IBM

outthink threats

IBM SECURITY SERVICES

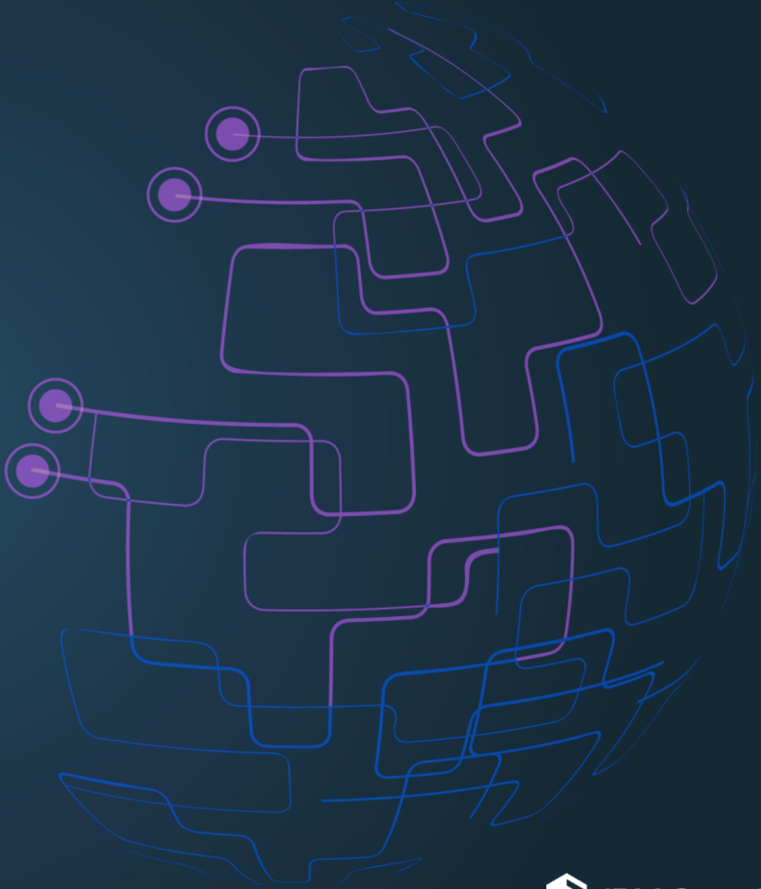
Brendon Munn
IBM Security Services
Channel Sales Leader - North America

Tech Data

IBM Security

Agenda

- □ What Differentiates IBM Security ?
- □ IBM Security Services
  - X-Force Incident Response and Intelligence Services (IRIS)
  - X-Force Red Offensive Testing Services (XFR)
- □ IBM Security Sales Contact



What Differentiates IBM Security ?

Who we are ...

- Largest enterprise cybersecurity provider
- 20+ Security acquisitions since 2002
- Leader in 12 security market segments
- 8,000+ security employees
- 2T+ security events monitored per day

Who depends on IBM Security?

IBM Security secures

100%

of the US Fortune 100

95%

of the Global Fortune 500

Finance

49 out of 50 of the world's largest financial services and banking companies

Tech

13 out of 15 of the world's largest technology companies

Healthcare

14 out of 15 of the world's largest healthcare companies

Telecom

The 10 largest telecom companies

Automotive

19 out of 20 of the world's largest motor vehicle and parts companies

Airline

8 out of 10 of the world's largest airline companies

We are invested to be the best

12

market segments where analysts ranked IBM Security as a "Leader“

Gartner, Forrester, IDC, Frost & Sullivan, Ovum, and KuppingerCole

SIEM

Security Analytics

Web Fraud Detection

Identity Governance

Access Management

Identity as a Service

Identity Management

Authentication

Data Security and Database Security

Unified Endpoint Management

Managed Security Services

Cybersecurity Incident Response Services

IBM Security Services

- ❑ X-Force Incident Response Intelligence Service (IRIS)
- ❑ X-Force Red Offensive Service (XFR)

X-Force Incident Response and Intelligence Services (IRIS)

IBM Security

IBM X-Force IRIS

Incident Response and Intelligence Services

Uses highly skilled experts with decades of leading-edge incident management and security intelligence experience

Helps clients make the critical transition from incident response to incident preparation

Reduces the time and costs associated with successful incident recovery

Proactive Preparation | Incident Planning | Incident Triage

X-Force Incident Response and Intelligence Services (IRIS)

HOW DOES IT WORK?

An **annual retainer** service that helps clients proactively prepare for and respond to threats by applying the latest threat intelligence and technical and investigative skills acquired from hundreds of breach investigations.

- Global delivery team available in all geographies across all industries.
- Proactively prepares with IR program assessment, IR playbooks and tabletop exercises to enhance your incident response program, management and recovery
- Get 24/7, rapid response to a cybersecurity incident with our around-the-clock global hotline, and help reduce potential adverse impact
- Gain deep insight into how and why the incident started with forensic analysis, enabling agile response to law enforcement queries and regulatory requirements

IBM X-Force IRIS
Incident Response and Intelligence Services

X-Force Incident Response and Intelligence Services (IRIS)

Level	Description	SLA
Ad Hoc	• Time and materials terms and conditions	• Triage: Best Effort • Onsite: Best Effort
Tier 1	• Kickoff Workshop • Quarterly Status Review • 60 annual subscription hours • Additional hourly staff-rate	• Triage: 4 hours • Onsite: Best Effort
Tier 2	• Kickoff Workshop • 2 Proactive Services Units • Quarterly Status Review • 80 annual subscription hours for IR or proactive services • Additional discounted hourly staff-rate	• Triage: 1 hour • Onsite: 24-48 hours
Tier 3	• Kickoff Workshop • 3 Proactive Services Units • Dark Web Search Services • Quarterly Status Review • 150 annual subscription hours for IR or proactive services • Additional discounted hourly staff-rate	• Triage: 1 hour • Onsite: 24-48 hours
PSU	• Proactive services unit add on with Retainer	• N/A

24 x 7 x 365 Global Incident Response Hotline – All Tiers

X-Force Incident Response Service

- 24x7x365 Global Incident Response Hotline – All Tiers

Tier 1

» Kickoff Workshop

» Quarterly Status Review

» 60 annual subscription hours

» Additional hourly staff-rate

SLA

» Triage: 4 hours

» Onsite: Best Effort

X-Force Incident Response Service

- 24x7x365 Global Incident Response Hotline – All Tiers

Tier 1

- Kickoff Workshop
- Quarterly Status Review
- 60 annual subscription hours
- Additional hourly staff-rate

SLA

- Triage: 4 hours
- Onsite: Best Effort

Tier 2

- Kickoff Workshop
- Quarterly Status Review
- 80 annual subscription hours for IR or proactive services
- 2 Proactive Services Units
- Additional discounted hourly staff-rate

SLA

- Triage: 1 hour
- Onsite: 24-48 hours

X-Force Incident Response Service

- 24x7x365 Global Incident Response Hotline – All Tiers

Tier 1

- Kickoff Workshop
- Quarterly Status Review
- 60 annual subscription hours
- Additional hourly staff-rate

SLA

- Triage: 4 hours
- Onsite: Best Effort

Tier 2

- Kickoff Workshop
- Quarterly Status Review
- 80 annual subscription hours for IR or proactive services
- 2 Proactive Services Units
- Additional discounted hourly staff-rate

SLA

- Triage: 1 hour
- Onsite: 24-48 hours

Tier 3

- Kickoff Workshop
- Quarterly Status Review
- 150 annual subscription hours for IR or proactive services
- 3 Proactive Services Units
- Dark Web Analysis Service
- Additional discounted hourly staff-rate

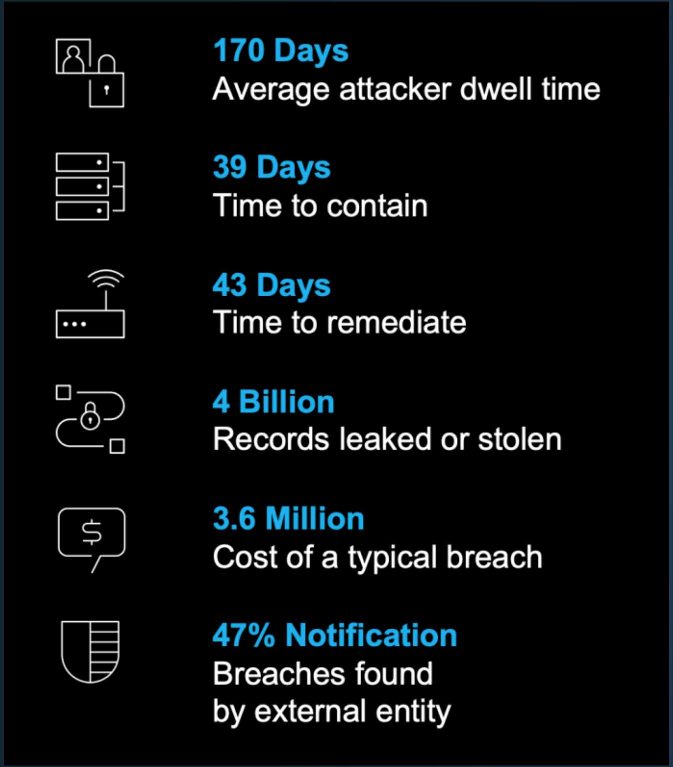
SLA

- Triage: 1 hour
- Onsite: 24-48 hours

X-Force IRIS - Menu of Proactive Services

IRIS Proactive Services Menu	Description	Proactive Units
Incident Response Program Assessment	Review client’s existing IR program, interview key stakeholders to understand people, processes and technology and deliver a prioritized roadmap on how to improve	1
CTI Program Assessment	Review of client’s threat intelligence services using industry best practices, and defining priority intelligence requirements	1
Incident Response Playbook Customization	Edit the existing playbook and/or create new playbook targeted towards the highest priority incidents to potentially occur within the environment	1
Standard Tabletop Exercise	Simulated attack scenario to test a client’s incident response plan/playbook	1
Dark Web Search Service	Search the Dark Web for specific areas of interest using key words, analyze the results and provide key findings and recommendations	1
Cybersecurity Incident Response Plan – High Level Review	Provide a high-level assessment of client’s existing incident response plan and areas for improvement	1
Security Incident First Responder Training	2-day workshop enables client IT staff to properly secure and collect critical data in preparation for forensic analysis	1
Strategic Threat Assessment	Review a client’s key assets to characterize threat events by the typical attackers, the likely infection vectors, and the techniques and procedures that adversaries employ	1
Cybersecurity Incident Response Plan – Full Development	Provide a complete incident response plan for clients that do not currently have an IRP, includes a tabletop exercise of the new plan	4
Active Threat Assessment	Detect current and historical threats across the enterprise utilizing IBM generated intelligence and IOC/IOA detection methodologies	Custom

Proactively prepares with IR program assessment, IR playbooks and tabletop exercises to enhance your incident response program, management and recovery.



170 Days
Average attacker dwell time

39 Days
Time to contain

43 Days
Time to remediate

4 Billion
Records leaked or stolen

3.6 Million
Cost of a typical breach

47% Notification
Breaches found
by external entity

X-Force IRIS Key Features:

- Leading with the top experts in the industry, responsible for hundreds of major breach investigations
- The right skills to deal with the most critical incidents and breaches in the world
- Getting clients out of a continuous state of breach and approach incident response proactively
- Globally available experts, assets and delivery
- Becoming a strategic partner, to implement a comprehensive, successful program

X-Force Incident Response and Intelligence Services (IRIS)

If you are experiencing a **breach**, contact the IRIS team.

US hotline
1-888-241-9812

Global hotline
(+001) 312-212-8034

IBM Security

X-Force Red

Who is X-Force Red?

- X-Force Red (XFR) is an autonomous team of veteran hackers, within IBM Security, hired to break into organizations and uncover risky vulnerabilities that criminal attackers may use for personal gain.

- X-Force Red offers offensive security services which include penetration testing, vulnerability management services, red teaming, code reviews, static analysis and vulnerability assessments.

- Their goal is to help security leaders identify and remediate security flaws, covering their entire digital and physical ecosystem.

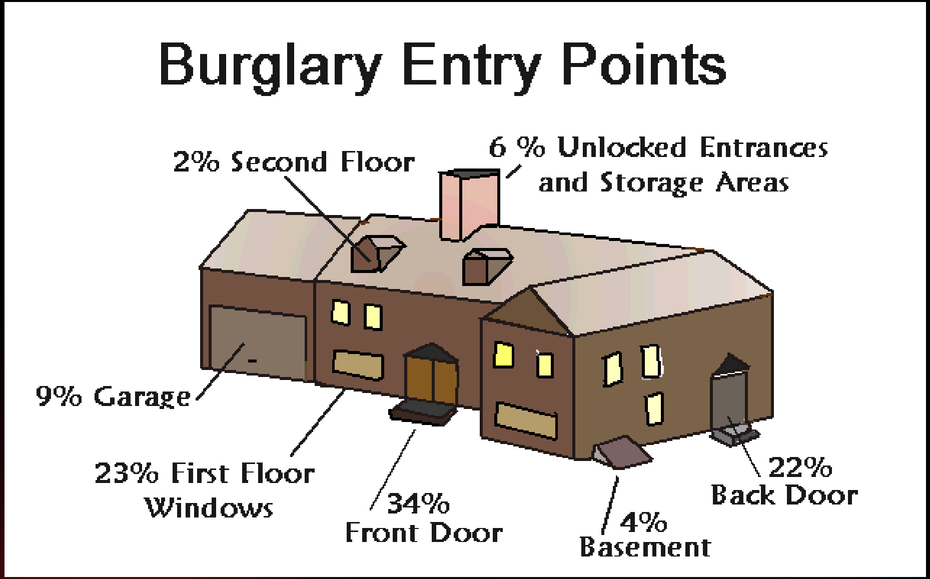
- 200+ people globally

- Industry renown hackers such as:
  - Space Rogue, Evilmog, Snow, Videoman, retBandit, Major Malfunction

How X-Force Red defines penetration testing

A penetration test is an attack and exploitation simulation designed to uncover a target's security weaknesses.

Penetration testers are hackers who use the same manual methods and tools criminals would use to break into organizations and compromise valued assets.



X-Force Red Penetration Testing Differentiators

Flat Rate Pricing: X-Force Red price is a flat rate “gift card” format where clients can pull from the allotted dollar amount to test whatever they want. No contract re-negotiations or signings needed if clients change which applications/networks/systems they want tested.

Specialized expertise: X-Force Red has specialized practices and expertise for ATM, blockchain, mainframe, IoT, OT/ICS and automotive testing.

Senior Level Expertise: X-Force Red testers have at least a decade of testing experience

Customized Reports: Each report and set of remediation recommendations are customized for each client. They include screenshots of the exploits used, high level executive summary.

One Retest Included: X-Force Red offers one retest at no additional cost to verify patches are applied.

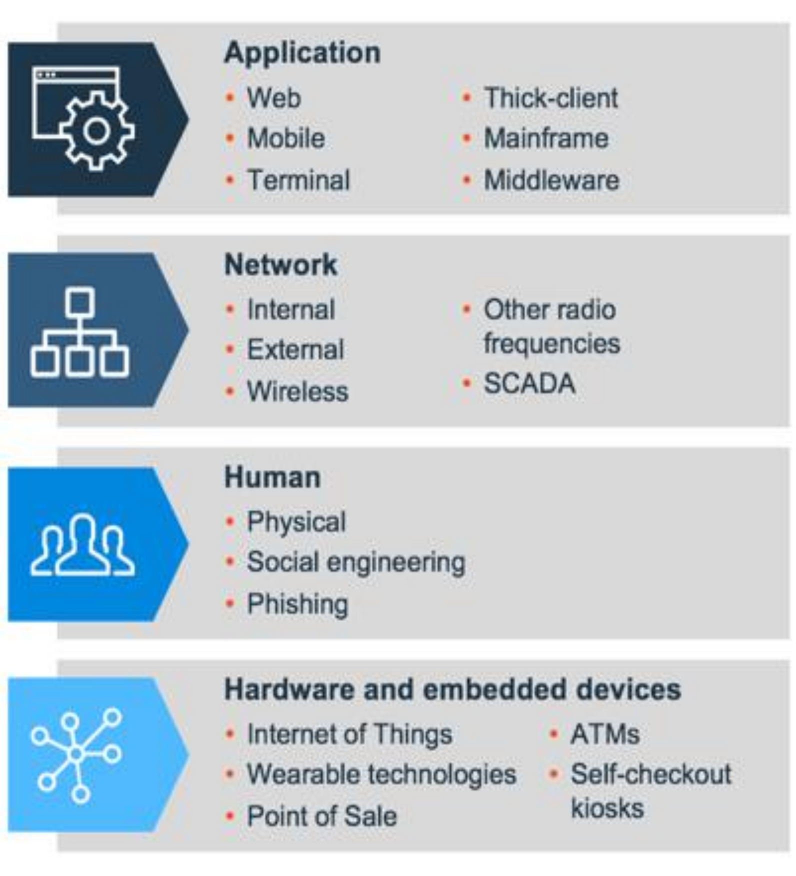
X-Force Red - Penetration Testing Services

❑ Identify and fix critical vulnerabilities quickly across entire infrastructure from systems, applications, devices to personnel

❑ Manually test every facet of infrastructure in a detailed way that tools alone cannot do.

❑ Help organizations maintain compliance with regulatory standards (GDPR, PCI DSS, SOX, etc.)

❑ Manual testing mimics real-world attackers using the same tools, techniques and practices.



Application

- Web
- Mobile
- Terminal
- Thick-client
- Mainframe
- Middleware

Network

- Internal
- External
- Wireless
- Other radio frequencies
- SCADA

Human

- Physical
- Social engineering
- Phishing

Hardware and embedded devices

- Internet of Things
- Wearable technologies
- Point of Sale
- ATMs
- Self-checkout kiosks

Application Testing

X-Force Red's hackers understand application behaviors, communication, and how attackers could circumvent the logic. They can also chain vulnerabilities together to show how an attacker may compromise an application. XFR's Application Testing identifies, prioritizes and helps organizations fix high risk application vulnerabilities before and after deployment.

Penetration Testing

- X-Force Red penetration testers manually break into applications and uncover vulnerabilities. Tool-based intelligence coupled with human intelligence.
- X-Force Red penetration testers look for "as of yet unknown" vulnerabilities
- Three levels of effort: Entry, Standard, Advanced

Vulnerability Assessment

- Scan applications and validate vulnerabilities, weed out false positives and identify additional vulnerabilities based on scan output indicators
- Poke and prod performed manually by X-Force Red VMS team
- Raw, automated, static scanning

Source Code Review

- Manual code review; X-Force Red penetration testers manually test code
- Static analysis and code review

Network Security Testing

Network penetration testing identifies opportunistic attacks such as if the digital front door is left open, allowing an attacker to walk in and rifle through data. Manual network testing uncovers vulnerabilities that scanners cannot uncover such as logic flaws, back doors, and misconfigured products.

Penetration Testing Services

- Assess the security of devices from a network perspective, focusing on exposed services, configurations, and infrastructure.
- Can be done from both an external and internal perspective for up to 4 class C networks.
- Additional class C networks can be added, as necessary.

Vulnerability Assessments

- Can be done from both an external and internal perspective using automated tools
- Manual review for any false positives
- Manual poke and prod to identify additional vulnerabilities indicated by scanner output

Human Testing Services

X-Force Red Social Engineering involves creating ruses to trick personnel into divulging sensitive information or providing access to their computers.

Physical Engagements

Uses disguises, props, USB drops, badge cloning, lock picking, tailgating, dumpster diving and other techniques to achieve established goals

X-Force Red Attacker Reconnaissance

Extensive Open-Source Intelligence (OSINT) gathering to find publicly available information about targets that attackers could use to compromise clients

Phishing and Spear-Phishing

Crafts customized real-world phishing emails based on information collected from attacker reconnaissance research

Vishing

Works with the client to develop goals such as eliciting sensitive information from employees, or asking employees to visit a malicious website controlled by X-Force Red

Hardware Testing

X-Force Red Hardware Testing identifies and helps fix hardware design flaws before and after products go to market. The service includes manually pulling apart devices to find vulnerabilities tools cannot find.

Hardware Device Testing

- Testing aimed at anything electronic and the enclosure or housing that makes up part of the device.
- Standard hardware includes basic testing such as a smart light globe
- Advanced test includes more complex testing such as industrial control system or a crypto wallet.

X-Force Red Hardware Testing Services

- Device Discovery and Prioritization
- Builds and Tests Attack Scenarios
- Secure By Design
- Reporting and Remediation

X-Force Red
Vulnerability Management Services (VMS)

IBM Security

Vulnerability Management Services (VMS)

Self-Service or Managed Scanning: Using whichever best-of-breed scanning solution the customer prefers, X-Force Red provides deployment, support and premium services to help secure our customer's most critical assets

Scan Fundamentals: Helps customer understand which systems and applications are the most important, and configure the scan tool to identify vulnerabilities at the right depth and frequency

Prioritization: X-Force Red ranks vulnerabilities based on asset criticality and active exploitation in the wild

False Positive Reduction: X-Force Red validates identified vulnerabilities, delivering only legitimate vulnerabilities

Remediation Management: Remediation oversight & subject matter expertise for remediation efforts, including tracking to completion

IBM's vulnerability management service ranks vulnerabilities within minutes as well as identifying if the vulnerability is being weaponized in the wild and the value of vulnerable asset.

X-Force Red VMS Differentiators

- **X-Force Red Portal** provides a centralized view of prioritized vulnerabilities, including how many exploits exist against a specific vulnerability
- **Vulnerability differentiation** that ranks vulnerabilities based on which ones are actively being exploited and asset value
- **False positive reduction** validates if a vulnerability is real vs. a false positive before it is sent for remediation
- **Automated ranking formula** prioritizes vulnerabilities within minutes, which significantly speeds up remediation time and saves resources typically needed for manual vulnerability management programs.
- **Flexibility** with the tools can be run inside client networks when privacy regulations require it (very common). Service can be hosted in the Cloud or on client's infrastructure.
- **Remediation facilitation** enables clients to fix critical vulnerabilities using their current resources. Ensures vulnerabilities are delivered to the appropriate remediators, tracked and fixed.

X-Force Red - Media Coverage

- CNBC - FBI warns of criminal ATM cash-outs, here's how to protect yourself
- Forbes - From Radiation Detection To Flood Defenses, Smart City Security Really Sucks
- eWeek - IBM X-Force Red Grows With New Labs and ATM Testing Service
- BBC - Warning over 'panic' hacks on cities
- CNN - Charles Henderson on CNN Headline News
- Fox Business Network - IBM: Major cities around the world vulnerable to hack attacks
- Wired - The Sensors That Power Smart Cities Are a Hacker's Dream
- CNBC - Secrets to a better password and fewer hacks: Go long, use variety, and sometimes lie
- CNBC Nightly Business Report - Protecting Passwords ()
- WSJ Pro Cybersecurity News - Editor’s Notebook: Voices from the WSJ Pro Cybersecurity Executive Forum
- Washington Post - The Cybersecurity 202: We surveyed 100 security experts. Almost all said state election systems were vulnerable.

IBM Security

Red Con - August 19th, 2020

X-Force Red is hosting a virtual conference called, "Red Con," on August 19th. The event will feature a series of talks, one of which includes a new zero-day vulnerability discovered by X-Force Red's researchers that could potentially impact millions of IoT devices.

The goal of the event is to inform and enlighten you and your team by presenting new research, attack tools and techniques, and other topics that may be top-of-mind during these transitional times. It will not be a sales pitch.

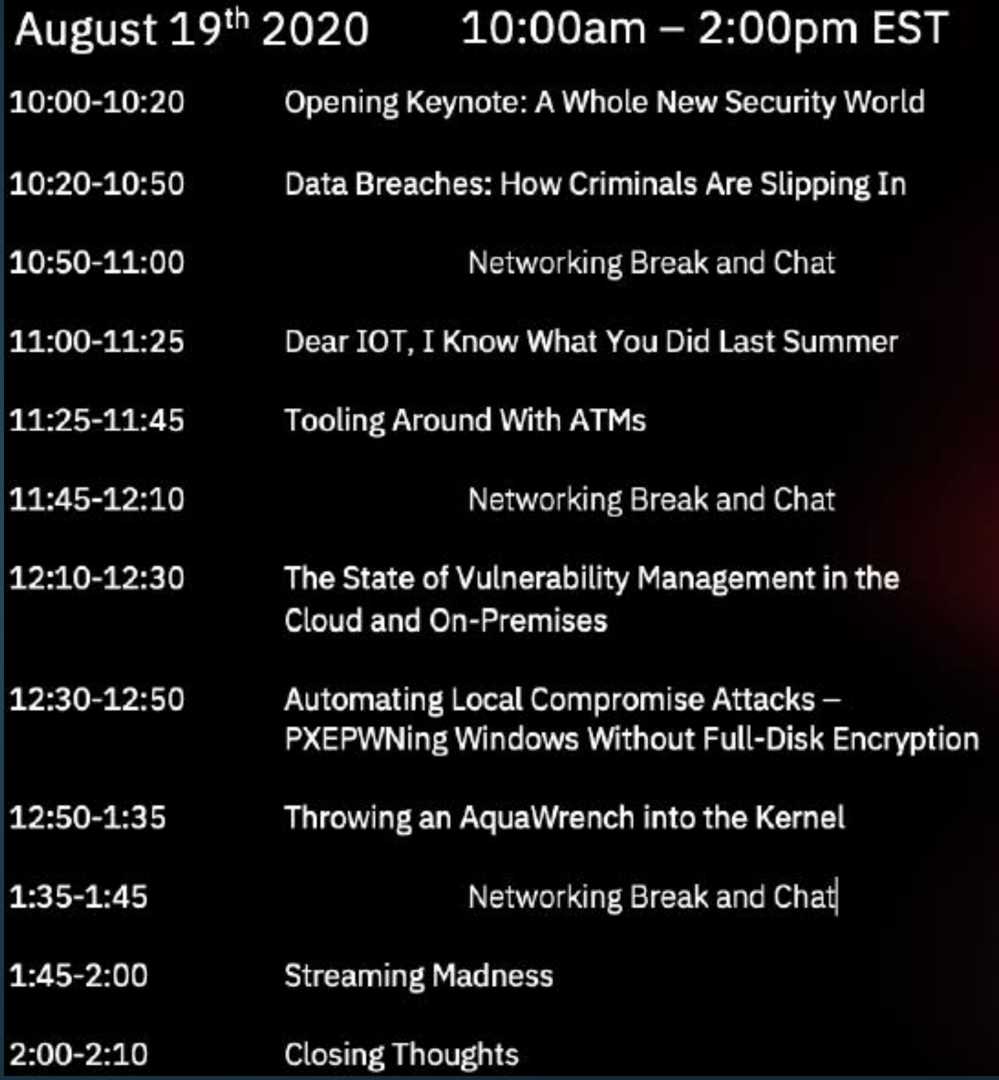
In addition to the zero-day research, other talks include:

- How the security landscape has shifted since COVID-19 began, and which challenges may arise as we head into the future.
- A dissection of well-known and not-so-well known breaches, from the viewpoint of an attacker.
- How live streaming content providers may be putting themselves at risk of a compromise
- New attack tools and techniques developed by X-Force Red's testers

Here's a link to the registration page: https://ibm.biz/BdqVTv We hope you can attend!

IBM Security

RED CON Agenda



August 19th 2020 10:00am – 2:00pm EST

10:00-10:20	Opening Keynote: A Whole New Security World
10:20-10:50	Data Breaches: How Criminals Are Slipping In
10:50-11:00	Networking Break and Chat
11:00-11:25	Dear IOT, I Know What You Did Last Summer
11:25-11:45	Tooling Around With ATMs
11:45-12:10	Networking Break and Chat
12:10-12:30	The State of Vulnerability Management in the Cloud and On-Premises
12:30-12:50	Automating Local Compromise Attacks – PXEPWNing Windows Without Full-Disk Encryption
12:50-1:35	Throwing an AquaWrench into the Kernel
1:35-1:45	Networking Break and Chat
1:45-2:00	Streaming Madness
2:00-2:10	Closing Thoughts

IBM Security Sales Engagement Process

Business Partner Program

- Security Services proposal includes (2) Order documents:
  - IBM Statement of Work; executed between IBM & the customer
  - Business Partner Price Quote; executed between BP & the customer
- IBM is responsible for the service descriptions/activities
- Business Partner is responsible for invoicing the customer
  - BP gets margin based on the price uplift on the cost provided from Tech Data.
- Engage directly with IBM Security Services Sales Leader for sales support

IBM Sales Contact

Brendon Munn	Security Services Sales Leader North America – Channel		bmunn@us.ibm.com (o) 850-613-4247 (m) 678-245-9637

IBM

outthink threats

THANK YOU

IBM Security

Supporting Documents, Web Links, and Videos

IBM Security Web Links:

https://www.ibm.com/security/services

https://www.ibm.com/security/services/ibm-x-force-incident-response-and-intelligence

https://www.ibm.com/security/services/offensive-security-services

https://www.ibm.com/security/services/managed-detection-response

X-Force IRIS

Optimize your personnel, process, and technology roadmaps

Incident Response Program Assessments

A proactive cyber breach defense that helps you review, and enhance your incident response program to build the foundation for incident response and recovery

- IBM security experts, working hand-in-hand with you
- Best practices review
- Interviews with key stakeholders
- Recommendations for improvements

Detailed Roadmap to help you determine where your program needs to grow and specific recommendations to help you get there.

How does it work?

IBM will review your existing incident response policies and then take a deeper dive with interviewing key stakeholders to understand your people, processes and technology and deliver a prioritized roadmap on how to improve your program.

Improve your response to cyber attacks

Cybersecurity Incident Response Planning Services

Help prepare your organization to better respond to cyber incidents and attacks.

Help you choose the right response tools, resources, and processes.

Provide IR playbooks with step-by-step instructions on how to respond to specific types of incidents.

Offer different levels of assessment and planning services tailored to the needs of your organization.

How does it work?

It provides a framework for effectively responding to any number of potential incidents and specifically defines the organization, and roles and responsibilities of all respondents, establishes authority for making major decisions, and documents communication flows and notification procedures.

Prepare your security teams to act against real cyber attacks

Standard Tabletop Exercises

IRIS experts will give a presentation that covers scenarios based on real-world experiences.

These tabletop exercises can help:

- Test business processes, procedures, and responsiveness
- Stakeholders communicate more openly and build relationships
- Expose gaps in processes and technologies
- Enhance cyber awareness, readiness, and coordination

Lead time
6–8 weeks

Locations
Client site
Hotel
Remote

Gain the insights of dark web forums and marketplaces

X-Force Dark Web Analysis Services

Our experts mine the Dark Web to find information about clients to warn them about leaks of their confidential information

How does it work?

The X-Force Intelligence Services team will search the Dark Web for specific areas of interest using key words. They will sort through the results to turn raw messy data into actionable preventive defense.

X-Force RED

Testing with X-Force Red

0:57

IBM Security