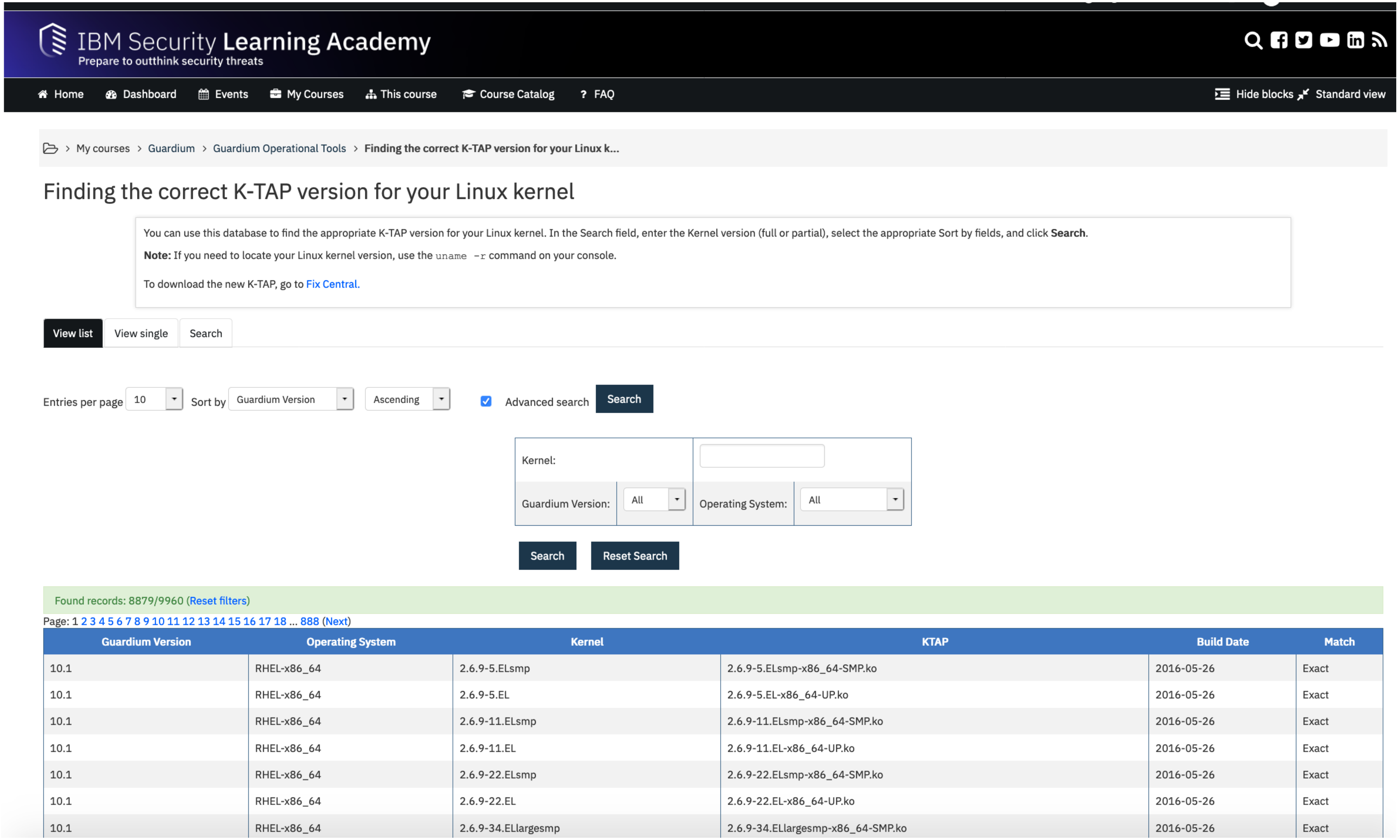
Expanded library

This course and over 7,000+ additional courses from our full course library.

Hands-on library

Finding the correct K-TAP version for your Linux kernel

http://ibm.biz/GuardiumKTAP


IBM Security Learning Academy
Prepare to outthink security threats
Home
Dashboard
Events
My Courses
This course
Course Catalog
? FAQ
Hide blocks
Standard view
My courses › Guardium › Guardium Operational Tools › Finding the correct K-TAP version for your Linux k...

Finding the correct K-TAP version for your Linux kernel

You can use this database to find the appropriate K-TAP version for your Linux kernel. In the Search field, enter the Kernel version (full or partial), select the appropriate Sort by fields, and click **Search**.

Note: If you need to locate your Linux kernel version, use the `uname -r` command on your console.

To download the new K-TAP, go to Fix Central.

Entries per page: 10
Sort by: Guardium Version
Ascending
☑ Advanced search

Kernel:
Guardium Version: All
Operating System: All

Found records: 8879/9960 (Reset filters)

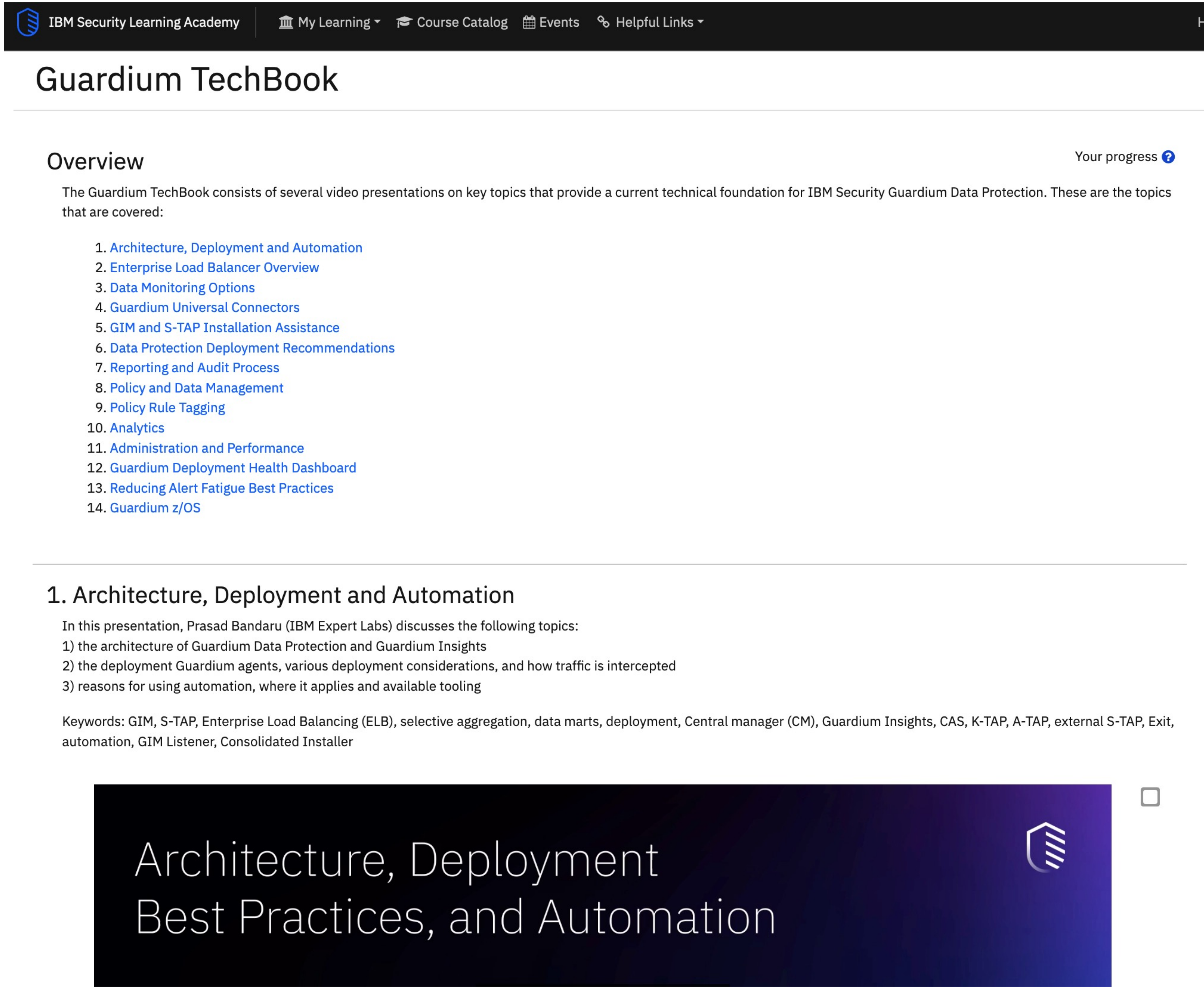
Page: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 ... 888 (Next)

Guardium Version	Operating System	Kernel	KTAP	Build Date	Match
10.1	RHEL-x86_64	2.6.9-5.ELsmp	2.6.9-5.ELsmp-x86_64-SMP.ko	2016-05-26	Exact
10.1	RHEL-x86_64	2.6.9-5.EL	2.6.9-5.EL-x86_64-UP.ko	2016-05-26	Exact
10.1	RHEL-x86_64	2.6.9-11.ELsmp	2.6.9-11.ELsmp-x86_64-SMP.ko	2016-05-26	Exact
10.1	RHEL-x86_64	2.6.9-11.EL	2.6.9-11.EL-x86_64-UP.ko	2016-05-26	Exact
10.1	RHEL-x86_64	2.6.9-22.ELsmp	2.6.9-22.ELsmp-x86_64-SMP.ko	2016-05-26	Exact
10.1	RHEL-x86_64	2.6.9-22.EL	2.6.9-22.EL-x86_64-UP.ko	2016-05-26	Exact
10.1	RHEL-x86_64	2.6.9-34.ELlargesmp	2.6.9-34.ELlargesmp-x86_64-SMP.ko	2016-05-26	Exact

Guardium TechBook

Consists of several video presentations on key topics that provide a current technical foundation for IBM Security Guardium Data Protection

https://www.securitylearningacademy.com/enrol/index.php?id=6411



Guardium TechBook

Overview

The Guardium TechBook consists of several video presentations on key topics that provide a current technical foundation for IBM Security Guardium Data Protection. These are the topics that are covered:

1. Architecture, Deployment and Automation
2. Enterprise Load Balancer Overview
3. Data Monitoring Options
4. Guardium Universal Connectors
5. GIM and S-TAP Installation Assistance
6. Data Protection Deployment Recommendations
7. Reporting and Audit Process
8. Policy and Data Management
9. Policy Rule Tagging
10. Analytics
11. Administration and Performance
12. Guardium Deployment Health Dashboard
13. Reducing Alert Fatigue Best Practices
14. Guardium z/OS

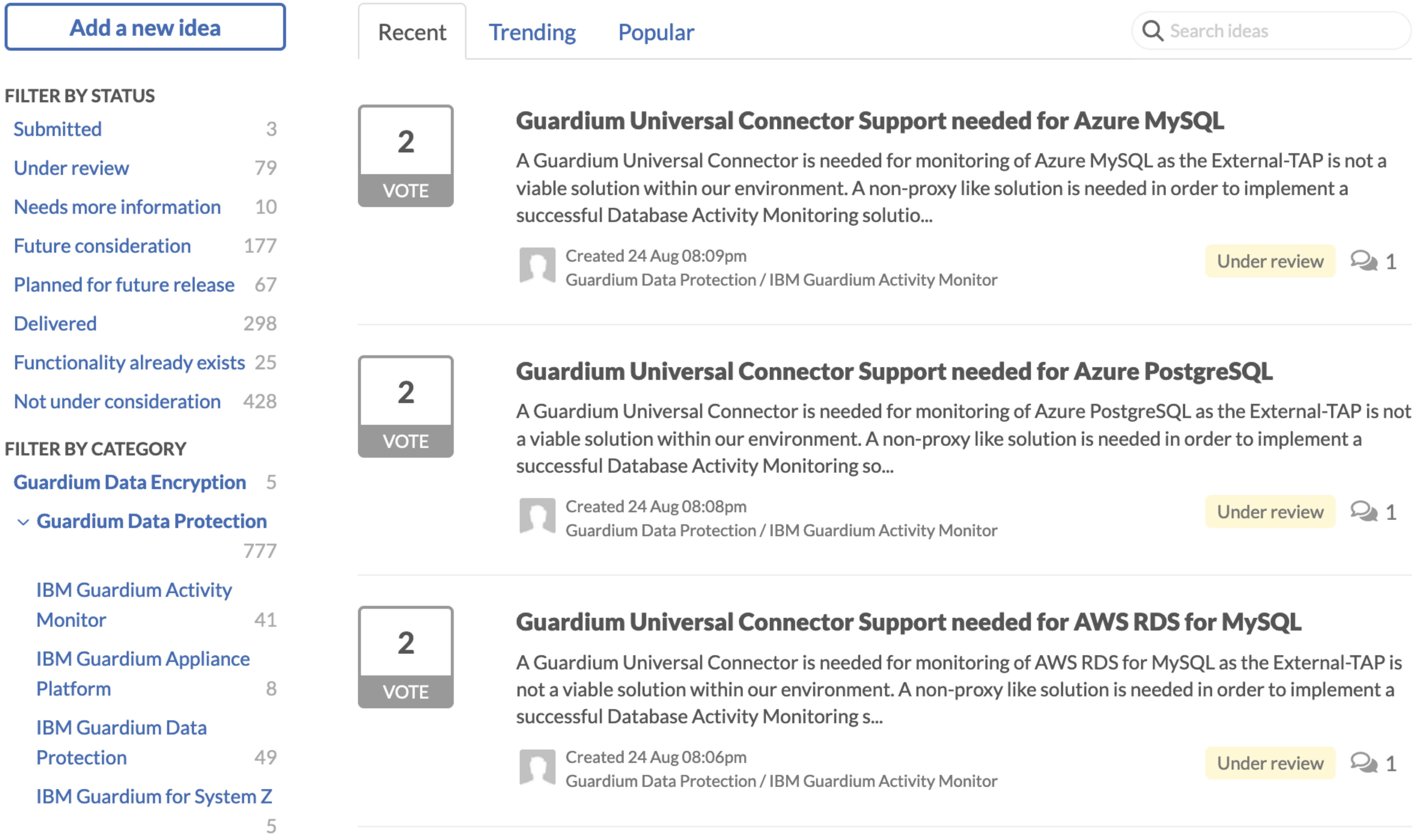
1. Architecture, Deployment and Automation

In this presentation, Prasad Bandaru (IBM Expert Labs) discusses the following topics:
1) the architecture of Guardium Data Protection and Guardium Insights
2) the deployment Guardium agents, various deployment considerations, and how traffic is intercepted
3) reasons for using automation, where it applies and available tooling

Keywords: GIM, S-TAP, Enterprise Load Balancing (ELB), selective aggregation, data marts, deployment, Central manager (CM), Guardium Insights, CAS, K-TAP, A-TAP, external S-TAP, Exit, automation, GIM Listener, Consolidated Installer

Ideas aka Requests for Enhancements (RFEs)

IBM Security Guardium Ideas Portal https://ibmsecurity.ideas.ibm.com/



FILTER BY STATUS

Submitted	3
Under review	79
Needs more information	10
Future consideration	177
Planned for future release	67
Delivered	298
Functionality already exists	25
Not under consideration	428

FILTER BY CATEGORY

Guardium Data Encryption	5
Guardium Data Protection	777
IBM Guardium Activity Monitor	41
IBM Guardium Appliance Platform	8
IBM Guardium Data Protection	49
IBM Guardium for System Z	5

2 VOTE

Guardium Universal Connector Support needed for Azure MySQL

A Guardium Universal Connector is needed for monitoring of Azure MySQL as the External-TAP is not a viable solution within our environment. A non-proxy like solution is needed in order to implement a successful Database Activity Monitoring solutio...

Created 24 Aug 08:09pm
Guardium Data Protection / IBM Guardium Activity Monitor
Under review 1

2 VOTE

Guardium Universal Connector Support needed for Azure PostgreSQL

A Guardium Universal Connector is needed for monitoring of Azure PostgreSQL as the External-TAP is not a viable solution within our environment. A non-proxy like solution is needed in order to implement a successful Database Activity Monitoring so...

Created 24 Aug 08:08pm
Guardium Data Protection / IBM Guardium Activity Monitor
Under review 1

2 VOTE

Guardium Universal Connector Support needed for AWS RDS for MySQL

A Guardium Universal Connector is needed for monitoring of AWS RDS for MySQL as the External-TAP is not a viable solution within our environment. A non-proxy like solution is needed in order to implement a successful Database Activity Monitoring s...

Created 24 Aug 08:06pm
Guardium Data Protection / IBM Guardium Activity Monitor
Under review 1

Universal Connectors

Available UCs are listed here:
https://github.com/IBM/universal-connectors/blob/main/docs/available_plugins.md

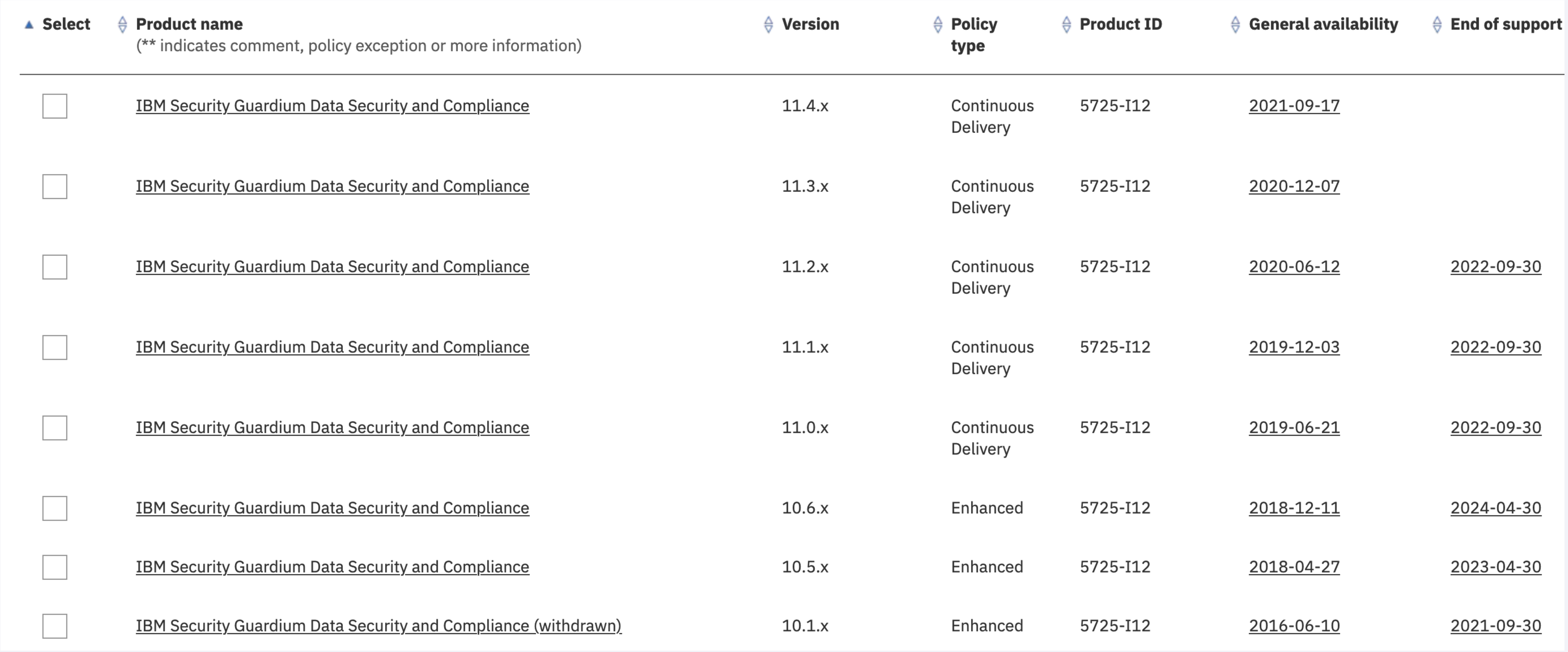
Overview page:
https://github.com/IBM/universal-connectors

Tech Day on Building your own UCs
https://www.securitylearningacademy.com/course/view.php?id=6361

Reminder: GDP End of Support dates

V11.0, 11.1, 11.2 are already EOS as of Sept 20 2022
V10.5 EOS April 30 2023
V10.6 EOS April 30 2024

https://www.ibm.com/support/pages/lifecycle/search/?q=5725-I12



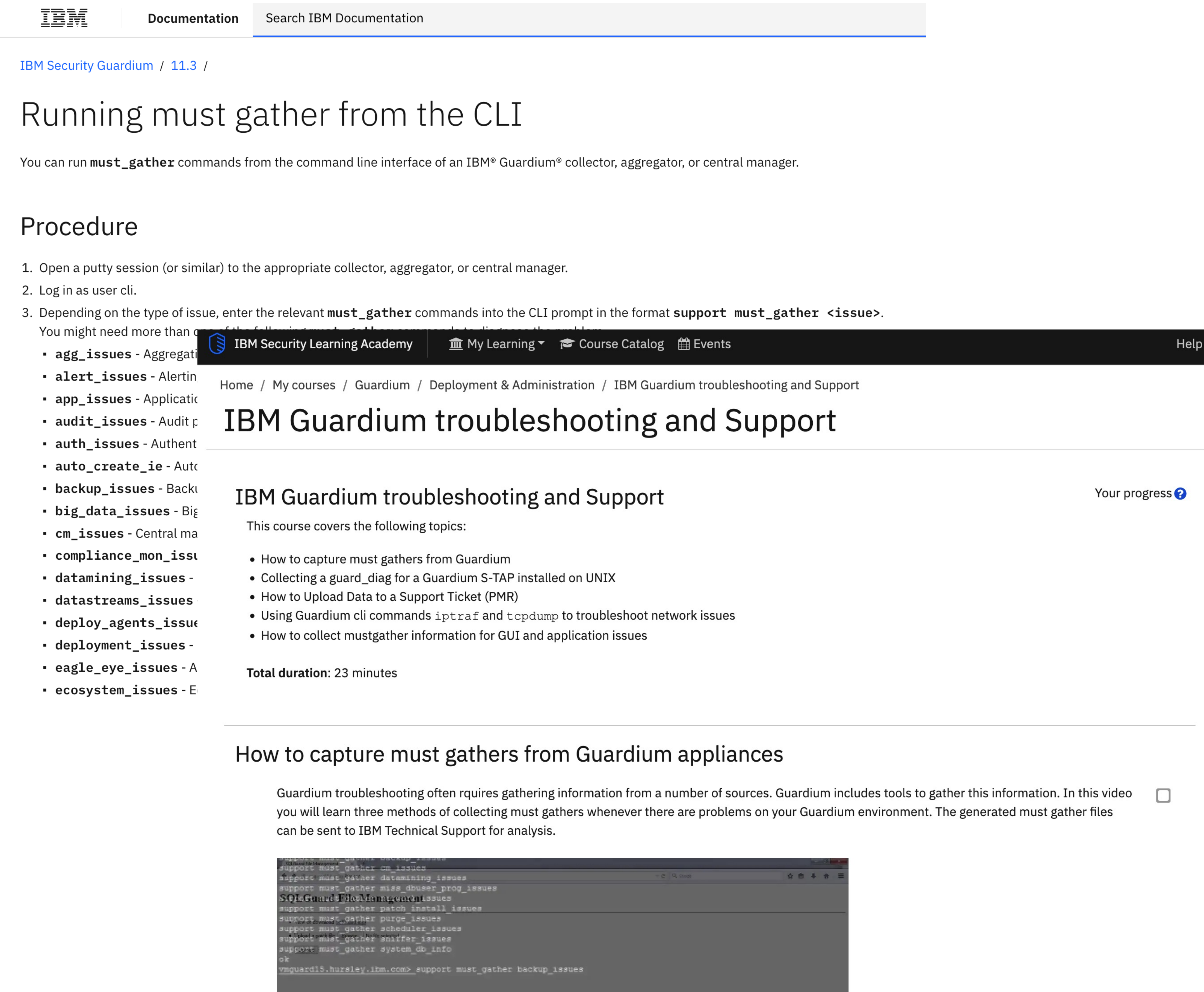
Select	Product name (** indicates comment, policy exception or more information)	Version	Policy type	Product ID	General availability	End of support
☐	IBM Security Guardium Data Security and Compliance	11.4.x	Continuous Delivery	5725-I12	2021-09-17	
☐	IBM Security Guardium Data Security and Compliance	11.3.x	Continuous Delivery	5725-I12	2020-12-07	
☐	IBM Security Guardium Data Security and Compliance	11.2.x	Continuous Delivery	5725-I12	2020-06-12	2022-09-30
☐	IBM Security Guardium Data Security and Compliance	11.1.x	Continuous Delivery	5725-I12	2019-12-03	2022-09-30
☐	IBM Security Guardium Data Security and Compliance	11.0.x	Continuous Delivery	5725-I12	2019-06-21	2022-09-30
☐	IBM Security Guardium Data Security and Compliance	10.6.x	Enhanced	5725-I12	2018-12-11	2024-04-30
☐	IBM Security Guardium Data Security and Compliance	10.5.x	Enhanced	5725-I12	2018-04-27	2023-04-30
☐	IBM Security Guardium Data Security and Compliance (withdrawn)	10.1.x	Enhanced	5725-I12	2016-06-10	2021-09-30

Important support links – must gathers

Running must gather from the CLI:
https://www.ibm.com/docs/en/guardium/11.3?topic=support-running-must-gather-from-cli

Capturing must gathers:
https://www.securitylearningacademy.com/course/view.php?id=843

STAP diags:
https://www.ibm.com/support/pages/ibm-mustgather-collecting-data-guardium-stap



IBM Security Guardium / 11.3 /

Running must gather from the CLI

You can run **`must_gather`** commands from the command line interface of an IBM® Guardium® collector, aggregator, or central manager.

Procedure

1. Open a putty session (or similar) to the appropriate collector, aggregator, or central manager.
2. Log in as user cli.
3. Depending on the type of issue, enter the relevant **`must_gather`** commands into the CLI prompt in the format **`support must_gather <issue>`**.
   You might need more than o
   - **`agg_issues`** - Aggregati
   - **`alert_issues`** - Alertin
   - **`app_issues`** - Applicatio
   - **`audit_issues`** - Audit p
   - **`auth_issues`** - Authent
   - **`auto_create_ie`** - Auto
   - **`backup_issues`** - Backu
   - **`big_data_issues`** - Big
   - **`cm_issues`** - Central ma
   - **`compliance_mon_issu`**
   - **`datamining_issues`** -
   - **`datastreams_issues`**
   - **`deploy_agents_issue`**
   - **`deployment_issues`** -
   - **`eagle_eye_issues`** - A
   - **`ecosystem_issues`** - E

Home / My courses / Guardium / Deployment & Administration / IBM Guardium troubleshooting and Support

IBM Guardium troubleshooting and Support

IBM Guardium troubleshooting and Support

This course covers the following topics:

- How to capture must gathers from Guardium
- Collecting a guard_diag for a Guardium S-TAP installed on UNIX
- How to Upload Data to a Support Ticket (PMR)
- Using Guardium cli commands `iptraf` and `tcpdump` to troubleshoot network issues
- How to collect mustgather information for GUI and application issues

Total duration: 23 minutes

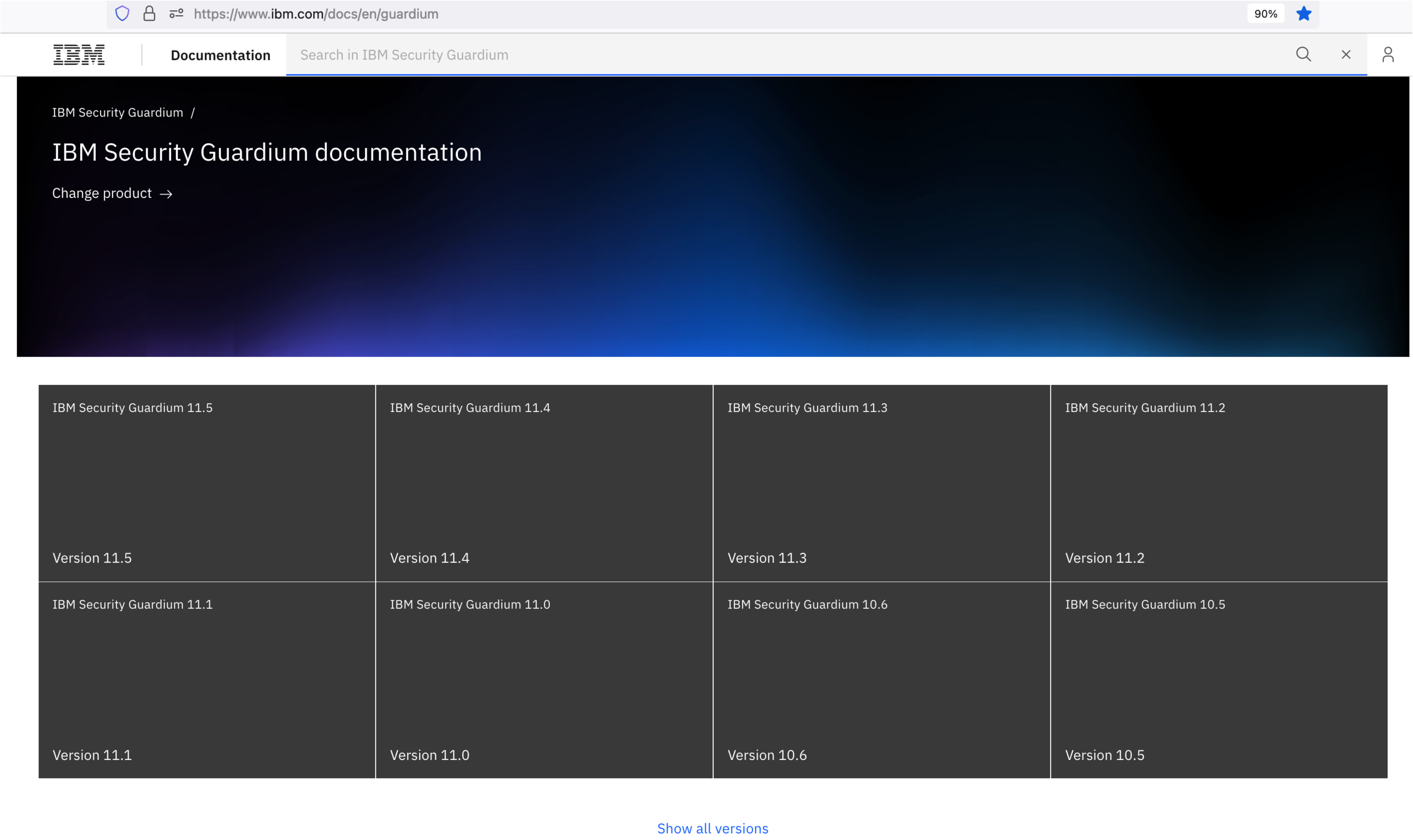
How to capture must gathers from Guardium appliances

Guardium troubleshooting often rquires gathering information from a number of sources. Guardium includes tools to gather this information. In this video you will learn three methods of collecting must gathers whenever there are problems on your Guardium environment. The generated must gather files can be sent to IBM Technical Support for analysis. ☐

```
support must_gather cm_issues
support must_gather datamining_issues
support must_gather miss_dbuser_prog_issues
support must_gather patch_install_issues
support must_gather purge_issues
support must_gather scheduler_issues
support must_gather sniffer_issues
support must_gather system_db_info
ok
vmguard15.hursley.ibm.com> support must_gather backup_issues
```

IBM Documentation

https://www.ibm.com/docs/en/guardium



https://www.ibm.com/docs/en/guardium

IBM Security Guardium /

IBM Security Guardium documentation

Change product →

IBM Security Guardium 11.5 Version 11.5	IBM Security Guardium 11.4 Version 11.4	IBM Security Guardium 11.3 Version 11.3	IBM Security Guardium 11.2 Version 11.2
IBM Security Guardium 11.1 Version 11.1	IBM Security Guardium 11.0 Version 11.0	IBM Security Guardium 10.6 Version 10.6	IBM Security Guardium 10.5 Version 10.5

Show all versions

SupportTalk replays

Webinar series focused on Support topics with Q & A to help you manage your Guardium environment and avoid support calls.

Troubleshooting Guardium Agents (GIM and S-TAP)
https://www.securitylearningacademy.com/enrol/index.php?id=6844

Upgrading to Guardium V11 Best Practices
https://www.securitylearningacademy.com/course/view.php?id=6754

Guardium Data Marts
https://www.securitylearningacademy.com/course/view.php?id=6227

Enterprise Load Balancing Tips for Configuration and Troubleshooting
https://www.securitylearningacademy.com/course/view.php?id=6187

Using Guardium's out-of-the-box views to ensure your Guardium system's health
https://www.securitylearningacademy.com/enrol/index.php?id=6109

Aggregation Basics and Best Practices
https://www.securitylearningacademy.com/course/view.php?id=6072