Security Intelligence Tutorial, Demo & Use Case Videos

This document contains a growing list of very useful Security Intelligence Tutorial & Demo videos posted on YouTube™. The latest version of this file can be downloaded from this public Box folder, go to the end (currently page 3): https://ibm.box.com/s/ich0yyiw54y0ek6s9a66xvtjku8e42rc

What is a SIEM?

What is a SIEM? Part One (Aug 2021) (**14:01**)	https://youtu.be/MtqFMe4zSpQ
What is a SIEM? Part Two (Aug 2021) (**12:02**)	https://youtu.be/iD522z7vzeQ
What is a SIEM? Part Three (Aug 2021) (**11:15**)	https://youtu.be/_10i0Cp0Y1U

IBM Security learning Academy https://youtu.be/eTdVteVOraM **July 12,2017**

New QRadar Offenses and Searches UI (Analyst WorkFlow)

QRadar UI updated 1.4.1 (Feb 2021) (**7:38**)	https://youtu.be/m-ZIgX7ZL48
QRadar UI and Advisor updates (Oct 2020) (**8:01**)	https://youtu.be/nX38b-NLZBo
QRadar new UI: Offenses (June 2020)	https://youtu.be/3U9wIgzo0Ak
QRadar New UI: Searches (June 2020)	https://youtu.be/GjITI5aFvPU
QRadar New UI: Installation (June 2020)	https://youtu.be/-Ieu8IUbC-U

Dealing with Ransomware and Phishing

Part 1 Intro, vectors and leveraging standard flow (July 2021) (**9:09**)	https://youtu.be/XG-4fbEvDw8
Part 2 Where to get the right rules (July 2021) (**8:53**)	https://youtu.be/yV8WkBwH1G0
Part 3 Getting the best Threat Intel (July 2021) (**10:05**)	https://youtu.be/YqEGSFDinu8
Part 4 Log Sources. QNI, UBA and NTA (July 2021) (**12:18**)	https://youtu.be/QSs4TpukJg0
Part 5 Writing a simple rule (July 2021) (**12:07**)	https://youtu.be/dEiAoEE5h80
Part 6 Remediating with a SOAR tool (July 2021) (**9:09**)	https://youtu.be/ALRx2W53TB8
Detecting Ransomware: Shadow Copies Deletion (Aug 2021) (**2:29**)	https://youtu.be/GOsDd2lhZt4
Detecting Ransomware: Cerutil to a bad URL (Aug 2021) (**2:08**)	https://youtu.be/7gnz2Hz4rnc
Detecting Ransomware: Credential Dumping (Aug 2021) (**2:58**)	https://youtu.be/SXE6itW5NE0
Detecting Ransomware: Malicious IOCs (Aug 2021) (**1:18**)	https://youtu.be/pHVAkne9gDg
Detecting Ransomware: Other Bad Things (Aug 2021) (**4:10**).	https://youtu.be/UNpO18-9p4U

End Point Rules App (Content Pack)

Radar Endpoint Rules Updated (Aug 2021) (**0:45**)	https://youtu.be/3JBvtcQ4O0Y
Cobalt Strike Detection (Sept 2021) (**10:50**)	https://youtu.be/T7ui-DR6sgU

Think Like a Hacker

Introduction: (April 2020)	https://youtu.be/3K6_73Imv2E
What this video series is and is not (April 2020)	https://youtu.be/EFWFdsxQc04
Use Cases:	
Detecting the nasty Zerologon exploit (Sept 2020)	https://youtu.be/6wI1E3S1xfs
Privilege escalation and Persistency Win7 (April 2020)	https://youtu.be/RSoCv_PhC8U
Obfuscation with Special Characters (April 2020)	https://youtu.be/Hudh3Inum5I

Obfuscation and compression (April 2020)	https://youtu.be/XvOP3uKWCMM
Two Great Searches (April 2020)	https://youtu.be/mCWPof1CyGA
Persistency without privilege escalation (April 2020)	https://youtu.be/CAxyMBLAhJk
COM Hijacking, this is nasty (April 2020)	https://youtu.be/mi2-qvhcNYc
First Attack on a Win10 (April 2020)	https://youtu.be/dwh3wzVdRIg
Dot Net CLR Profile Hijacking (April 2020)	https://youtu.be/XVDzTQLRYvQ
Second Attack Win10 UAC Bypass (April 2020)	https://youtu.be/XSy-LT1SDHQ
Detecting Kerberos golden ticket Attacks with Sysmon	https://youtu.be/ESUVZ1KkjOk
Golden Ticket Attack Detection, what ATA catches or misses	https://youtu.be/qR5jw2f0RzA
Over Pass The Hash and Domain Sync	https://youtu.be/Ao7D9GBhv8c
Remote in memory attack without any user interaction	https://youtu.be/o-_DwZuDCU8
Execute a WMI Query Remotely using Pass The Hash	https://youtu.be/NLUbANm9ODA
Sysmon Detecting Mimikatz	https://youtu.be/gKa_CZAz3Jc
Win10 Phishing, escalation, password capture and lateral movement	https://youtu.be/_uJv7Ssh2sU
Golden SAML Attack (Jan 2021) (**11:40**)	https://youtu.be/OAPLyKlgOj0
Enable ADFS logs into QRadar (Jan 2021) (**4:41**)	https://youtu.be/TaEQc9cnxrI

Lab Setup:

ZeroLogon Dealing with false positives part three (Sept 2020)	https://youtu.be/bnDYke6zLdM
ZeroLogon Dealing with false positives part two (Sept 2020)	https://youtu.be/ipnWlZ9CagY
ZeroLogon Dealing with false positives (Sept 2020)	https://youtu.be/yHavVLW2fng
Setting the detection for Zerologon (Sept 2020)	https://youtu.be/Zm9NLXcOGGQ
Win7 Sysmon and Wincollect Installation (April 2020)	https://youtu.be/RKk3JHmkm4E
Installing Kali (April 2020)	https://youtu.be/uv6RYfVVvXQ
Installing the Sysmon Rules in QRadar CE (April 2020)	https://youtu.be/GzdI2abbVo4
Win10 Sysmon and Wincollect Installation (April 2020)	https://youtu.be/MZ8WrkcLGYY
Lab Preparation for Lateral Movement in Win10 (May 2020)	https://youtu.be/u-J9A_ChSyY

Optional:

Using msfvenom for a different Kali IP (April 2020)	https://youtu.be/6NECOIJqo6E
Launching the myLove exe from a word document (April 2020)	https://youtu.be/bAE-73q3V9k

New and Free QRadar CE 733

New Free QRadar CE version 733 (Feb 2020)	https://youtu.be/_fltNyDIkq4
QRadar CE 7.3.3 Adding a DSM/Parser (Feb 2020)	https://youtu.be/4pDfMmlUKs0
QRadar CE 733 Add an App from the App Exchange (Feb 2020)	https://youtu.be/26OU7cWaRWQ
QRadar CE 733 Intro to Rules Offense and Searches (Feb 2020)	https://youtu.be/6sJf4ElrWqY
I do not see logs or flows in the console (tcpdump) (Feb 2020)	https://youtu.be/VpYjAmOazm4
QRadar CE on Virtual Box (Feb 2020)	https://youtu.be/0zqXknGNwio
Hide Internal QRadar Logs (Feb 2020)	https://youtu.be/tviLbBMgzeQ
My QRadar CE Stopped Collecting Logs (Jan 2021) (**2:11**)	https://youtu.be/FYtIAtiB6yE

Writing Custom Rules

Modifying a Rule by using Building Blocks (tuning) (Jan 2022) (**13:50**)	https://youtu.be/jCClK6Orc-I
Why Building Blocks? (Jan 2022) (**8:05**)	https://youtu.be/PcyPhjyxV-U
Why do I care about Remote to Remote Context (Jan 2022) (**2:41**).	https://youtu.be/DaghOzBRKiI
Creating Custom Rules Part 1 Windows Example (May 2021) (**18:20**)	https://youtu.be/r7EwxfNBrKo
Creating Custom Rules Part 2 Other Rule Tests (May 2021) (**6:48**)	https://youtu.be/IsvflrnLcik

Security Intelligence Tutorial, Demo & Use Case Videos

Creating Custom Rules Part 3 Payload Contains (May 2021) (**5:30**) https://youtu.be/v_q68FwbjzQ
Creating Custom Rules Part 4 Context, domains, etc (May 2021) (**4:30**) https://youtu.be/0dYwDkUTmLM
Creating Custom Rules Part 5 Counters, tables, times (May 2021) (**5:09**) https://youtu.be/4sEGa4sBfw8
Creating Custom Rules Part 6 Rule's Performance (May 2021) (**15:00**) https://youtu.be/Rx54prdvSxM

Pulse

Pulse Dashboards Included in QRadar Apps (Nov 2021) (**1:56**) https://youtu.be/87rd9jBidlw
Monitoring WinCollect Agents with Pulse (Apr 2021) (**5:20**) https://youtu.be/4k_H5PxUOTc
Pinning Pulse Dashboards (Sept 2020) https://youtu.be/adrNTphGrU0
Pulse Dashboard Log Source Auditing (Sept 2020) https://youtu.be/8UYdPFMnyUw
Convert Reports to Pulse without AQL knowledge (Sept 2020) https://youtu.be/5wrd3S9foYs
Drilling down in Pulse Dashboards (July 2020) https://youtu.be/t7yUUpAT7bI
Making API Calls from Pulse, Part One (June 2020) https://youtu.be/SS-6xDzgn3k
Making API calls from Pulse, Part Two (June 2020) https://youtu.be/h9fNpjE-2Dc
Pulse 2.4 New Workflow Part One (June 2020) https://youtu.be/vm3Pmf8hLI4
Pulse 2.4 New Workflow Part Two (June 2020) https://youtu.be/Q9M6harUxDc
Great Searches Pulse Dashboards with input parameters (March 2020) https://youtu.be/Ci6VJ6oifls
Building our first Pulse Dashboard with input parameters (March 2020) https://youtu.be/UUqGixIz8zo
Finishing the first Example and invitation to share (March 2020) https://youtu.be/27Sa-U15-Iw
Exporting a Pulse Dashboard as a JSON file (March 2020) https://youtu.be/uwQvH1sgvXQ
Adding dashboards to QRadar's Pulse (Feb 2020) https://youtu.be/YXCvUMweUks
How to cheaply do expensive searches in Pulse GlobalViews (April 2020) https://youtu.be/HcYnMzniR5c
GlobalViews from existing accumulators (April 2020) https://youtu.be/0uTlFx9GAPs
Building an AQL Search in flows (April 2020) https://youtu.be/YBPQsisJWG4
Building an AQL Search in logs (events) (April 2020) https://youtu.be/K6BAdzP4XOk
Userids for Pulse and Sharing Dashboards (April 2020) https://youtu.be/M5A7_89lVTE
Using Geo Location in Pulse (April 2020) https://youtu.be/ZOoFjib77kM

Cloud Pak For Security

My take on Could Pak For Security, May 2021 Part One (**9:59**) https://youtu.be/icYT4qNRKOs
My take on CP4S, May 2021 Part Two: Threat Investigator (**9:59**) https://youtu.be/5QFgmHnNieU
My take on CP4S, May 2021 Part Three: Playbook Designer (**10:59**) https://youtu.be/ncL8I9NkTRM
Selling the value of CP4S to Qradar customers (Aug 2020) https://youtu.be/RlDnsqxI2_g
Connecting Cloudpak to my local QRadar instance (Aug 2020) https://youtu.be/2Y5C0aG8UFU
Connecting Cloudpak to CarbonBlack (Aug 2020) https://youtu.be/LJC22eLVlsw
Introduction (July 2020) https://youtu.be/65qKEkMC_VU
Use Case One (July 2020) https://youtu.be/kGruzAEzric

Use Case Manager App

Simple Tricks To Improve your QRadar Part One (Feb 2021) (**8:56**) https://youtu.be/uV9TWATnROY
Simple Tricks To Improve your QRadar Part Two (Feb 2021) (**4:44**) https://youtu.be/duE7XImPIYk
UCM V3 Tutorial Intro and Navigation (Oct 2020) https://youtu.be/ndnhNacHrkk
UCM V3 Tutorial Recommended Apps and Log Sources (Oct 2020) https://youtu.be/6N9zeUJ2wCk
UCM V3 Tutorial Improving QRadar without spending a penny (Oct 2020) https://youtu.be/Ux_0cHIstsg
UCM V3 Tutorial Making the case for additional log sources (Oct 2020) https://youtu.be/H2HjxTGmC28
UCM V3 Tutorial Log sources per Rule(Oct 2020) https://youtu.be/C36nALRfxOI
UCM V3 Tutorial Using filters (Oct 2020) https://youtu.be/IbJLvXQuw2M
UCM V3 Tutorial MITRE Part One (Oct 2020) https://youtu.be/iTVOhYpp7Dc
UCM V3 Tutorial MITRE Part Two (Oct 2020) https://youtu.be/WwywPCFN4wo

Security Intelligence Tutorial, Demo & Use Case Videos

Use Case Manager App V2.3 Part One (June 2020)	https://youtu.be/lnu0F41CiWY
Use Case Manager App V2.3 Part Two MITRE (June 2020)	https://youtu.be/PrIaFFExJ6M
UCM V3 Tutorial - MITRE Part Three (3:15) (Oct 2020)	https://youtu.be/zzLQES3LQqM
QRadar Tuning tips from Alaa Part One, Introduction (April 2020)	https://youtu.be/s4PX5UFI9y8
QRadar Tuning Tips from Alaa, Part 2 Eliminate Noisy Offenses (April 2020)	https://youtu.be/P-9qGSDijx8
QRadar Tuning Tips from Alaa Part 3, Rules with many events (April 2020)	https://youtu.be/FqciXq-R-8U
QRadar Tuning Tips from Alaa Part 4, Network Hierarchy (April 2020)	https://youtu.be/aOzuVCOLn-I
QRadar Tuning Tips from Alaa Part 5, BB and Reference Sets (April 2020)	https://youtu.be/ffU-8Mqjzdk
Use Cases App, Mining your Rules (Oct 28, 2019)	https://youtu.be/vqVOVZ6Rm6M
Finding uninstalled Rules (Aug 2021) (**1:44**)	https://youtu.be/y9QvlRYu-cI
No Need to Leave the UCM (Sep 2021) (**1:03**)	https://youtu.be/ueAP-d_fj5k

Art of the Possible Demo Topics

Ease of Ingestion of Data and Fast Value in QRadar **(7:06)** (Oct 2020)	https://youtu.be/fIqsQ8BsXG4
The Value of Advisor **(9:49)** (Oct 2020)	https://youtu.be/yGUti00XO14
The Value of Standard Flows **(7:09)** (Oct 2020)	https://youtu.be/-HhbOiLNj9E
The Value of QNI **(11:30)** (Oct 2020)	https://youtu.be/0og_UH_4Wk4
Why Additional EPSs **(3:03)** (Oct 2020)	https://youtu.be/c9TQNrLTv_w
The Value of Plain Vanilla UBA **(10:28)** (Oct 2020)	https://youtu.be/-kd0DAvEXvc
The Value of UBA with Machine Learning **(6:00)** (Oct 2020)	https://youtu.be/vErSuyDP6r0
The Value of a Real Time Correlation Engine **(11:39)** (Oct 2020)	https://youtu.be/Hcaq7mhvALE
Does it make sense to feed QRadar with scan data? **(4:39)** (Oct 2020)	https://youtu.be/n3oZ-z2nJz0

QRadar and MITRE

UCM V3 Tutorial MITRE Part One (Oct 2020)	https://youtu.be/iTVOhYpp7Dc
UCM V3 Tutorial MITRE Part Two (Oct 2020)	https://youtu.be/WwywPCFN4wo
UCM V3 Tutorial - MITRE Part Three (3:15) (Oct 2020)	https://youtu.be/zzLQES3LQqM
Use Case Manager 2 3 Part Two MITRE (June 2020)	https://youtu.be/PrIaFFExJ6M
QRadar and the MITRE Attack Framework (March 2020)	https://youtu.be/933JZ262OVU

Searching in QRadar

Search Performance: Quick Filters (Log4J example) (Dec 2021) (**12:09**)	https://youtu.be/3I7402aek98
Search Perf: Regex and AQL Functions (Log4J example) (Dec 2021) (**12:09**)	https://youtu.be/DFs7plpt7Sc
Analyst Custom Searches (March 2021) (**2:37**)	https://youtu.be/Wfv5vPN83V8
Ariel Searches (May 30, 2019)	https://youtu.be/26OU7cWaRWQ
Quick Filter (May 30, 2019	https://youtu.be/Rhzs1DghZYs
Filtering in Log and Network tabs (June 27, 2019)	https://youtu.be/jlD5cYLpqXI
Building an AQL Search in flows (April 2020)	https://youtu.be/YBPQsisJWG4
Building an AQL Search in logs (events) (April 2020)	https://youtu.be/K6BAdzP4XOk
Learning Ariel Query Language (June 12, 2019)	https://youtu.be/VNpGVPZO9DA
Two Random tips on searches (April 18, 2019)	https://youtu.be/7UChqiTzrzs
AQL Translator (Feb 22, 2019)	https://youtu.be/4ZrQ68TFgt0
Investigating Search times with QDI (June 10, 2019)	https://youtu.be/HgC_YTtG3G0
Logical OR Searches (Aug 2,2019)	https://youtu.be/CjRwUJL8vGI

Securing your networks at home or small office (pfSense)

IBM released a NetGate pfSense DSM (Sept 2020)	https://youtu.be/ajWl-pAamTo
Perhaps the best lab for learning Cyber Security (Dec 2019)	https://youtu.be/aRVJmlqXAdQ
Segmenting your networks with pfSense (May 2019)	https://youtu.be/FPgPHJvLmh0

Security Intelligence Tutorial, Demo & Use Case Videos

Create you very own and secure VPN at home (Dec 2019)	https://youtu.be/V9znn_z_4W4
Why I am so happy I replaced my ISP router at home (June 2019)	https://youtu.be/Y8mA-BN_clQ
Use The Free QRadar CE to Monitor your Home's Network (Flows) (May 2019)	https://youtu.be/iPAA-Y-sXPg
Filtering in Log and Network tabs (June 26, 2019)	https://youtu.be/jlD5cYLpqXI
A simple way of adding the DSM via Content Extension (May 2020)	https://youtu.be/blGMaj8Pus0
Installing the pfSense DSM: (June 2019)	https://youtu.be/QWkXix8v_LY
Enabling pfSense to send logs to QRadar (June 2019)	https://youtu.be/8X8unbbMFmw
Using the DSM Editor to create a pfSense parser (June 2019).	https://youtu.be/gN7JMpbuAy0
Exporting the pfSense DSM using the Content Management Tool (June 2019)	https://youtu.be/BddAxDuddO8
Resetting your pfSense password (May 2019)	https://youtu.be/e3Z6wScMVsU
Update Backup and Restore in PFSense (May 2019)	https://youtu.be/uD878Tf7kpY
Small tip to increase privacy at home with pfSense (May 2019)	https://youtu.be/gJMs7ZwXfrg
Segmenting with pfSenses uses VLANs (May 2019)	https://youtu.be/EdgZcvu9CwI_
Recovering a broken NetGate router (June 11, 2019)	https://youtu.be/LevrnBYLWLw
Getting Proxy Logs (Squid) from pfSense (June 27, 2019)	https://youtu.be/ylOXMlN15zQ
Getting Proxy Logs (Squid) from pfSense with SSL interception (June 27,2019)	https://youtu.be/QTpPzgHN8P0
pfSense SSL interception can break some things (July 9,2019)	https://youtu.be/rxD8tI42RlQ
Getting long URLs from pfSense Squid logs (July 9, 2019)	https://youtu.be/CLt4Q-d6FY8
Getting pfSense logs from allowed traffic (July 9, 2019)	https://youtu.be/AgA_Q4RrMJ0
A malware infection and propagation in my home network (Aug 1,2019)	https://youtu.be/ibcZWi9Vlds
You get more than you asked for when browsing (Aug 2,1019)	https://youtu.be/Hl66cNo0hzE
DNS Security (Aug 2, 2019)	https://youtu.be/rRYZWxLFu98
Packet capture (pcap) from pfSense (Aug 8,2019)	https://youtu.be/S3VGlVJP5Ns
Back to basics DHCP in pfSense (Aug 2019)	https://youtu.be/WIjqG3x-dbU
Back to basics Gateway, DNS and Proxy (Aug 2019)	https://youtu.be/insx5oJAUA8
Back to basics Blocking bad traffic (Aug 2019)	https://youtu.be/wAZnSG-5o74
Back to basics Linux networking definitions (Aug 2019)	https://youtu.be/CEg7rrOttx8
Enhancing pfSense DNS Log Collection (Aug 2019).	https://youtu.be/8c6jKc1aSlc
Build your own pfSense Box (Aug 1019)	https://youtu.be/m61hkWCHuQw
What do you get with the free QRadarCE and pfSense at home (Sept 2019).	https://youtu.be/bE9UpEzFgu8
Keep video games working with pfSense (Sept 2019)	https://youtu.be/uySEsfhxEu0
Adding Free Packages to your QRadarCE (Sept 2019)	https://youtu.be/5B6VOfTZOd0
Port Forwarding in pfSense (Dec 2019)	https://youtu.be/Z62AWF_B2jo
Upgrading The Speed of my Home Internet (Jan 2021) **(11:56)**	https://youtu.be/iQg_EB4w14k
Blocking All Traffic From Bad Countries Part 1 Intro (June 2021) (**11:24**)	https://youtu.be/kf8JqE0kV-Q
Blocking All Traffic From Bad Countries Part 2 Intro (June 2021) (**9:28**)	https://youtu.be/--0cjeEzdqU
Blocking All Traffic From Bad Countries Part 3 Intro (June 2021) (**6:42**)	https://youtu.be/d0tqLSJJrNY
Blocking All Traffic From Bad Countries Part 4 Intro (June 2021) (**5:24**)	https://youtu.be/EgD8vaVXZ3A
Investigating Offenses at Home (June 2021) (**7:29**)	https://youtu.be/5jUTgtfPDZ8
Blocking Traffic from Specific IPs in pfSense (July 2021) (**2:32**)	https://youtu.be/H-2TIESD7PI

Impossible Travel Rules

Impossible Travel Rules Part One (Sept 2021) (**12:46**)	https://youtu.be/BgHTrcOFrnk
Impossible Travel Rules Part Two (Sept 2021) (**9:40**)	https://youtu.be/6vveOBQKSpY

How Parsing works in QRadar

Custom Event Properties (Oct 2021) (**15:51**)	https://youtu.be/W2XuNKIAUJg
Introduction (April 2020)	https://youtu.be/MP6grxJvxn0
Can QRadar write the Regex for me? (Oct 2020) (1:28)	https://youtu.be/05o8On-ufYk
Basic QRadar Tutorial Part One Offenses (Oct 2020) (**17:25**)	https://youtu.be/4tY7zf5LDkk
Basic QRadar Part Two How a DSM works (Oct 2020) (**17:14**)	https://youtu.be/kkp4uKy9m6c
Basic QRadar Part Three Creating a custom DSM (Oct 2020) (**20:24**)	https://youtu.be/XuibdLyPrsM
Basic QRadar Part Four Closing Remarks (Oct 2020) (**3:36**)	https://youtu.be/gR62JFGLPoc
Do I have the right DSM Parser installed? (April 2020)	https://youtu.be/keF6FLqizmM
SIM Generic (April 2020)	https://youtu.be/Lc5h5fQdfmk

Stored and Unknown (April 2020)	https://youtu.be/GgPW5OVwoMY
DSM Tutorial Part One (Jan 24 2018)	https://youtu.be/LRhNMejQFNM
DSM Editor Tutorial 2020, JSON (Dec 2019)	https://youtu.be/8f86_yEWOj4
DSM Editor Tutorial 2020, CEF JSON and LEEF (Dec 2019)	https://youtu.be/8vIjcFcuoXs
Parsing Order Intro (April 2020)	https://youtu.be/H2G9o6CHF-8
Parsing Order Examples (April 2020)	https://youtu.be/AnbVb5UlXZg
Syslog Redirect (April 2020)	https://youtu.be/c-JXGGhhHwE
QRadar DSM Editor Tutorial in less than 10 minutes	https://youtu.be/KF40bba_kp0
Be mindful of property's format (April 2020)	https://youtu.be/DnqEXnBboiI
Parsing Setting the Lab (April 2020)	https://youtu.be/nh4_VOoojwk
No more RegEx for Custom Event Properties (Aug 7,2018).	https://youtu.be/DSgIENJSPRs
AQL Custom Properties (Aug 10, 2018)	https://youtu.be/f7pMsh3lPXE
Regex Cheat Sheet (Oct 2020) (**6:39**)	https://youtu.be/opGXUfSDGjg

Universal Cloud REST API Protocol

Universal Cloud REST API Protocol Part One (Sept 2020)	https://youtu.be/fqoank4ZtRA
Universal Cloud REST API Protocol Part Two (Sept 2020)	https://youtu.be/MqSxJShrHDg
Microsoft Cloud Application Security App logs (Feb 2021) (**8:55**)	https://youtu.be/f59ypmChFbM

ESXi

ESXi Networking Introduction	https://youtu.be/tsgdXS38GGw
Enabling copy paste in ESXI VCenter VSphere	https://youtu.be/KJLaQZGLeOc
Installing pfSense on ESXi	https://youtu.be/9k1bNbNkN58

Detecting Attacks on Domain Controllers with Just Plain Windows Logs

Golden Ticket Attack Detection (Dec, 2019)	https://youtu.be/qR5jw2f0RzA
Over Pass The Hash and Domain Sync (Dec 2019)	https://youtu.be/Ao7D9GBhv8c
Remote in memory attack without any user interaction (Dec 2019)	https://youtu.be/o-_DwZuDCU8
Query Remotely using Pass The Hash (Dec 2019)	https://youtu.be/NLUbANm9ODA
Session Enumeration (Dec 2019)	https://youtu.be/i879fwk9VuM

SysFlow Cloud Security

What this series is all about (Dec 2020) (**2:54**)	https://youtu.be/jRphiwWBxdU
Kubernetes Whiteboard Intro (March 2020) (**12:15**)	https://youtu.be/X1wogDXA2Fg
SysFlow Whiteboard Intro (Dec 2020) (**17:22**)	https://youtu.be/buXSmrYwM-k
SysFlow Container Awareness (Dec 2020) (**5:00**)	https://youtu.be/rLosUF65IPg
SysFlow Detecting an Attack on a Host (Dec 2020) (**4:03**)	https://youtu.be/P5hCl4WN1qg
SysFlow Detecting a Compromised Kernel from a Container (Dec 2020) (**6:00**)	https://youtu.be/5nRVRXX8d-g

Support

How to request QRadar support from IBM (March 2021) (**1:25**)	https://youtu.be/KolnelCtT2g
Speed up ticket resolution on log sources (June 2020)	https://youtu.be/c9kCUx3xG_E
Security Tokens and API Keys in QRadar (July 2020)	https://youtu.be/N-Mvqnf8jIM

AWS Security Tutorial

AWS Elastic Kubernetes Services Logs into QRadar (May 2021) (**7:50**)	https://youtu.be/DvfssQKfy9Y
Installing AWS CLI and EKSCTL (May 2021) (**7:06**)	https://youtu.be/W4u2kvtwD_k
S3 Bucket, SQS and VPC Flow Log for QRadar (April 2021) (**6:57**)	https://youtu.be/SFwkYnT_8I4

Security Intelligence Tutorial, Demo & Use Case Videos

VPC Flows from AWS in QRadar (April 2021) (**7:55**) https://youtu.be/qOTJ5nXDVcU
AWS WAF Configuration for QRadar and More (April 2021) (**9:04**) https://youtu.be/pVlOnPducEI
QRadar in a Hybrid Cloud Environment, Part One (March 2021) (14:18) https://youtu.be/xK-8k5FJNJo
QRadar in a Hybrid Cloud Environment, Part Two (March 2021) (8:36) https://youtu.be/6V8W128p3FU
AWS Security Tutorial AWS Dictionary (July 2018) https://youtu.be/iLg40tUQKi4
Getting Cisco Umbrella S3 Bucket Logs in QRadar (July 2018) https://youtu.be/NC6G51D96Zs
AWS Security Tutorial S3 EC2 Cloudtrail and IAM (July 2018) https://youtu.be/mTnuqlxSCfo
AWS Security Tutorial CloudWatch Log Groups (July 30, 2018) https://youtu.be/Gh6SBT3gQT0

QRadar running inside AWS:

Console 7.4.1 in AWS (Dec 15, 2020) (**11:18**) https://youtu.be/73tdzuqteoQ
Console 7.3.2 in AWS (July 8, 2019) https://youtu.be/6VZRp158ETs
App Host 7.3.2 in AWS (July 8, 2019) https://youtu.be/wYRpnC7fgsE
Managed Host 7.3.2 in AWS (July 8, 2019) https://youtu.be/SF6aiXJuy9k
Creating a QRadar 7.3.1 instance (console) in AWS (March 29, 2019) https://youtu.be/oYfiVpUtyCk
Creating a QRadar 7.3.1 Managed Host in AWS (March 29, 2019) https://youtu.be/-vdLklkskdM

QRadar in Azure:

QRadar 733 console in Azure (Feb 2020) https://youtu.be/meolwp7knK4
QRadar 7.3.3 Managed Host in Azure (Feb 2020) https://youtu.be/ono1sVOKIBo
QRadar App Host deployment in Azure (Feb 2020) https://youtu.be/e6o8a_Sbf8
QRadar 733 console in Azure (Feb 2020) https://youtu.be/meolwp7knK4
QRadar 7.3.3 Managed Host in Azure (Feb 2020) https://youtu.be/ono1sVOKIBo
QRadar App Host deployment in Azure (Feb 2020) https://youtu.be/Qe6o8a_Sbf8
Creating a QRadar Instance in Azure (Console) (Nov 9,2018) https://youtu.be/bF2UtqnSTTA
Creating a QRadar Managed Host in Azure (Nov 9,2018) https://youtu.be/jGScZIoPj_U
Generating Key Pairs for Authentication (Nov 9,2018) https://youtu.be/tjLbyKkXnBw

QRadar in Google Could:

QRadar Console Deployment in Google Cloud (Nov 2019) https://youtu.be/MIqj7D1VDw0

QRadar logs from IBM Cloud:

Configuring IBM cloud and QRadar to get logs (Nov 2021) (**14:27**) https://youtu.be/4vVHJOCK12A

osquery:

osquery Introduction (Feb 2020): https://youtu.be/_bsPifjRy6g
osquery 1 Why getting OS logs is not good enough (Feb 2020): https://youtu.be/weh5jOwmDww
osquery Part 2 installation and initial configuration(Feb 2020): https://youtu.be/0bx9ZiW7C_o
osquery Part 3 getting the logs to QRadar using syslog-ng (Feb 2020): https://youtu.be/SmfAO5yECa0

osquery Part 4 parsing osquery and standard Linux logs (Feb 2020): https://youtu.be/5OWvyJWScBs

Modern Dashboards in QRadar:

Adding dashboards to QRadar's Pulse (Feb 2020). https://youtu.be/YXCvUMweUks

New Pulse App, Quite an evolution (April 18,2018) https://youtu.be/ScFJny5zIIE

New Pulse App, Quite an evolution, Part 2 (April 18,2018) https://youtu.be/SCE_iV_qa4c

New Pulse App, Quite an evolution, Part 3 (April 18,2018) https://youtu.be/wphgfJBwk58

X-Force and QRadar

X-Force and VIRUSTOTAL Free Integration (June 2021) (**2:18**) https://youtu.be/A6WPqH1iAf0

The New Threat Intelligent App (Sept 2020) https://youtu.be/eRC1HQx2CoE

Am I Affected Part One (March 5,2017) https://youtu.be/-yWepLFePJI

Am I Affected Part Two (May 13, 2017) https://youtu.be/Vk2UF7c2xUM

Am I Affected Part Three (May 25, 2017) https://youtu.be/fosokuYIVrA

QRadar 7.3.2 Migration from AppNode to AppHost

Part 0 (Feb 12, 2019) https://youtu.be/HACJiafw5Jo

Part 1 (Feb 12, 2019) https://youtu.be/ONvpikqpge8

Part 2(Feb 12, 2019) https://youtu.be/Pz1z37OyBYQ

QRadar on Cloud (QRoC)

Almost all QRadar Apps can now work with QRoC (July 29,2019) https://youtu.be/rVjLGHBaN0w

QRoC and QRadar on Prem Part 1 (Nov 15,2018) https://youtu.be/-R9ZXTpZB9k

QRoC and QRadar on Prem Part 2 (Nov 15,2018) https://youtu.be/q_knbPROXcM

Steps to deploy a QRoC Data Gateway in Azure (Feb 2019) https://youtu.be/8eJkWDqr9Xc

DataGateway on Prem Part One (Aug 2019) https://youtu.be/h-J4xadlqc0

DataGateway on Prem Part Two (Aug 2019) https://youtu.be/_HmE6sNPmZY

Getting Logs When Systems are in the Cloud:

More Hybrid Cloud Use Cases (June 2021) (**1:21**) https://youtu.be/Wsc78Ji_ijQ

Cloud Visibility App 1.4.0 (October 2020) (**8:43**) https://youtu.be/JWoizGq2Z4k

Update on Office365 Capabilities (Sept 2019) https://youtu.be/LrSB-I9Rywo

Steps to deploy a QRoC Data Gateway in Azure (Oct 2019) https://youtu.be/8eJkWDqr9Xc

Cloud Visibility and content extensions (Oct 16, 2018) https://youtu.be/GrQCCyBqTnQ

Akamai DSM now supports REST API (Aug 1, 2018) https://youtu.be/MyQ81rwlI6w

Cisco Umbrella (S3 Buckets) (May 10,2018) https://youtu.be/NC6G51D96Zs

SAP logs via API Part One (May 10, 2018) https://youtu.be/MzDedjxZ9HM

SAP logs via API Part Two (June 13, 2018)	https://youtu.be/Rc8PsG9odts
Azure Event Hub (March 8, 2018)	https://youtu.be/SylTklpn2ko
Office 365 (March 31, 2017)	https://youtu.be/km-2mMR6nCc
Box (March 16,2017)	https://youtu.be/8g2AjsM9Q2g

Migration from other SIEM to QRadar (Nov 2017)

Syslog Redirect sending ArcSight logs to QRadar	https://youtu.be/y2xIEkGjV1g

QRadar Community Edition (Sept 2018)

Introduction (Sept 1,2018)	https://youtu.be/bbuquuVOXos
CentOS installation (Dec 2, 2018)	https://youtu.be/V7I0jWanKiw
QRadar 7.3.1 Community Edition Install (Sept 1, 2018)	https://youtu.be/2ButNPY4nLQ
Script to make the CE installation even easier (Oct 1, 2018)	https://youtu.be/F6_PI7BJ2RY
Finding DSMs in Fix Central/iso image (Nov 27,1018)	https://youtu.be/m0QghmLIF20
Adding a DSM	https://youtu.be/acwq1c1XXwA
Very Basic Searches	https://youtu.be/bqhPWQoBaMw
Advanced Searches	https://youtu.be/xf5RFFbkneI
App Exchange	https://youtu.be/UX3MICfP4k4
Network Hierarchy	https://youtu.be/QI_8mQFGdXE
Adding Flows	https://youtu.be/AJovcvi07nw
Dealing with offenses	https://youtu.be/D6qOSG2-k7M
Adding X-Force Thread Feeds	https://youtu.be/YkREukAOqts
Where to look for additional information	https://youtu.be/5jxWB2RzDtw
Opening ports in QRadar Community Edition	https://youtu.be/KN1A0DwfgoA

QRadar Deployment Architecture

Using 'awk' and zgrep commands (Jan 2021) (**9:28**)	https://youtu.be/wWClk7qp3BQ
Using the 'less' , 'grep' and tail commands (Jan 2021) (**10:07**)	https://youtu.be/yFlCLqV07Ds
Counting Events Per Second EPS (Jan 2021) (**6:55**)	https://youtu.be/hE242wXCqWY
Checking QRadar's Overall Performance in a pinch (Jan 2022) (6:48)	https://youtu.be/Wc6sgKcH9Kg
Dealing with Expensive Searches (Jan 2022) (**8:20**)	https://youtu.be/n06MLLMe_TM
Historical Correlation (Aug 2021) (**5:13**)	https://youtu.be/8AxtgMNwma0
More Hybrid Cloud Use Cases (June 2021) (**1:21**)	https://youtu.be/Wsc78Ji_ijQ
Make sure your Geo Location (Maxmind) is updated (Oct 2020) (**1:46**)	https://youtu.be/h1-PZiKhvGg
Controlling Access in QRadar's Console (May 2021) (**4:27**)	https://youtu.be/rCEjkAkeLfU
Monitor and Notify About QRadar Resources (May 2021) (**2:31**)	https://youtu.be/oNyrSYlscnM
Monitoring QRadar CPU usage in a pinch (Feb 2021) (**7:53**)	https://youtu.be/J6_Zx-sJjo4
Checking QRadar's Overall Performance in a pinch (Jan 2022) (**6:48**)	https://youtu.be/Wc6sgKcH9Kg
Install or Update your QRadar Licenses (June 6, 2019)	https://youtu.be/sLu8N76KDNE
Auto Discovery: very useful but not perfect (April 11,2019)	https://youtu.be/1oNbPBJepeM
Linux logs autorecognized by QRadar (April 10,2019)	https://youtu.be/Dmf2iwRqATI
Why send NetFlows to QRadar (March 13, 2019)	https://youtu.be/u1f3igbUMDc
QRadar's support for VLANs (March 8, 2019)	https://youtu.be/I9yrixNvVvA
Disconnected Log Collector DLC Part One (March 1, 2019)	https://youtu.be/SAVQSOikqTk
Disconnected Log Collector DLC Part Two (March 7, 2019)	https://youtu.be/n1RSDxtyEV8
Mapping Flows to Applications, Part 1 (Jan 17,2019)	https://youtu.be/JshLLIzSEAw
Mapping Flows to Applications, Part 2 (Jan 20,2019)	https://youtu.be/qiogrzRXApk
Mapping Flows to Applications, Part 3 (Jan 23,2019)	https://youtu.be/OvP0lVpbOhE
Log Sources App V3 (Jan 11, 2019)	https://youtu.be/d3-JZGT-XhA

Security Intelligence Tutorial, Demo & Use Case Videos

Logs Sources App V4 (June 12,2019) https://youtu.be/Q2ShsY1JMbY
Monitoring QRadar appliances with QDI (May 6,2018) https://youtu.be/r9L79n4Ll_U
New QDI versión (June 2021) (**3:40**) https://youtu.be/URawlbj2clc
QRadar Flow License Give Back (Dec 18, 2018) https://youtu.be/TwMUy9zo0O4
QRadar Data Store (April 30, 2018) https://youtu.be/ainft09Q0ls
QRadar On Cloud (QROC) (Jan 23,2018) https://youtu.be/8KQjUrw1JnA
Deployment Architecture Part One (Jan 11, 2018) https://youtu.be/pl85saA_4BU
Deployment Architecture Part Two (Jan 11, 2018) https://youtu.be/CrCm5grwLRI
Deployment Architecture Part Three Cloud (Jan 19, 2018) https://youtu.be/63LYYSBpTeQ
AppNode Part One – Preparing the OS (April 5, 2018) https://youtu.be/wCKGffUK8Qk
AppNode Part Two – Moving the Apps (April 5, 2018) https://youtu.be/YmP3abXmRvU
Bulk Editing Log Sources (July 30, 2018) https://youtu.be/R9nzDaMTYI0
No more RegEx for Custom Event Properties (Aug 7,2018) https://youtu.be/DSgIENJSPRs
This is getting ri·dic·u·lous·ly easy (Aug 8,2018) https://youtu.be/X5fzAE-UH3w
Reference Maps (Aug 10,2018) https://youtu.be/G1oGtppC3Sg
AQL Custom Properties (Aug 10, 2018) https://youtu.be/f7pMsh3lPXE

Regular Expresions RegEx

Regex Cheat Sheet (Oct 2020) (**6:39**) https://youtu.be/opGXUfSDGjg
Regex for Security Introduction (Jan 2022) (**6:52**) https://youtu.be/ITsTQfyrfIs
Regex for Security Example Two (Jan 2022) (**5:24**) https://youtu.be/ZmzbTvVEf_c
Regex for Security Greedy and Lazy (Jan 2022) (**8:53**) https://youtu.be/Iept4u881vU
Regex for Security Example Four (Jan 2022) (**9:42**) https://youtu.be/c2qAY8v8vGI
Regex for Security Part Five case insensitivity (Jan 2022) (**2:20**) https://youtu.be/AFW3jKI10DA
Regex for Security Part Six two more examples (Jan 2022) (**5:15**) https://youtu.be/o2PZ_DTXN5A
Can QRadar write the Regex for me? (Oct 2020) (**1:28**) https://youtu.be/05o8On-ufYk
My demonstration a AQL Series Payload, Regex Searches (2017) https://youtu.be/_9_JgEPbZvU
Search Perf: Regex and AQL Functions (Log4J example) (Dec 2021) (**12:09**) https://youtu.be/DFs7plpt7Sc

QRadar and Sysmon (from SysInternals)

My demonstration at Think 2019 (Feb 14,2019). https://youtu.be/FQcV3Ja1x3M
Sysmon Introduction (Aug 7,2017) https://youtu.be/Xl31zNp4YUY
Sysmon PoweShell Use Case 1 (Aug 7,2017) https://youtu.be/PWiw-RpLIbw
Sysmon PowerShell Use Case 2 (Aug 7,2017) https://youtu.be/_eaMMo8sPtA
Sysmon PowerShell Use Case 3 (Aug 7,2017) https://youtu.be/sZUAuYpSe7Q
Sysmon Use Case 4 Bogus Windows Process (Aug 15,2017) https://youtu.be/gAS-B9gb3RY
Sysmon Use Case 5 Nasty Injection & Encoded Attacks (Aug 15 2017) https://youtu.be/kC2hIJxqF8Q
Sysmon Use Case 6 Detecting other Libraries (Aug **15, 2017)** https://youtu.be/omWnyACNEcM
Sysmon Use Case 7 Privilege escalation Aug 21,2017 https://youtu.be/yitGRL-WJCM
Sysmon Use Case 8 Privilege escalation Cont. Aug 21,2017 https://youtu.be/8u6G6SEw3kE
Sysmon Use Case 9 More Privilege Escalation Detection (Aug 28) https://youtu.be/0Wy59Otr_Ag
Sysmon Use Case 10 Creating an Admin Account (Aug 28,2017) https://youtu.be/bJgaFSjuMSs
Sysmon Use Case 11 Name Pipe Impersonation (Aug 31,2017). https://youtu.be/pSBQ7NabDUY
Sysmon Use Case 12 Detecting Mimikatz (Aug 31,2017) https://youtu.be/gKa_CZAz3Jc
Sysmon Lateral Movement Detection, Example One (Sept 27,2017) https://youtu.be/IBEIN9sl4Ik
Sysmon Lateral Movement Detection, Example Two (Oct 4,2017) https://youtu.be/whjpScDYaY4
Sysmon Lateral Movement Detection, Example Three (Oct 10 2017) https://youtu.be/7PXzi3pbmFo
Sysmon WinCollect Stand Alone Install & Config (Aug 7,2017) https://youtu.be/4Hx1rm8UX5k
Sysmon Install & Config (Aug 7,2017) https://youtu.be/vqGoXQEK8pA
Sysmon Rules and Funct. Install and Test (Aug 7,2017) https://youtu.be/T5SGPhmIAdw

Security Intelligence Tutorial, Demo & Use Case Videos

Sysmon Kali (Aug 7,2017) https://youtu.be/2816tEAKFuw
Sysmon Patching is not Enough (Aug 7,2017) https://youtu.be/D-_941mrGHI
Sysmon Installation Notes (Aug 31,2017) https://youtu.be/xlu9vD7Nlw0
Deploying Sysmon easily with BigFix (Sept 11,2017) https://youtu.be/580o_c3UYNc
Sysmon Content Pack detecting Badrabbit (Oct 27,2017) https://youtu.be/eyHuf33LD5k
Sysmon and Watson chasing Badrabbit (Nov 16,2017) https://youtu.be/ah8rmpfS6-k

QRadar Content Management Tool (CMT)

Migrating QRadar Content Using CMT Part One (Dec 21, 2017) https://youtu.be/MBoaYUZCnZQ
Migrating QRadar's Network Hierarchy with an App (Dec 25, 2017) https://youtu.be/oT87FrqT6_0
Migrating one Specific Use Case (Dec 26,2017) https://youtu.be/sdduMc-Cnqc

QRadar WinCollect

WinCollect Version 10 A remarkable Update (Oct 2021) (**9:30**) https://youtu.be/BYwhg1T2vSA
Commercial Tool for deploying WinCollect (ScienceSoft) (Oct 2020 (**6:54**) https://youtu.be/RP6G2IEqp6w
Commercial Tool for deploying WinCollect I forgot (Oct 2020) (**0:53**) https://youtu.be/fpJoMmYlhY8
WinCollect 101 (Aug 2019) https://youtu.be/-sMMmuRqiOk
WinCollect Stand Alone (Aug 2019) https://youtu.be/PtV6DtPx4Pc
WinCollect Managed (Aug 2019) https://youtu.be/qH_yiKfhUHY
Piggy Back on WinCollect File Forwarder (Aug 2019) https://youtu.be/2n45wRyT25o

QRadar Multitenancy, Network Hierarchy and Domains

QRadar Mutitenancy (Nov 26, 2017) https://youtu.be/Xrn7q9v3vAk
Basics of CIDR Ranges (Nov 26, 2017) https://youtu.be/MmA0-978fSk

QRadar Tuning and Other Concepts

Use Case Manager App V2.3 Part One (June 2020) https://youtu.be/lnu0F41CiWY
Use Case Manager App V2.3 Part Two MITRE (June 2020) https://youtu.be/PrIaFFExJ6M
QRadar Tuning tips from Alaa Part One, Introduction (April 2020) https://youtu.be/s4PX5UFI9y8
QRadar Tuning Tips from Alaa, Part 2 Eliminate Noisy Offenses (April 2020) https://youtu.be/P-9qGSDijx8
QRadar Tuning Tips from Alaa Part 3, Rules with many events (April 2020) https://youtu.be/FqciXq-R-8U
QRadar Tuning Tips from Alaa Part 4, Network Hierarchy (April 2020) https://youtu.be/aOzuVCOLn-I
QRadar Tuning Tips from Alaa Part 5, BB and Reference Sets (April 2020) https://youtu.be/ffU-8Mqjzdk
Use Cases App, Mining your Rules (Oct 28, 2019) https://youtu.be/vqVOVZ6Rm6M
QRadar Tuning App:
Tile One: Most Active Rules (March 5,2019) https://youtu.be/GzgY4_bcHyw
Tile Two: Rules that dispatch the most events (March 5, 2019) https://youtu.be/aiUEhQJE5qc
Tile Three: Network Hierarchy (March 5, 2019). https://youtu.be/ot5FdH80yH0
Tile Four: Key Building Blocks and Reference Sets (March 5, 2019) https://youtu.be/6GeXj0lZXdM
Installation: (March 7, 2019) https://youtu.be/7KFiGH5SFbU
QLean App (Sept 10,2018) https://youtu.be/_-o_bea872Y
Tuning: Introduction https://youtu.be/xhrYeD3Pxiw
Server Discovery: https://youtu.be/gdQKS9HBEa8
Building Blocks and Reference Sets: (June 14,2017) https://youtu.be/UmKMbfmjqKQ
Network Hierarchy Part One (June 14,2017) https://youtu.be/mNyd8FNns_4

Security Intelligence Tutorial, Demo & Use Case Videos

Network Hierarchy Part Two: (June 14,2017 https://youtu.be/JagB0Ctd7tg
Tuning wrap up (June 14,2017) https://youtu.be/OGiIi39azT4
Visualizing the content of Maps of Set: (Sept 21,2017) https://youtu.be/3QKCWcw7Src

QRadar Network Insights (QNI) and DNS Attacks

Detecting Log4J activity with just QNI. Part One (Dec 2021) (**12:09**) https://youtu.be/3l7402aek98
Detecting Log4J activity with just QNI. Part Two (Dec 2021) (**8:20**) https://youtu.be/DFs7plpt7Sc
Detecting Log4J EXPLOIT with just QNI. Part Three (Dec 2021) (**6:43**) https://youtu.be/fAla98pSTKk
Step by Step Investigation Log4J EXPLOIT QNI. Part Four (Dec 2021) (**14:01**) https://youtu.be/BfkOI8N4Eyo
QNI and Yara - Use Case One (June 2021) (**7:55**) https://youtu.be/jpWVxgLs2js
QNI and Yara - Use Case Two (June 2021) (**2:50**) https://youtu.be/V7RDANatDRo
QNI Tutorial Part One (Feb 2021) (**10:46**) https://youtu.be/LF1pYNVoR4I
QNI Tutorial Part Two (Feb 2021) (**9:56**) https://youtu.be/T0K6_Y6_oaA
QNI Tutorial Part Three (Feb 2021) (**10:08**) https://youtu.be/NkboZ-wmXvI
QNI Tutorial Part Four (Feb 2021) (**9:26**) https://youtu.be/d2qO3pKnwxY
QNI as Software Only (July 2020) https://youtu.be/j06FxWVceuc
Detecting SIGRed CVE 2020 1350 (July 2020) https://youtu.be/LoFN1TWPaHs
UPDATE: QRadar detecting malicious sites related to COVID 19 (marc 2020) https://youtu.be/jcg4ZD625Go
QRadar detecting malicious sites related to COVID 19 (March 2010) https://youtu.be/OMTOWYPTfMw
Detecting the Mozart malware (March 2020) https://youtu.be/C7BCBJHhAwE
Detecting Curve Ball network exploitations CVE-2020-0601 (March 2020) https://youtu.be/b8T92PqKX3M
Flows and Beyond Part One. Introduction: (Jan 2020) https://youtu.be/9TlYAhIpUNs
Flows and Beyond Part Two. QNI: (Jan 2020) https://youtu.be/g3xdXEapsb4
Flows and Beyond Part Three. When all is encrypted: (Jan 2020) https://youtu.be/Qv7zJDWV_9A
Phishing Detection, Investigation and Remediation (Sept, 2019). https://youtu.be/8BiwDvmwKx8
QRadar detecting attacks hiding in DNS traffic (May 2019) https://youtu.be/YLCoMn7awMM
Adding the DNS Analyzer Template to QRadar's Pulse (may 2019). https://youtu.be/kyIf8_FNlUg
Phishing, the attacker's view (Feb 14, 2018) https://youtu.be/tyKWrKUEirI
QRadar Flow Tutorial. Part One (Feb 12, 2018) https://youtu.be/RWf3AmWOk0U
QRadar Flow Tutorial. Part Two (June 14, 2018) https://youtu.be/eYTj9FwpxYo
QRadar Network Insights QNI. https://youtu.be/Kn8eC-L_dbs
Defending against DNS attacks. CyberSentinel. Part One https://youtu.be/7ep5V2sfLjs
Defending against DNS attacks. CyberSentinel. Part Two https://youtu.be/IZVFHM6dYao

QRadar Time Series

Time series Part 1 https://youtu.be/rLPQ1T9eWLA
Time series Part 2 https://youtu.be/6qkIDxtjoFo

QRadar Why isn't my rule firing? Series

The Rule Debugger tool has been ported to QRadar 7.3.1 (Sept 2, 2018) https://youtu.be/4Ebb1uhVmBI
QRadar Why isn't my rule firing? Part 0
You are going to love this troubleshooting tool https://youtu.be/VkwggreENSs
QRadar Why isn't my rule firing? Part 1
How to collect & replay logs https://youtu.be/lBUFRGvfnWs
Replaying Logs that came from the Cloud (Aug 2021) (**3:09**) https://youtu.be/Wg1kmNHfmYs

QRadar Why isn't my rule firing? Part 2.
How to replay flows https://youtu.be/UcVIE8ObWK4
QRadar Why isn't my rule firing? Part 3.
Our first rule https://youtu.be/I-ZP-344xek

QRadar Why isn't my rule firing? Part 4. False Positives	https://youtu.be/LuEEoix4usU
QRadar Why isn't my rule firing? Part 5. Exporting and Importing Rules	https://youtu.be/VWTs3MtUF8M
QRadar Why isn't my rule firing? Part 6. Exporting elements from dev. to production	https://youtu.be/FdO4kFjpcKU
QRadar Why isn't my rule firing? Part 7. Troubleshooting multi test rules	https://youtu.be/nJbFK7OX9es
QRadar Why isn't my rule firing? Part 8. Case Sensitivity and Network Hierarchy	https://youtu.be/xM9iM33vuSA

QRadar Advisor with Watson

QRadar Modern UI Updated (Dec 2021) (**15:53**)	https://youtu.be/GuOjAr5myDY
New UI updated to 1 8 1 (June 2021) (**2:23**)	https://youtu.be/cOJbKHt1bVE
The Value of Advisor **(9:49)** (Oct 2020)	https://youtu.be/yGUti00XO14
QRadar UI and Advisor updates (Oct 2020) (**8:01**)	https://youtu.be/nX38b-NLZBo
Maximizing QRadar Advisor's Value Part One (Aug 2020	https://youtu.be/UT39mm0AevY
Maximizing QRadar Advisor's Value Part Two (Aug 2020)	https://youtu.be/LBBk0crxDRY
How Advisor uses Toxicity and Relevance of IOCs (Feb 2020)	https://youtu.be/dECYx1xpYbA
Speed up Offense Investigations with Advisor (Jan, 2020)	https://youtu.be/htwwuD1qymk
Use case for QRadar Advisor with Watson 2.01 (Jan 4, 2019)	https://youtu.be/63oWxdBc1yw
QRadar Advisor with Watson 2.0 (Dec 2018)	https://youtu.be/7Mp1YAE8Al8
QRadar's Watson Advisor Example (Aug 2,2018)	https://youtu.be/NSXmHLClOVc
Hey Watson, What do you know about this? (April 16, 2018)	https://youtu.be/0-kZjQSK-hU
Configuration and one example (Jan 10, 2018)	https://youtu.be/GilUqT79kaI
Another example. (Jan 10,2018)	https://youtu.be/UY1JbxoKLh0
CozyDuke use case	https://youtu.be/VGEz1mKqtaQ
QRadar Advisor, Beta:	https://youtu.be/2dFd7Y2pTZQ

QRadar Apps

Carbon Black (May 13, 1018)	https://youtu.be/3skRNwGkiy0
Carbon Black (Jan 23, 2018)	https://youtu.be/hN4BatUgI-Q
Rule Explorer (Jan 19,2018)	https://youtu.be/YXC04mzuR5Q

QRadar Use Case Series

Printnightmare (CVE-2021-34527) exploited after patched (July 2021) (2:30)	https://youtu.be/xjwdf5xObHQ
Monitoring UNMANAGED devices when working from home, Trusteer (July 2020)	https://youtu.be/S95heX92sN8
Detecting Squatting with QRadar Searches (June 2020)	https://youtu.be/qSq-QcuwFi4
Detecting attempts to exploit CVE 2020 0601 (Jan 2020)	https://youtu.be/iaK8MDvlibY
QRadar Detecting Sophisticated Attacks on Windows Part One (May 21,1018)	https://youtu.be/YewnFpDw1t4
QRadar Detecting Sophisticated Attacks on Windows Part Two (May 21,1018)	https://youtu.be/_M28_sRIzaY
SMS Notifications from QRadar **July 28**	https://youtu.be/T3OryGDucQg
Pulse 1.0.2 **July 28**	https://youtu.be/7yMm5o7h_0o
Creating a rule that fires with internal comms to C&C (or bad site)	https://ibm.biz/BdrjyD
Monitoring VPN access from countries, you do not do business with	https://ibm.biz/BdrjyR

Security Intelligence Tutorial, Demo & Use Case Videos

Detecting a remote scan followed by attempts to login		https://youtu.be/QewdWiGRHHA
Detecting multiple login failures to compliance servers		https://youtu.be/BRk3JFRB55E
Detecting a chat to a malicious site using non standard ports		https://youtu.be/qa0EMWr9-bA
Detecting UDP scans and getting flows from the IPS		https://youtu.be/Slbe85LU8fI
Phishing Detection, Investigation and Remediation (Sept, 2019)		https://youtu.be/8BiwDvmwKx8
Detecting Phishing e-mails		https://youtu.be/IRsuNX3pKBo
QRadar Detecting DDoS attacks and Superflows		https://youtu.be/dpO8MNzS-UA
Populating Reference Sets from Soltra and other threat sources		https://youtu.be/VaoNMy94f94
Detecting Successful Attacks with QRadar	Part One	https://youtu.be/xr-GHzklr6g
	Part Two	https://youtu.be/Rb0Vo6XznZY
	PartThree	https://youtu.be/rW8QHBLnD1M

QRadar Detecting Phishing & Ransomware

UPDATE: QRadar detecting malicious sites COVID 19 (March 2020)	https://youtu.be/jcg4ZD625Go
QRadar detecting malicious sites related to COVID 19 (March 2010)	https://youtu.be/OMTOWYPTfMw
Phishing Detection, Investigation and Remediation (Sept, 2019).	https://youtu.be/8BiwDvmwKx8
QRadar QNI Quad 9 and Reaper (Dec 22, 2017)	https://youtu.be/KWUpet9Y9Vw
QRadar Flows Detecting Reaper Malwar (Dec 6, 2017)	https://youtu.be/f0kilm-zBNU
Detecting phishing via hashes using QNI (Aug 18,2017)	https://youtu.be/EsqpXIaQlBA
Discover Hidden Malware with QRadar Part 1: Introduction July 2,2017	https://youtu.be/-Wfb5I0pJYg
Discover Hidden Malware with QRadar Part 2: SMB exploit July 2,2017	https://youtu.be/_lwJxHd68jY
Discover Hidden Malware with QRadar Part 3 More July 2,2017	https://youtu.be/1-bvzAIeY_w
Discover Hidden Malware with Part 4: Petya Content Pack July 5,17	https://youtu.be/J5IO3X8GqXQ
Pertya June 28,2017	https://youtu.be/7jC9UCYI7TA
New Petcha Detecting it with QRadar and PAM June 29,2017	https://youtu.be/VJR3SkWXMYE
WannaCry Part 1 IPS and QRadar with before the breach detection	https://youtu.be/pt2KK35TzBY
WannaCry Part 2 WannaCry content pack from App Exchange	https://youtu.be/5YHi1L9Nqfg
WannaCry Part 3 Feed your WannaCry Ref Set from the X-Force	https://youtu.be/vIYk69MYsp8
WannaCry Part 4 QVM detecting WannaCry exploited Vulnerabilities	https://youtu.be/BO5AWlj_qwQ
WannaCry Part 5 Content Pack Update, Payload to Hex and Watson	https://youtu.be/DUSTTQJxEuM
QRadar stopping Ransomware on its tracks. Part 1	https://youtu.be/ENYbSiUsfaE
QRadar stopping Ransomware on its tracks. Part 2	https://youtu.be/mpykyoWlnGI
QRadar stopping Ransomware on its tracks. Part 3	https://youtu.be/CVIBI6SnpgI
QRadar and Bigfix Stop Ransomware (Custom Script Action) Part One	https://youtu.be/P90e4iEJ32s
QRadar and BigFix Stop Ransomware (Custom Script Action) Part Two	https://youtu.be/sJOovKKX_SM
QRadar and Bigfix Stop Ransomware (Custom Script Action) Part Three	https://youtu.be/-hGsYEDBbi8
QRadar and Bigfix Stop Ransomware (Custom Script Action) Part Four	https://youtu.be/k0fKj4jAFXs
QRadar detecting Phishing and Ransomware	https://youtu.be/BTRxRpMMmpI

Detecting Fraud with QRadar

Detecting fraud, Dormant accounts awakening	https://youtu.be/MjS16uP5cHY
Detecting fraud, A URL with key word from a bad IP	https://youtu.be/_ZDj18Swzcg
Detecting fraud, account takeover	https://youtu.be/oUp3HYVrfQU
Detecting fraud, more examples	https://youtu.be/llLQ8DlKhQQ

QRadar User Behavior Analytics

My Take on the Value of UBA in QRadar (July 2020)	https://youtu.be/wrIzPw5_tl8

Security Intelligence Tutorial, Demo & Use Case Videos

Tuning UBA Part One, Tips from Bruno (April 2020)	https://youtu.be/jhTzPUd9HG4
Tuning UBA Part Two, Tips from Bruno (April 2020)	https://youtu.be/gPUibhA53Mg
Protecting cyber employees when working from home (March 2020)	https://youtu.be/fRzQVQbG32I
UBA's Machine Learning in Action (May 2020)	https://youtu.be/bjvdbmOzdRg
A clear use case for UBA and Watson Advisor (June 26,2019)	https://youtu.be/w_UBhmXacp4
Another use case for UBA (June 26,2019)	https://youtu.be/czDA8C4tti0
UBA 3.4 (Oct, 21019)	https://youtu.be/vjf-jXUmOTE
UBA 3.3 (July 25,2019)	https://youtu.be/mSpjQ6uzFyU
UBA 3.2 (April 23,2019)	https://youtu.be/wzf-1v36Bqc
UBA 3.1.0 (Dec 20,2018)	https://youtu.be/3ZRHia3BxkU
Nice UBA + Advisor Lab (Dec 17,2018	https://youtu.be/a__FX8Xgzp4
UBA 3.0 Tuning (Sept 21,2018)	https://youtu.be/Ntc8C0ZVPyg
QRadar UBA 3.0 just released (Sept 21,2018)	https://youtu.be/DKUX4tNES4s
UBA 2.7 (May 28,2018)	https://youtu.be/oXUegVMKClw
UBA 2.5 (Feb 1, 2018)	https://youtu.be/UDp9n5c1YDc
UBA 2.4 (Jan 8,2017)	

https://youtu.be/5WZXsWfi9tc

UBA version 2.0 with Machine Learning	https://youtu.be/RgF1RztR1yg
UBA version 1.1	https://youtu.be/5-VWAIPHZ6w
UBA version 1.2	https://youtu.be/fe3OwEUL7Vc
UBA example launching restricted programs	https://youtu.be/OA5A0pYs93I
Detecting insider threat: USB inserted + bad website visited	https://youtu.be/mV_cFTw__PQ
Custom offenses contributing to UBA risk score	https://youtu.be/BzjCeADp5fo

QRadar Logs from Cloud and Analytics

QRadar Cloud Discovery App Part 1 Discovery (April 19, 2018)	https://youtu.be/lqZT7Yj5ZqU
QRadar Cloud Discovery App Part 2 Analytics (April 19, 2018)	https://youtu.be/lG6UGb0XXtI
QRadar Cloud Analytics App version 1.0	https://youtu.be/1fJPc6jdrq4
Box logs into QRadar	https://youtu.be/8g2AjsM9Q2g
QRadar and Office 365	https://youtu.be/km-2mMR6nCc

QRadar & Resilient

How to deal with Phishing Incidents (May 2020)	https://youtu.be/8nO_xZ3uVRo
QRadar and Resilient Integration Details (May 2020)	https://youtu.be/IntzaM99EUU
Resilient as a Workflow extension to QRadar (May 17,2019)	https://youtu.be/KMuq-WIrztw
QRadar and Resilient - Basic Integration (Aug 5, 2018)	https://youtu.be/xnFLcf8FuCs
QRadar and Resilient - Functions (Oct 10, 2018)	https://youtu.be/bnoVmQCQLNo
QRadar and Resilient - Functions Installation (Oct 10, 2018)	https://youtu.be/29HiTZxeCtg
QRadar for detection and Resilient for resolution (Sept 2019)	https://youtu.be/Pop85sl4fWQ

Some of QRadar's Integration

Securing Kubernetes Deployments with ACS (StackRox) (June 2021) (**5:09**)	https://youtu.be/6bTvwgeYA2Q
IBM Verify (Feb 2021) (**5:32**)	https://youtu.be/zN2HEqcvc4A
Cisco Fire Power: DSM and App (March 2020).	https://youtu.be/AKKsi-1KPQ8
Radar I2 and Resilient working together (Oct 2019):	https://youtu.be/JLTEEvyEr3s
A more elaborated example of QRadar and I2 Integration (Oct 2019):	https://youtu.be/vnxIUjm68hY
DomainTools (Oct 23, 2019)	https://youtu.be/RMfulqzVaMA
SCADA, ICS, OT Integration: Nozomi App (March 27, 2019)	https://youtu.be/pT3Hk9zj3OE
Gigamon App for QRadar (Jan 25,2018)	https://youtu.be/VM3LdrgDU-I
QRadar Splunk App (Sept 21,2018)	https://youtu.be/e21eHgvwnyU

Security Intelligence Tutorial, Demo & Use Case Videos

QRadar + BigFix + Scanner Who is right? (Sept 21,2018) https://youtu.be/WM4gXfGwNaM
QRadar + BigFix Who else got bitten (Sept 21,2018) https://youtu.be/5W1QGTULEt0
QRadar + BigFix Endpoint Inspection (Sept 2018) https://youtu.be/n1pPJ8C-PTk
Best Practices for Protecting Databases (Nov 25, 2017) https://youtu.be/rRaxHotyAQk

AppScan and Qradar

QRadar and AppScan Integration June 20,2017 https://youtu.be/ZkGGuGzhhs4
QRadar and AppScan Integration The Details June 20,2017 https://youtu.be/2FCIYlNqXzQ
BigFix App for Qradar Version 2.0 (Nov 23,2017) https://youtu.be/shuHRzBV1Bw
The Value of QRadar and BigFix Integration (Nov 23,2017) https://youtu.be/gXQMQHzbB-I

QRadar and Bigfix: 3 Reasons in 5 minutes Aug 11, 2017 https://youtu.be/yXErfcfZH04

BigFix App for QRadar Part One https://youtu.be/HXJuoVz_58c
BigFix App for QRadar Part Two https://youtu.be/r98wg1vMGsg

Understand QRadar/BigFix Integration in about 15 minutes:

QRadar and BigFix Integration Part1. Get vuln. data from BigFix https://youtu.be/1YUrzywMFgQ
QRadar and BigFix Integration Part2. Real time vuln. data from BigFix https://youtu.be/zLKQ6CbDTKU
QRadar and BigFix Integration Part3. Getting logs from BigFix https://youtu.be/ZEO6LI5QlAc
QRadar and BigFix Integration Part4. Dashboard in Bigfix Console https://youtu.be/64HMrcS2w00

QRadar IPS & BigFix helping to fight Ransomware & other attacks https://youtu.be/UELw-sZkwjA
Technical Details https://youtu.be/HMs6mjDvwQo
IPS and QRadar Forensics Detecting and investigating Ransomware https://youtu.be/IhSJQT9d8pk

Integration whiteboard

QRadar Network Protection Connector https://youtu.be/73SMeSAXQ4c
Dealing with Vulnerabilities https://youtu.be/chAu5jrYLTs
Data Bases and Mainframes https://youtu.be/JRzlb10NQN4
Using IPSs more effectively https://youtu.be/9qYhANNBNPk
Dealing with Advanced Malware https://youtu.be/uXELdLirLm4
Mobile and Patching https://youtu.be/cHDIwNydkYw
Leveraging Identity Management Intelligence https://youtu.be/8GhnhIUgYy4
Web Access Management https://youtu.be/XbV0O_n5sB8
X-Force https://youtu.be/-lsu--1DPCg
Forensics https://youtu.be/BvTPy9GKHBU

Integration Demos

Guardium Data Encryption also protects your servers against ransomware (Oct 2019) https://youtu.be/Ns9OvWqgNNE
Guardium, IPS and Carbon Black (Jun 2017) https://youtu.be/XYHnumgJFcM
Part One https://youtu.be/iHaHS9xTsXE
Part Two https://youtu.be/cRavhpqfVqs
Part Three https://youtu.be/7pWRqYtNdRU
Part Four https://youtu.be/lQE_WEG22WY
Part Five https://youtu.be/aUqflef8Uog
ISIM and QRadar Integration examples https://youtu.be/YvbNlQ4lf-Q
The symbiotic relationship between BigFix and QVM https://youtu.be/tPValdswHwA
Technical Details https://youtu.be/2MfHziZnGfo

Mitigate Attacks with IBM BigFix & QRadar https://youtu.be/sCncDEDI138
Detect & remediate vulnerabilities faster https://youtu.be/NUJZBcOiqaI
BigFix Query https://youtu.be/teUsb6Wa8tQ

IPS, BigFix, QRadar SIEM/QVM/QRM integration demo https://youtu.be/rW8QHBLnD1M

Steps to configure these technologies:

"BigFix to QRadar" configuration https://youtu.be/EyNFI4vuKSc
"QRadar to BigFix" configuration https://youtu.be/EcxicHXBgkA
QVM scanner configuration https://youtu.be/B30jZKvbrnc
IPS configuration (alerts and flows) https://youtu.be/v62LsbmH6xE

IPS and QRadar

QRadar and IPS Automatic Quarantines. Part One https://youtu.be/acWefmmkISc
QRadar and IPS Automatic Quarantines. Part Two https://youtu.be/AtJigoIkgBA

Palo Alto Integration

Configure Palo Alto to send Logs to QRadar. Part 1 https://youtu.be/kLecgZEsOjQ
Configure Palo Alto to send NetFlows for QRadar. Part 2 https://youtu.be/HuS7J07czAY
Configure Palo Alto and QRadar to automatically block bad IPs. Part 3 https://youtu.be/-lV3tVK6a1Y
Configure Palo Alto and QRadar to automatically block bad IPs. P4 https://youtu.be/SWmcoKkw60s

Carbon Black Integration

QRadar and Carbon Black Integration https://youtu.be/YbuzkQMAwcE
QRadar, Carbon Black Response and IBM BigFix https://youtu.be/D0CVbItza9g

Guardium, QRadar, IPS and PIM working together (July 2, 2016) https://youtu.be/8ht6QL9E2FY
Protecting mainframes, DBs and AD https://youtu.be/PzSv5mYci1Q

IBM Mainframe

Real time logs from mainframes Part One https://youtu.be/G7uNEDsEfJk
Real time logs from mainframes Part Two https://youtu.be/59qYMaoSing
Is the mainframe your SIEM's dark spot? https://youtu.be/lD8rR4IQhQs
Mainframe does not have to be a security silo https://youtu.be/9tDItmjcVU8
How to easily collect mainframe events https://youtu.be/A7vTtgYP-Qw
Health Check for mainframes using RACF or ACF/2 https://youtu.be/Ur9mS29n4Zs

i-Series/AS/400/OS400 **https://youtu.be/Ca-eYpLnIlw**

How to easily collect logs from it

Guardium Integration

Sending logs from V10 (April 2,2018) https://youtu.be/TfpItWTJIJE

Integration Look https://youtu.be/dPkYuPKunWs
Vulnerabilities https://youtu.be/OahQLas_fPk
Guardium & QRadar Demo (May 13,2013) https://youtu.be/s0_IAota9ts

AppScan, ISAM, IPS & QRadar Demo https://youtu.be/_Sr0BBHkAd4
Bi directional Integration https://youtu.be/7wbqdzdI4MM
IPS Integration - Quarantine from QRadar to IPS https://youtu.be/zhdB55Zjo9s

Big Data

SIEM versus BigData (Feb 5, 2019) https://youtu.be/8ldxb9TcFqU
QRadar BigData extension https://youtu.be/I_4ASz0cOQs
QRadar basics and Big Data https://youtu.be/i6wezpafLNo

AQL Tutorial

AQL Basics in 15 minutes (Jan 2022) (**16:21**) https://youtu.be/57v5TAwSywg
Dealing with Expensive Searches (Jan 2022) (**8:20**) https://youtu.be/n06MLLMe_TM
AQL Series- AQL Introduction June 26,2017 https://youtu.be/J_xeOGq3b40

Security Intelligence Tutorial, Demo & Use Case Videos

AQL Series- Where, Group, Having, Order	June 26,2017	https://youtu.be/0E1sVKuWMmg
AQL Series- Counting	June 26,2017	https://youtu.be/Pf3BO1cNa80
AQL Series- Ref Set, Assets and UBA	June 26,2017	https://youtu.be/VmQodzEYBKk
AQL Series- Health Metrics and X Force	June 26,2017	https://youtu.be/cPK6nW0667o
AQL Series More Health Metrics and API calls	2017	https://youtu.be/q5vyQIL2Olg
AQL Series Payload, Indexed and Regex Searches	2017	https://youtu.be/_9_JgEPbZvU

Part 1. Documentation and basic syntax.	2016	https://youtu.be/-ZHVubxGO2s
Part 2. Very useful AQL functions:	2016	https://youtu.be/KfXrij5hGSM
Part 3. Leveraging the X-Force calls	2016	https://youtu.be/Bpq-T8pgNwI
Part 4. Investigating APTs using AQL	2016	https://youtu.be/n99ttBe4WcQ
Part 5. Nested IF/ELSE and CASE statement	2016	https://youtu.be/aoRiVYnIIQk
Part 6. Custom AQL functions	2016	https://youtu.be/6z8zjXw-xE4
Part 7 AQL queries to a table from LDAP	2016	https://youtu.be/VTlnanRdfXQ

Two Random tips on searches	(April 18, 2019)	https://youtu.be/7UChqiTzrzs
AQL Translator	(Feb 22, 2019)	https://youtu.be/4ZrQ68TFgt0
Cool AQL Custom Functions to Deal with Multiple	(June 2020)	https://youtu.be/EolEmCxCYcc
Detecting Squatting with QRadar Searches	(June 2020)	https://youtu.be/qSq-QcuwFi4
Joins in QRadar? Sort of	(July 2020)	https://youtu.be/s9evhXPd2cU
Joins in QRadar? Installation	(July 2020)	https://youtu.be/bf7IjLZUzrw
Ho to write a Custom AQL Function	(Dec 2021) (**10:52**)	https://youtu.be/eaLjiKJTSqA

QRadar RESTful API

QRadar API 101 (June 2021) (**9:53**)	https://youtu.be/swGI5QWB29g
Example of using the QRadar API with the X Force (Jan 2020)	https://youtu.be/twZX-c6WI4w
How to use the API	https://youtu.be/pPC23DDYiVc
Connecting to QRadar API (based on 7.2.6 demo)	https://youtu.be/30Tq-oWLIRw

QRadar Application Example with AQL via REST API

Part 1 (July 2016)	https://youtu.be/XE9UBI9spQ8
Part 2 (July 2016)	https://youtu.be/Kd96J3AU9cs

CyberSentinel

QRadar. Defending against DNS attacks. CyberSentinel. Part One https://youtu.be/7ep5V2sfLjs

Integration AppScan, IPS and QRadar

https://youtu.be/fUmYZ0TpKes
https://youtu.be/NMaNCOwe6C4
https://youtu.be/7wAE4TnyERI

QRadar & IBM Control Desk (ICD/SCCD) Integration	https://youtu.be/3ZctrDd41aw
Maas360 and QRadar Integration	https://youtu.be/VvilnI2pQ0A

Why QRadar?

What Makes QRadar so Special 2021 Part One (Oct 2021) (**19:19**)	https://youtu.be/Y52BrFmw_Xc
What Makes QRadar so Special 2021 Part Two (Oct 2021) (**22:03**)	https://youtu.be/RKV9rWhEo9o
What Makes QRadar so Special 2020 Part One (May 2020)	https://youtu.be/2UJu44Hhj20
What Makes QRadar so Special 2020 Part Two (May 2020)	https://youtu.be/wk-sic9YrYk
QRadar's evolution over the years (Feb 2020)	https://youtu.be/lw7YDvPMXlo
QRadar's secret Sauce (April 9,2018)	https://youtu.be/1TeUK3ESzo4
What makes QRadar So Special (Oct 6, 2017)	https://youtu.be/dpMn0GrAsCg
Flows Tutorial. Part One (Feb 12, 2018)	https://youtu.be/RWf3AmWOk0U

Security Intelligence Tutorial, Demo & Use Case Videos

QRadar Flows	https://youtu.be/mlm_g5vqk1k
Why QRadar is so special (in 30 minutes)	
Part One	https://youtu.be/ditD3aD4Y-Q
Part Two	https://youtu.be/Uoyl9y-wUZI
Part Three	https://youtu.be/2Y6pwDdLCwU
Why QRadar delivers value so rapidly	https://youtu.be/LqnNkReUXe4
What makes QRadar so special?	
Part One	https://youtu.be/g749DASrzgU
Part Two	https://youtu.be/HV6X-NLD4c0
What makes QRadar so Special (updated with QVM)	https://youtu.be/-RU-PSsddmc
Some of QRadar 7.2.6 Features	https://youtu.be/onTkiCm2yJA
QRadar App Exchange (based on 7.2.6 demo system)	https://youtu.be/1M7JUBJJE1c
QRadar App - QRadar User Behaviour Analytics	https://youtu.be/ARVsuQaSF9E
Easy to administer (based on 7.2.6 demo system)	
Customizing QRadar	https://youtu.be/HpE6mU_NAMw
Looking for anomalies	https://youtu.be/iAv8cZAqN2A
Creating behaviour, anomaly &threshold rules	https://youtu.be/LgksZvchS38
Searches in QRadar	https://youtu.be/sYcfxB0p3oU
QRadar 7.2.7 new features in 9 minutes	https://youtu.be/WQ3IZfYPcbg

QRadar SIEM

QRadar Server Discovery	https://youtu.be/gdQKS9HBEa8
QRadar Taxonomy	https://youtu.be/5RcsaHOBKX8
Tuning QRadar Part 1	https://youtu.be/xhrYeD3Pxiw
QRadar SIEM Core Foundation Enablement	https://youtu.be/hlrZPsz82pM
A look inside IBM Security QRadar / Offense Workflow	https://youtu.be/69rnM_hR9Lw
QRadar Offense Investigation Walkthrough	https://vimeo.com/177564412
Workflows in QRadar (based on 7.2.6 demo system)	https://youtu.be/u7u4J4lcfdc
Security Intelligence	
Part One:	https://youtu.be/eedzh6U5AEk
Part Two:	https://youtu.be/Bck5jNRZf3w
QRadar Rule creation: Baseline of trusted users	https://youtu.be/kRVsbxsYHg0
Creating Searches, Rules and Offenses using Categories	https://youtu.be/hlw7npbq0j0
QRadar and Network Flows	
Simple analogy to explain the value of flows	https://youtu.be/T3Z8bBp7ylc
The power of flows	https://youtu.be/C9UUuVZ1TmE
The value of flows	https://youtu.be/8fXII1rXFHQ
Explaining QFlows (and adding them to QRadar)	https://youtu.be/r1r3ontFVfw
Data Loss and Flows	https://youtu.be/I_ZM4IzxGno
DDoS and Superflows	https://youtu.be/XDbcG000zHw
Anomaly on aggregated search	https://youtu.be/lqhUYVUWihI
Policy Violation	https://youtu.be/Am8O6tgmUpY
Offense Chaining	https://youtu.be/TM5sAgencY8
Unauthorized user	https://youtu.be/aD9136ZrUkg
Detecting beaconing	https://youtu.be/X1auYa_nTAQ
Reports (based on 7.2.6 demo system)	https://youtu.be/VsIO4_4Xz2Q
Asset DB in QRadar (based on 7.2.6 demo system)	https://youtu.be/7dIOdpk3KF4
Advanced Searches	
Introduction	https://youtu.be/Wt03C9SxO3w

Editing some searches	https://youtu.be/L6UwGCG3DPw
Detecting beaconing at irregular intervals	https://youtu.be/GBEGyV11kMg
Creating reports with application names and user names	https://youtu.be/ODgBM2viXTg
Using sophisticated searches when investigating offenses	https://youtu.be/kB1Hi--Vs8Y
QRadar Tutorial (based old demo system)	
-1 Offenses 1025, 885 and 953	https://youtu.be/h63fyGlprTw
-2 Offenses 911, 995 and 929	https://youtu.be/N9ul6gfGimc
-3 Offenses 916, 938 and 906	https://youtu.be/624_AFAaF78
-4 Offenses 919, 898 & QRM Policy	https://youtu.be/dAMjGijuVmY
-5 QRM Simulation of Changes	https://youtu.be/KywEpLd3m9k
QRadar Offenses (based on 7.2.6 demo system)	
Why sending vulnerability data to QRadar (April 12, 2018)	https://youtu.be/t_t_QRl0NiM
QRadar detects exploited vulnerabilities	https://youtu.be/OlkmbKoHPAI
Detecting Jailbroken iPhones	https://youtu.be/cvJIoHYB0f0
Either in the building (badged) or remote (VPN) but not both	https://youtu.be/igrZ_FYME4c
Detecting stolen credit card data	https://youtu.be/PhK6TKnMWrE
Offenses with one thing in common	https://youtu.be/DH_J6rEc09o
QRadar is easy to administer (based on 7.2.6 demo system)	
Customizing QRadar	https://youtu.be/HpE6mU_NAMw
Detecting anomalies	https://youtu.be/iAv8cZAqN2A
Creating behavior, anomaly and threshold rules in QRadar	https://youtu.be/LgksZvchS38
Searches in QRadar	https://youtu.be/sYcfxB0p3oU
QRadar Tuning – Tutorial	https://youtu.be/NZuTruTxMeY
QRadar Testing rules with LogRun, TCPReplay & Right-click	https://youtu.be/LHv6_JjhFU4
QRadar Detecting DDoS attacks and Superflows	https://youtu.be/dpO8MNzS-UA

QRadar Risk & Vulnerability Managers

QVM Dashboard	https://youtu.be/jjBg5c0_etk
QVM and QRM fast-pace tutorial	https://youtu.be/C6TqOPGy1zc
QRadar Vulnerability Manager Demo	https://youtu.be/7gHmVZ-f9IY
	https://youtu.be/Vg3u6Z0dZ4U
QRadar Risk Manager Tutorial	
1- White Board Intro	https://youtu.be/vj2mCONlRQQ
2- Connections & Topology	https://youtu.be/osxDKH6zpZw
3- Policies	https://youtu.be/QCcEzBQhyEk
4- More on Policies	https://youtu.be/fXNa_-HU35M
5- Simulation of Changes	https://youtu.be/KywEpLd3m9k
QRM & QVM modules (based on 7.2.6 demo system)	
QRadar Vulnerability Manager	https://youtu.be/EY4f94244j8
QRadar Risk Manager	https://youtu.be/wu48D-bYczw

QRadar Incident Forensics

Introduction	https://youtu.be/KPl4v1esscw
Use case #1	https://youtu.be/-2de18vjxRU
Use case #2	https://youtu.be/vPJshiECOvk
Use case #3	https://youtu.be/NqGqUyUfY3k
Use case #4	https://youtu.be/28Y39DbwmsQ
Nothing escapes the scrutiny of QRadar Forensics (based on 7.2.6)	https://youtu.be/uhGGboQyQdY

Security Intelligence Tutorial, Demo & Use Case Videos

File Analysis, looking for suspicious files (based on 7.2.6)	https://youtu.be/Cb-E7Et389U
Image Analysis (steganography) & Quick Start View (based on 7.2.6)	https://youtu.be/DJ_f1um-j6k
VGrid Surveyor Link Analysis and Query Builder (based on 7.2.6)	https://youtu.be/QShGR_naFxo
More on File, Image and Link Analysis (based on 7.2.6)	https://youtu.be/Lar7B9Mj6qc

Advanced Persistent Threats

What are APTs?	https://youtu.be/1qFga_DJs0c
An average of 225 days to detect an APT…	https://youtu.be/_hEX9vSmTII
Advanced Persistent Threats	
Part One	https://youtu.be/Fzl34he-qB8
Part Two	https://youtu.be/9vaEtX0d2gg
Part Three	https://youtu.be/LsYYtB5-WD0
Part Four	https://youtu.be/m-1Gr1UK3k8

MISC.

QRadar monitoring itself (Dec 2021) (**2:32**)	https://youtu.be/I0cU3yzqCyE
Why making vulnerabilities public? (Nov 2021) (**10:53**)	https://youtu.be/2HFDVMopmcc
Cybersecurity will continue to be hard Part 1 (Nov 2021) (**22:20**)	https://youtu.be/BIXwJ75nKw0
Cybersecurity will continue to be hard Part 2 (Nov 2021) (**11:49**)	https://youtu.be/aMOT_euNblk
Looking Manually at QRadar Logs (Feb 2021) (**4:46**)	https://youtu.be/l3TLr-fxTIA
Having a hard time finding the right patch (Feb 2021) (**2:08**)	https://youtu.be/h_NNILhcx1w
My QRadar CE stopped collecting logs (Feb 2021) (**2:11**)	https://youtu.be/FYtIAtiB6yE
Security Incidents in Medical Devices (Feb 2021) (**15:30**)	https://youtu.be/ltFBy3F_oBw
Regex Cheat Sheet (Oct 2020) (**6:39**)	https://youtu.be/opGXUfSDGjg
Observations on latest major data breach (March 21, 2019)	https://youtu.be/-r-YJnUmIHE
Guardium 10.6 Supports Sharepoint and NAS (Jan 7, 2019)	https://youtu.be/n4cVAUMP5LA
QRadar Value Assessment Program (Dec 10,2018)	https://youtu.be/3smNYOqtcgQ
Installing Guardium in Oracle Cloud (June, 2020)	https://youtu.be/LYVCJj_yXeU
Guardium Appliance in AWS (Dec, 2018)	https://youtu.be/m3FKEFjYm0A
Installing Guardium in Azure (Dec 4, 2018)	https://youtu.be/zUa4XvYwDYA
Cryptography in simple terms (Oct 4, 2018)	https://youtu.be/TdhA7kh0bw8
How are passwords compromised (Oct 17, 2018)	https://youtu.be/2ORNezaLJMw
DNS Resolvers Part 1, THREAT PROTECTION (April 17,2018)	https://youtu.be/dG2HXt1G6b8
DNS Resolvers Part 2, PRIVACY (April 26, 2018)	https://youtu.be/GPF1JnVVFmk
DNS Resolvers Part 3, PERFORMANCE (April 26, 2018)	https://youtu.be/ttNH-e2W-Xc
Quad 9	https://youtu.be/b7vxSLR2ptI
What is "Cognitive" Security?	https://youtu.be/WOI3qENuE_g
Cognitive Security - IBM Security Summit 2016	https://vimeo.com/171964887
Watson for Cyber Security	https://youtu.be/xG9jazUpEus
Dealing with ShellShock	https://youtu.be/jN2zXlQ520E
IPS: Snort Engines can be easily fooled	https://youtu.be/xSVT1aOIM2E
Security Cloud Enforcer - Introductory Whiteboard	https://youtu.be/1aIhaLxEPew
Why is Computer Security so hard?	https://youtu.be/ox_DDz3oLgc
Cross Site Scripting	https://youtu.be/llry5ZxTDUM