Security Intelligence Tutorial, Demo & Use Case Videos

This document contains a growing list of very useful Security Intelligence Tutorial & Demo videos posted on YouTube™. This file can be downloaded from this site: https://ibm.box.com/s/ich0yyiw54y0ek6s9a66xvtjku8e42rc

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

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

Searching in QRadar

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
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)

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
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
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

Security Intelligence Tutorial, Demo & Use Case Videos

Getting Proxy Logs from pfSense (June 27, 2019)	https://youtu.be/ylOXMlN15zQ
Getting Proxy Logs 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/WIjgG3x-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

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

AWS Security Tutorial

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 in AWS:

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:

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/MIgj7D1VDw0

Security Intelligence Tutorial, Demo & Use Case Videos

Modern Dashboards in QRadar:

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

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

Getting Logs When Systems are in the Cloud:

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/V7l0jWanKiw
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/xf5RFFbknel
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

Security Intelligence Tutorial, Demo & Use Case Videos

QRadar Deployment Architecture

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
Logs Sources App V4 (June 12,2019)	https://youtu.be/Q2ShsY1JMbY
Monitoring QRadar appliances with QDI (May 6,2018)	https://youtu.be/r9L79n4Ll_U
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
Part One (Jan 11, 2017)	https://youtu.be/pl85saA_4BU
Part Two (Jan 11, 2017)	https://youtu.be/CrCm5grwLRI
Part Three Cloud. (Jan 19, 2017)	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

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 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 CIRD Ranges (Nov 26, 2017)	https://youtu.be/MmA0-978fSk

QRadar Tuning and Other Concepts

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
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 and DNS

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

Security Intelligence Tutorial, Demo & Use Case Videos

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/6qklDxtjoFo

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
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

Speed up Offense Investigations with Advisor (Jan, 2020)	https://youtu.be/htwwuD1qymk
Use case for QRadar Advsior 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

Security Intelligence Tutorial, Demo & Use Case Videos

QRadar Use Case Series

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
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

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/EsqpXIaQIBA
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/J5IO3X8GgXQ
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/CVlBI6SnpgI
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

Security Intelligence Tutorial, Demo & Use Case Videos

Detecting fraud, account takeover	https://youtu.be/oUp3HYVrfQU
Detecting fraud, more examples	https://youtu.be/llLQ8DlKhQQ

QRadar User Behavior Analytics

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-VWAlPHZ6w
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/IqZT7Yj5ZqU
QRadar Cloud Discovery App Part 2 Analytics (April 19, 2018)	https://youtu.be/IG6UGb0XXtI
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 DSM Editor

DSM Editor Tutorial 2020, JSON (Dec 2019)	https://youtu.be/8f86_yEWOj4
DSM Editor Tutorial 2020, CEF and LEEF (Dec 2019)	https://youtu.be/8vIjcFcuoXs
Using the DSM Editor to create a pfSense parser (June 2019)	https://youtu.be/gN7JMpbuAy0
DSM Tutorial Part One (Jan 24 2018)	https://youtu.be/LRhNMejQFNM
QRadar DSM Editor Tutorial in less than 10 minutes	https://youtu.be/KF40bba_kp0

QRadar & Resilient

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

QRadar & Integration

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

Security Intelligence Tutorial, Demo & Use Case Videos

Gigamon App for QRadar (Jan 25,2018)	https://youtu.be/VM3LdrgDU-I
QRadar Splunk App (Sept 21,2018)	https://youtu.be/e21eHgvwnyU
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/ZEO6LI5QIAc
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/YvbNlQ4If-Q

Security Intelligence Tutorial, Demo & Use Case Videos

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 Series- Quick Filter and UI Searches June 26,2017 https://youtu.be/oXLiTVp_6sY
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/q5vyQlL2Olg
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/aoRiVYnlIQk
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

QRadar RESTful API

How to use the API	https://youtu.be/pPC23DDYiVc
Connecting to QRadar API (based on 7.2.6 demo)	https://youtu.be/30Tq-oWLIRw

CyberSentinel

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

QRadar Application Example with AQL via REST API

Part 1	https://youtu.be/XE9UBI9spQ8
Part 2	https://youtu.be/Kd96J3AU9cs

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?

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
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

Security Intelligence Tutorial, Demo & Use Case Videos

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
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

Security Intelligence Tutorial, Demo & Use Case Videos

MISC.

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 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/WOl3qENuE_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