CO DĚLAT, KDYŽ BEZPEČNOSTNÍ OCHRANA SELŽE? ZKUŠENOSTI S ŘÍZENÍM KYBERNETICKÝCH INCIDENTŮ

X-Force IRIS - **e-government 20:10**

2020-09-08

Michal Martínek
Security Services CEE

michal_martinek@cz.ibm.com

IBM Security

IBM

Incident response - Overview

Step by step of IRIS team support in case of security incident

Phase 1 – Identify and Investigate

1. **Call to IRIS team hotline**

- Experienced Forensics consultant

2. **Incident Triage**

- Current state assessment
- Set up Incident timeline
- Any behavioral changes (what was happening last days and weeks)
- Understand what is the impact of current situation (business, processes..)
- Any outbound communication
- What is compromised – accounts, permitions…
- Suggest next steps

Timing: Couple hours

Phase 2 – Get Visibility and Control

1. **Gain Visibility**

- Identify Back Door or CC
- Any hidden devices
- What and how was compromised
- Is it still active
- Block out the perimeter

2. **Tooling**

- EDR as part of service (Carbon Black, Crowdstrike)
- Collection of security event and relevant logs (AV, FW, Proxy, AD, SIEM etc.)

2. **Investigation**

- Fallow the IR playbooks
- Analyses

Timing: Based on incident complexity 48-72 hours

Phase 3 -Remediation

Bring it back

1. **Advice for remediation**

- Step by step suggestions how to proceed with remediation
- Outdated OS
- Perimeter patching
- AD Admin Groups
- Permition and Password changes
- Is it still active
- Timeline definition
- Back up running
- Is it still active

2. Malware analysis

- IRIS team will help with isolation and analysis of malicious code

3. Reversed Engineering

- IRIS team will use reversed engineering to stop the malware spread in your environment

Phase 4 – End of Engagement

Closing Phase of incident investigation.

End of engagement when everything is up and back

- disaster recovery phase

Incident report

- Management, Insurance, Regulator

Lessons learned

- As part of incident report client will receive set of recommendation for prevention of incident reoccurrence
- IRIS team can provide support with improvement of Incident response and other relevant topics with its **Proactive Services**

Timing: Usually couple days

X- Force IRIS

In case of security Incident

- DO NOT panic or react without a plan.
- DO NOT discuss the incident with others unless directed.
- DO NOT shutdown, power off or backup affected systems.
- DO NOT remotely access systems unless necessary.
- DO NOT use common privileged domain credentials.
- DO NOT install or execute any software on the systems.
- DO NOT conduct Anti-Virus or similar scanning processes.
- DO NOT attempt to retaliate against perpetrators.

Call the X-Force Hotline

IBM X-Force IRIS Vision Retainer

- The right skills and available experts, assets
- Experience to deal with the most critical incidents and breaches in the world.
- Helping clients to get back visibility and control during breach and approach incident response proactively.
- The Vision Retainer establishes a pre-negotiated set of terms and conditions for IBM to provide Incident Response (IR) services
- These terms provide the legal framework to protect sensitive information during an IR event.
- Vision Retainer may allow clients to convert existing retainer hours to proactive services and to purchase additional hours at a reduced, pre-negotiated rate

Vision Retainer service Tier 2

- 24/7 hotline support
- Kickoff Workshop
- 2 Proactive Services Units
- Quarterly Status Review
- Triage: 1 hour
- 80 annual subscription hours for IR or proactive services
- Additional discounted hourly staff-rate
- Own EDR and investigation tools
- Onsite: 24-48 hours

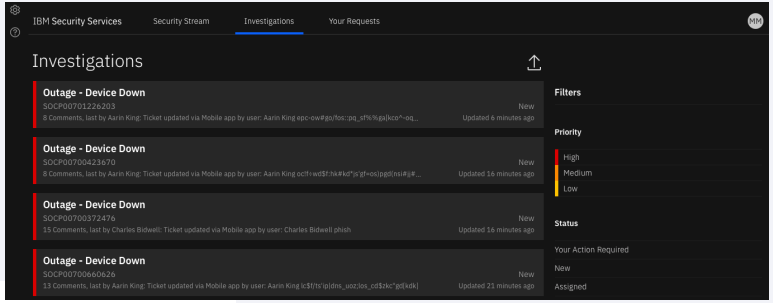
Proactive services

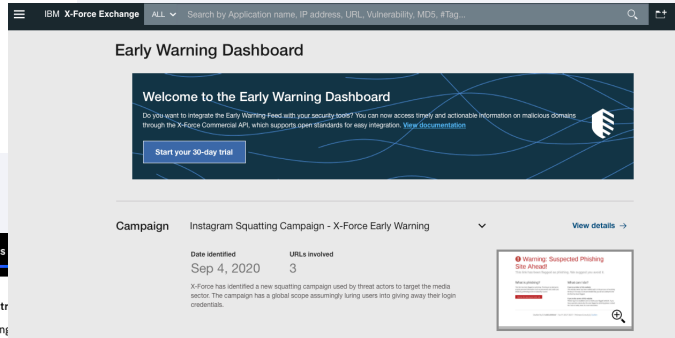
- Incident Response Program Assessment
- CTI Program Assessment
- Incident Response Playbook Customization
- Standard Tabletop Exercise
- Dark Web Search Services
- Cybersecurity Incident Response Plan –High Level Review
- Security Incident First Responder Training
- Strategic Threat Assessment
- Cybersecurity Incident Response Plan –Full Development
- Active Threat Assessment
- Custom Tabletop Exercise
- Cyber Crisis Management

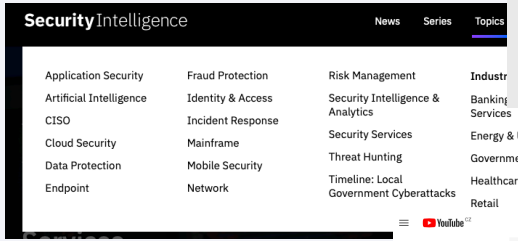
X- Force IRIS 24x7 Hotline

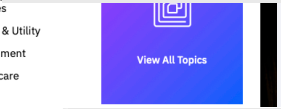
IRIS EMEA

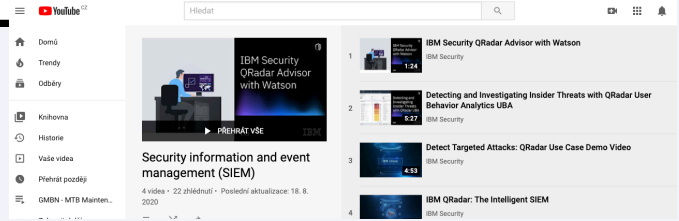
- Poland: (+48) 22 306 22 34
- UK: (+44) 20 3684 4872











https://apps.apple.com/us/app/ibm-security-services/id1350535586

https://center.sec.ibm.com/stream

https://securityintelligence.com

https://exchange.xforce.ibmcloud.com

https://www.youtube.com/ibmsecurity

NAKIT/NUKIB Minimální bezpečnostní standard v1.0
Logovací baseline a Usecase doporučení

Overview

X-Force IRIS Vision Retainer

Proactice services

IBM X-Force IRIS Proactive Services

Proactive Service Offering

Incident Response Program Assessment

- Assessment based on People, Process, Technology view on organization
- Predefined specialized questionnaires, documentation review and interviews
- Incident Response Program Assessment report will demonstrate current maturity of incident response

Threat Intelligence Assessment

- Assessment of Threat intelligence feeds used currently used by client
- Assessment of utilization of Threat Intelligence information in client’s environment
- Set of recommendation for improvement of clients Threat Intelligence

Playbooks Customization

- Assessment of existing incident response playbooks on customer side
- Customization of existing playbooks or delivery of missing playbooks
- About 5 incident response playbooks per one Proactive service unit

IBM X-Force IRIS Proactive Services

Proactive Service Offering

Tabletop exercise - Test

- Specific training scenarios prepared for client IR team
- Step by response walkthrough (who, what, when)

Darkweb analysis

- IRIS team will search the darkweb and look for information about your organization (proactive)
- As a result, you will be aware if the is the chance that some attack is planned on your organization or if it is already happening and you just do not know about that

Security Incident First Responder Training

- Deep dive technical training for your IR specialist
- They will learn how to effectively utilize existing security tools in your environment
- Your team will learn various incident investigation skills (e.g. OS investigation on Linux, Windows etc.)

IBM X-Force IRIS Proactive Services

Proactive Service Offering

Active threat assessment

- IRIS team will deploy advance EDR solution in your environment for couple days
- Active search for threats in your environment
- Recommendation to fix the existing issues

Premier Threat Intelligence

- IRIS team will provide for client the customized Threat Intelligence
- Threat intelligence can include YARA rules and SIEM rules to fasten reaction on new threat

Strategic Threat Assessment

- Identification of information assets which can be interesting for attackers
- Description of probable vectors of attacks
- Threat assessment and delivery of existing threat landscape

Where we are now

- Largest enterprise cybersecurity provider
- Leader in 12 security market segments
- 8,000+ security employees
- 20+ security acquisitions
- 70B+ security events monitored per day

War Story

Education Industry

24X7 breach hotline: US: 1-888-241-9812 Global: (+001) 312-212-8034

IRIS Vision Retainer team discovered and blocked MegaCortex ransomware campaign

For the full story: blog post

Problem

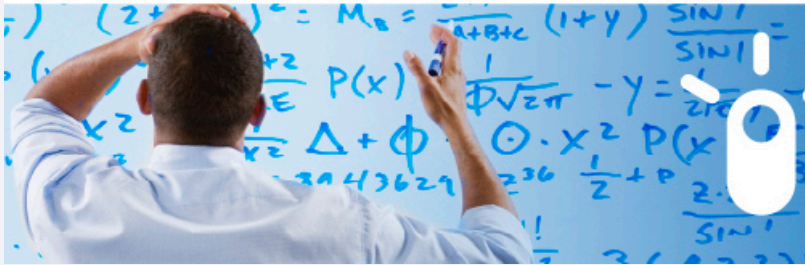
The client detected a possible security breach within their network based on suspicious network traffic to a known malicious IP address associated with illicit CobaltStrike activity. CobaltStrike allows facilitated command-and-control (C&C) on compromised systems and is used for lateral movement within the compromised environment.

Solution

The client contacted the IRIS incident global hotline and utilized their Vision Retainer subscription to deploy the IBM incident response team for boots-on-the-ground emergency incident support. This team deployed an endpoint detection & response (EDR) tool to help determine the scope of the incident and gain visibility into the network. Further analysis revealed the threat actor had already gained privileged account access on the network. After several days of investigation, IRIS observed the threat actor becoming active in the environment by uploading MegaCortex ransomware and scripts to deploy the ransomware enterprise-wide. IRIS quickly notified the client and worked with them to block the attacker from achieving their objective.

Outcome

With early detection and readiness through the client's Vision Retainer subscription, the MegaCortex attack that could have affected more than 15,000 endpoints and taken months to remediate was averted. Had this attack developed into the destructive phase, the cost could have been much worse — destructive attacks studied by IBM X-Force had an average cost of $239 million.



War Story

Public Sector Industry

24X7 breach hotline: US: 1-888-241-9812 Global: (+001) 312-212-8034

IBM X-Force IRIS works with city of Los Angeles to combat cybercrime

For the full story: press release

Problem

A client was looking to partner with a leader that could design, build, deliver and operate a cyber threat platform that provides accurate and up-to-the minute cyber threat data from both common and unique sources.

Solution

IBM X-Force IRIS partnered with enterprise intelligence management provider, TruSTAR to deliver a cloud-architected solution on AWS.

The collaboration leverages IBM Premier Threat Intelligence and Enterprise Intelligence Management with TruSTAR to make it easy for organizations to share threat information.

Outcome

The outcome is a platform that correlates key information with the associated threat group and the latest attack campaign that allows businesses to determine their level of risk.

Local businesses in Los Angeles can now share threat intelligence and use this information to improve their cyber defense.

Our team

All hold one or more industry standard certifications:

- CCE – Certified Computer Examiner
- CIFI – Certified Information Forensics Investigator
- GCFA – GIAC Certified Forensics Analyst
- CISSP – Certified Information Systems Security Professional
- CFCE – Certified Forensic Computer Examiner
- CISM – Certified Information Security Manager
- CISA – Certified Information Systems Auditor
- GREM – GIAC Reverse Engineering Malware
- GCIH – Certified Incident Handler
- EnCE – EnCase Certified Examiner
- X-PERT – X-Ways Professional in Evidence Recovery Techniques

Our analysts are experts from variety sectors:

- Federal – Special Agents and Forensic Examiners
- Police Detectives
- Department of Defence Agencies
- Air Force Office of Special Investigations
- Army Criminal Investigation Division
- Private Sector Security Firms

Some have authored books and papers on a variety of topics:

- Cisco router forensics and hardening
- Malware behaviour patterns
- Digital forensics and tools
- SANS First Responder
- CSIRP development and best practices
- Contributions to X-Force trend reports