Detect and Respond to Accelerating Threats

John Wheeler  
BISO, IBM Security  
VP of Strategy and Innovation, Services and Integrated Solutions

Wendi Whitmore  
Vice President, X-Force  
Threat Intelligence

Axel Schittek  
IT Governance Leader, Fiducia & GAD IT AG
Adapting to the world’s crisis, natural disasters, and upheavals

IBM Security has invested millions preparing for moments like this one.

We have demonstrated our resilience in the face of fires, floods, earthquakes, tsunamis, blackouts, lighting strikes, blizzards, and more.

Our robust set of business continuity plans and globally distributed operations, with pandemic planning, mean we can execute for our clients with calm and confidence.

Learn more at: https://www.ibm.com/security/COVID-19
IBM Security Unit and BISO
Response to COVID-19

Security Unit COVID-19 Command Center

- Command Center Leadership Team represented by functional leaders
- Regular stand-up Command Briefings
- Alert roster with 1-hour “Muster Readiness”

Command Center Briefings

- Relevant external news & notifications
- Emerging threat intelligence & cyber incidents
- Employee health & safety guidance/situations
- Site & business

It's our job to instill focus and calm while maintaining business continuity and staying ahead of rapidly evolving cyber threats.
Cybercrime is built on threat actors’ abilities to exploit fear, anxiety, and uncertainty—sentiments that continue to grow amid the pandemic.
Responding to COVID-19: Top priorities for the CISO

1. Enabling continuity of CISO operations
   • Maintain 24x7 security operations
   • Shift to virtual incident response

2. Respond to the changing threats
   • Vigilance against COVID-19 threats
   • Helping to secure remote workforce

3. General IT readiness and continuity
   • Essential functions and personnel
   • Critical applications and systems
   • Logistics and contingency plans

Helping keep our clients and our IBMers safe, secure and healthy.
Accelerating 24x7 detection and response capabilities

Axel Schittek
Vice President IT Governance
Fiducia & GAD IT AG
is the IT service provider for the cooperative financial banks in Germany

Fiducia & GAD IT AG provides Services and infrastructure for about 900 Banks

- 1.6b annual revenue in 2018
- 36k self service terminals, 166k workstations, 79m active accounts
- 4,400 experts and consultants in the delivery organisation
- 2x2 data center with 9 mainframes

IBM Think 2020 | Accelerating 24x7 detection and response capabilities @ Fiducia und GAD IT AG | Axel Schittek | Öffentlich (C1)
Focusing on customers in 4 target markets

We provide services to customers in four target markets focussing on our owners in the Cooperative Financial Network (CFN)*

Cooperative Financial Network)*

Cooperative Banks: Volksbanken Raiffeisenbanken

Companies within the Cooperative Financial Network

Cooperative Specialized Commercial Banks

Market Customers

Founded Principle

Integration Promoters

One IT in the CFN

Focused Market Expansion

*) Cooperative Financial Network (CFN) – Genossenschaftliche Finanzgruppe Volksbanken Raiffeisenbanken
Security operations in four disciplines

**Use Case Library**
- Standard frameworks (i.e. MITRE ATT&CK)
- Own advanced threats (i.e. ATM)
- Regulatoric requirements
- Compliance requirements (i.e. PCI-DSS)

**SIEM Core Operations**
- Identify and configure log sources
- Connecting of log sources
- End-2-End testing
- 7*24 On-Call SIEM operations

**Security Monitoring**
- 7*24 Monitoring & First Response (Level 1)
- 7*24 On-Call Incident Response (Level 2)
- Runbook Definition
- Threat Hunting

**Threat Intelligence**
- SIEM Use Case Engineering
- Threat Intelligence
- Automation & Reporting
Use cases: agile, industrialized life cycle management
Security incident response process

Stakeholder

SOC

SOC Level 1
24x7

SOC Level 2
Fiducia & GAD IT AG

Level 3
Fiducia & GAD IT AG - Security Management

Security Incident/QRadar Offense detected

QRadar Offense takeover → Incident Ticket initiation → Runbook Treatment → End Level 1

On request:
Level 2 SOC Hand Over → Final Treatment

On request:
Level 3 involvement

On request:
Initiation of use case enhancement

Reporting

SOC Level 1 – daily reporting

Additional daily reporting

Daily reporting verification

IBM Think 2020 | Accelerating 24x7 detection and response capabilities @ Fiducia und GAD IT AG | Axel Schittek | Öffentlich (C1)

© Fiducia & GAD IT AG 11
Our structured but agile approach delivers

**Prevention**
- Infrastructure
  - 4 data center
  - 35k log sources configured

**Detection**
- SIEM QRadar
  - ~100 HW Appliances
  - ~400k EPS capacity

**Reaction**
- SOC
  - 24*7 Security Monitoring with on-call Incident Response
  - Use Case Library
  - Runbook Library

Challenge with COVID-19

Switch a Cyber Defense Center from on-site to remote work in just one week
And the journey goes on

IBM QRadar Advisor with Watson
Early Beta Tester

IBM QRadar DNS Analyzer
Joined Development

FIDUCIA GAD
ZUKUNFTSERFAHREN

IBM

agree21SIEM & VR-SIEM
Project delivery
Improvising during chaos

76% of organizations do not have a consistently applied incident response plan

1 in 4
No incident response plan in place at all
What we’re seeing from security intelligence?
COVID-19 and the impact on cyber intel and security

Observations:

- Increased spam volumes
- Greater attack surface
- Increase in targeted malware from nation-state actors
- Targeting of health care facilities and personnel
- Corporate networks vulnerable through work-from-home employees

88% of global organizations have encouraged or required employees to work from home.
COVID-19 themed spam and related attacks

- Emotet Malware
- Trickbot Malware
- Oski Malware
- Lokibot Malware
- AutoIt Malware
- Agent Tesla
- CovidLock Malware
- Blackwater Malware
- Kpot InfoStealer Malware
- Hawkeye Malware

First email captured

Parallax Rat

Source: X-Force Exchange COVID-19 Collection
## Crisis management for cyber: Key characteristics

<table>
<thead>
<tr>
<th>Three common elements</th>
<th>Agile vs heavy process that enables quick decision making</th>
<th>Cross-functional teams (avoid siloes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat to organization</td>
<td>Whole-of-business response (entire business, not just IT/Security)</td>
<td>Culture that expects duty to respond, duty to act</td>
</tr>
<tr>
<td>Element of surprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short decision time to respond</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Empower your security team with COVID-19 readiness

Threat Intelligence Vigilance

Increase in spam activity related to Covid-19, high volume from China

Global topic of interest allows spammers to scale targeting (rather than focusing on a country holiday)

Targeting of healthcare facilities and personnel with DDoS

Increasing complexity and count of malware associated with Covid-19 Spam

Incident Response Readiness

Rehearse your cyber crisis management plan to call on your IR provider when team is WFH

Use Quad9 (free resource from IBM and partners) to detect spoofed and malicious domains

Go back to those security basics. The likely vector is spam. Reinforce to avoid suspicious links.

Threat Intelligence Mitigation

Share threat intel with X-Force IRIS via IBM Security Partner, TruSTAR.


Resources

IBM X-Force IRIS

IBM X-Force Exchange COVID-19 Collection
https://exchange.xforce.ibmcloud.com/search/coronavirus

X-Force IRIS COVID-19 Threat Intelligence Enclave brought to you by TruStar
https://www.trustar.co/en/covid-19
Thank you

**John Wheeler**  
BISO, IBM Security  
VP of Strategy and Innovation, Services and Integrated Solutions

**Wendi Whitmore**  
Vice President, X-Force Threat Intelligence, IBM Security

**Axel Schittek**  
IT Governance Leader, Fiducia & GAD IT AG
Notices and disclaimers

© 2020 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity. IBM products and services are warranted per the terms and conditions of the agreements under which they are provided. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
Notices and disclaimers continued

It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at: www.ibm.com/legal/copytrade.shtml.