BLACK CELL
Protecting critical infrastructures

Remote Work Monitoring Whitepaper

Table of contents

1. Remote Work, Mobile Work, Home Office

1.1 What is the purpose of a home office?

Remote work is not a specific occupation, but rather a flexible working arrangement, definable for specific tasks. Tasks can be performed remotely that

- require mental activity,
- they rely heavily on information processing and ICT technologies
- have well-defined objectives and clearly measurable results,
- the work is done on a computer,
- communication takes place electronically, primarily via the Internet.

Software development, project management, certain call-center tasks, accounting, payroll accounting are all examples of tasks that "made" for remote work.[1]

The remote worker works in his home utilizing the same device as they would in the office: their laptop. It connects to the corporate network via a VPN and the same corporate policies are enforced on the machine at home as in the office. The company doesn't work with paper documents, the employees do not carry heavy stacks of paper, instead the documents are available on central file servers. The security of company is ensured by not only technical and workflow organizational means, but also by administrative means including corporate policies and contractual obligations.

1.2 Increased Security Threat

Cyber-attacks are becoming more common and diverse around the world, yet companies are often ill equipped to detect and prevent them, according to a global survey of 1300 cyber security executives conducted by EY[2]. In the current pandemic situation, the introduction of work from home measures poses an increased security risk for companies if it is not accompanied by the creation of appropriate protocols and security systems.

Nearly 60 percent of companies have seen an increase in serious online attacks in the past year, according to EY's international research. Last year, nearly a quarter (23%) of successful fraud was linked to organized criminals, 21 percent were committed by activist groups, and 20 percent were caused by employee negligence. It took more than a month for 28 percent of the companies surveyed to recognize a serious security incident. Furthermore, 39 percent of organizations are unlikely to detect more advanced malware.

Based on the results of the research, companies need to protect their IT systems on more fronts than ever before, yet most decision-makers are only prepared for security tasks related to normal business operations. Although the vast majority of companies surveyed (92%) have a

[1] https://www.itbusiness.hu/archive/fooldal/rsscsatorna/Home_office-bol_nyomjak
[2] https://www.ey.com/Publication/vwLUAssets/2020_GISS_pdf/$FILE/ey-global-information-security-survey-2020-report.pdf

cyber security strategy, only one-fifth of executives trust the effectiveness of their defense systems.

2. Cybersecurity in Emergency Situations

One of the most important measures taken by employers in the current global health emergency in order to slow down the spread of the virus is the introduction of remote working. Employees are increasingly using their own devices in addition to company provided assets to access the organization's network, forcing companies to take immediate action. Protecting home workstations and devices has become a priority during this period.

Home networks do not have adequate protective measure and home workers often tend to conduct their private activities on corporate devices. If employees work on their own personal devices, then private and corporate activities will be completely indistinguishable without appropriate assets and supervision.

In the current unprecedented situation, it can already be seen that cyber-attacks have grown significantly[3], due to the fact that companies are concentrating on developing their remote work solutions and providing their core services, thus fewer resources are dedicated to IT security. This potential vulnerability is being exploited by attackers, spam and phishing campaigns are becoming more focused, malware and ransomware attacks are becoming more widespread, and there has been a significant increase in hacker activity affecting users and services[4].

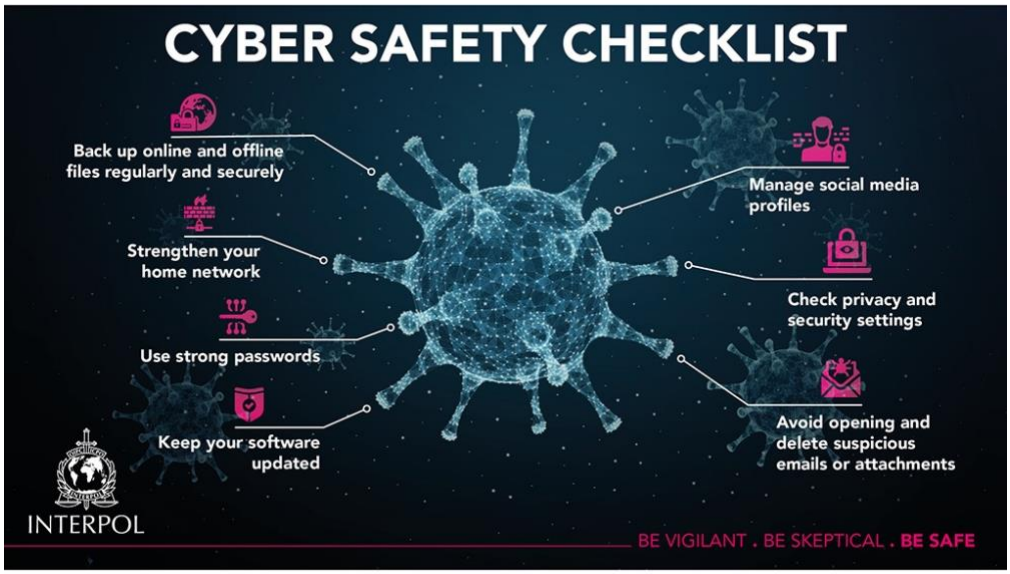


Figure 1
https://www.interpol.int/var/interpol/storage/images/_aliases/gallery/1/0/3/0/230301-1-eng-GB/COVID19_Infographics_mrt20_0211.jpg (2020.04.29 11:48)

[3] https://www.pwc.com/us/en/library/covid-19/cyber-attacks.html
[4] https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

2.1 Suggestions for Making Working from Home Safer

If a dedicated corporate asset is not provided (Figure 1):

- Make separate backups of your work and personal data if you use one device for multiple purposes.
- Create different user profiles if your computer is used by others (family members). All accounts should be password protected without administrator privileges and your password should not be known by anyone else. Only you should have administrative authority on your machine.
- Always check the legitimacy of prompts that ask for a password, be it online or in an application
- Keep your software and system up to date.
- Keep your antivirus solution up to date on all possible devices connected to your home network.
- Be careful while browsing and opening emails.
- Check the security of your home network, especially the wireless (Wi-Fi) network, enter a fresh strong password and use the most modern encryption allowed by your device (> WPA2). Turn off the WPS pin function if not needed.
- Only download and install legitimate content from trusted sources.
- Update the passwords of your online and social media accounts (Lowercase, number, special character) and use 2-factor authentication where possible!
- If possible, only visit websites that have SSL certificates (https: //)
- Only install legitimate apps on your mobile devices from the manufacturer's official app store and pay attention to what permissions you give these application (e.g.: A card game does not need to access a microphone or to send an SMS.)
- Keep your passwords confidential, don't store passwords directly in your browser, use a master password if necessary. Recommended password managers: LastPass, KeePass
  https://chrome.google.com/webstore/detail/lastpass-free-password-ma/hdokiejnpimakedhajhdlcegeplioahd
  https://keepass.info/

A recommended, reliable, and free antivirus program:
https://home.sophos.com/en-us/download-antivirus-pc.aspx

Assess the security level of your computer / workstation based on international recommendations and apply the recommended steps and settings:
https://learn.cisecurity.org/cis-cat-lite

When browsing the Internet, use an ad blocker/script blocker:
https://chrome.google.com/webstore/detail/adblock-plus-free-ad-bloc/cfhdojbkjhnklbpkdaibdccddilifddb?hl=hu

3. Black Cell's Solution

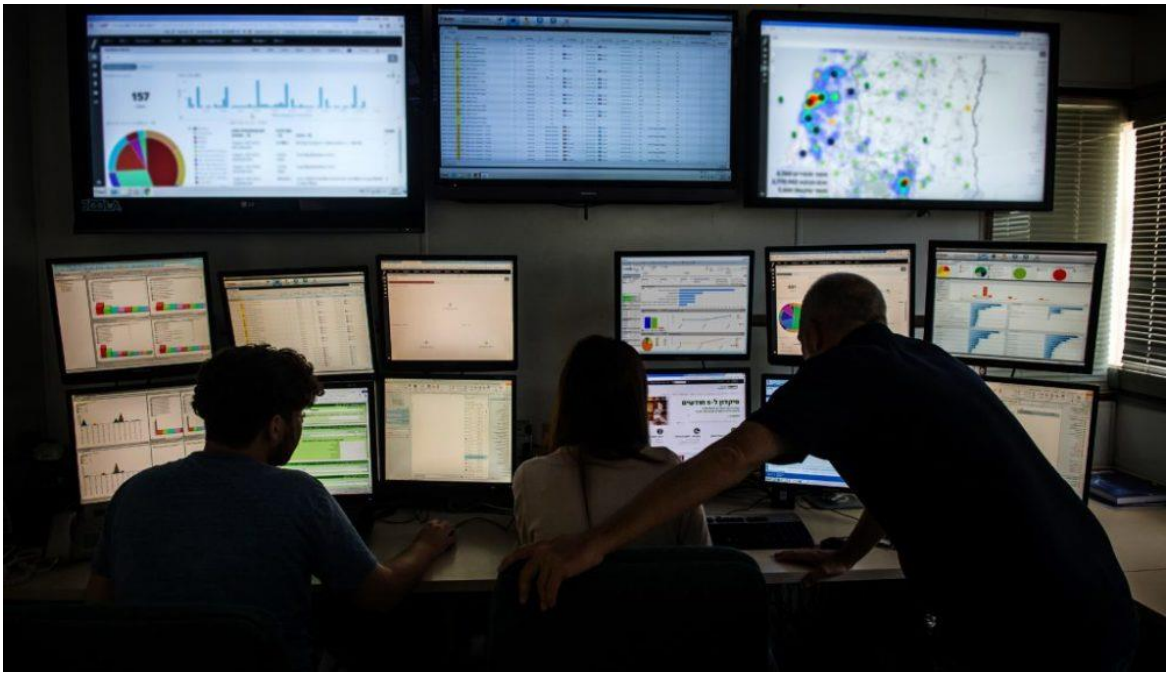
The goal of our company is to help employers adapt to employees working from home, as well as to promote the cyber security of their employees.

3.1 Home Office monitoring with Splunk Enterprise and IBM Qradar

Our service focuses primarily on users working from home and is made available to organizations that already have an integrated and configured IBM QRadar or Splunk Enterprise log analysis systems.

If there is no dedicated solution for endpoint monitoring, such as EDR, DLP, MDM, we can develop efficient monitoring methods based on log collection. On the other hand, if there is a dedicated solution for endpoint monitoring then we can extend its functionality, with automatic analytical and alarm system specialized for monitoring remote work activities.

Using correlation rules, automated alarms, dashboard visualizations, and dedicated Use-Cases for working from home, we can increase the traceability and manageability of your IT security operations.



The person or department designated for supervision receives reports and statements, and those responsible for IT security receives automatic alerts that may indicate a cyber security incident. The scenarios (playbooks) included in the Use-Case packages contain a detailed and accurate description of how to investigate and remedy the detected events.

Deployment and configuration requires the installation of an agent on the endpoints, which can be done centrally for users of Microsoft Active Directory domain controllers. In cases where this is not possible, we are available to help you plan the deployment. Logs are normalized and filtered on the remote workers device, and the speed at which logs are sent can be adjusted to avoid overloading the VPN.

The solution not only enables IT security monitoring, but also provides various methods to monitor the effectiveness of remote work in companies where such working arrangements have not been previously implemented. The results and outputs of various functionalities are displayed on a dashboard which the customer can access and may filter further. A report from any module is available on demand at any time or can be scheduled. (Figure 2-3)

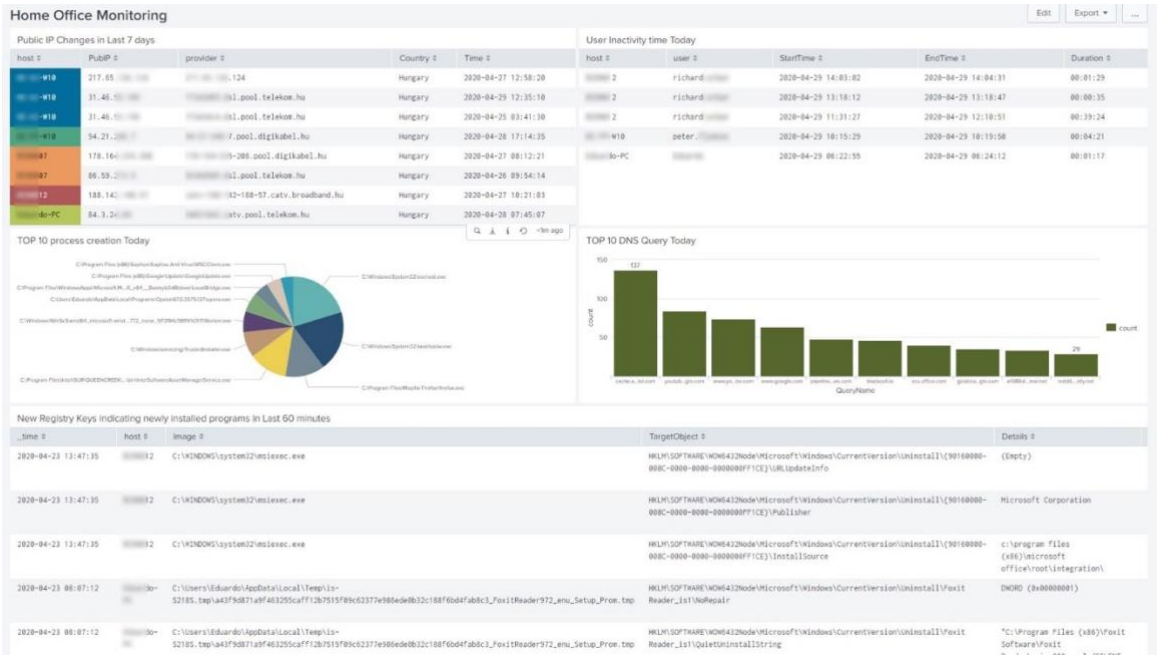


Figure 2

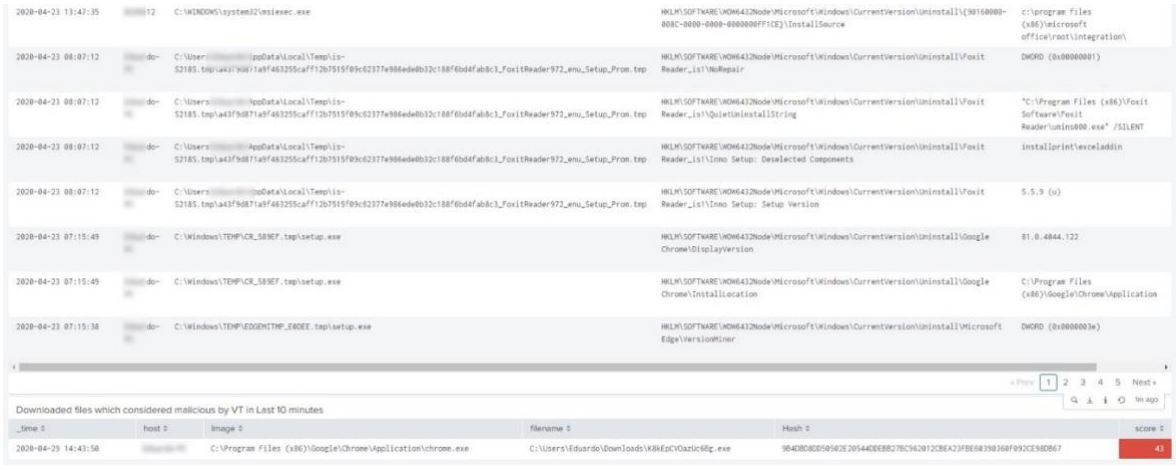


Figure 3

3.2 Technical Possibilities

The solution can work entirely on a log analysis basis in the following cases.

- Enterprise device with domain membership
- Enterprise device without domain membership
- Own device without domain membership

Supported operating systems:

- Microsoft Windows 7,8,10
- Ubuntu Linux *
- Debian Linux *
- Mac OS X *

* For Splunk Enterprise only

The endpoint agent buffers events for up to a week when the connection to the central node is lost. The connection to the central node is encrypted and compressed.

The solution monitors, among other things:

- Network connections and changes
- Installed and removed programs and related registry values
- File integrity monitoring
- Check downloaded files using Threat Intelligence
- Access and verify DNS requests and domains using Threat Intelligence
- Command line and Powershell logging
- Harmful behavior and toxic combinations
- Changes to local users and groups
- What programs are used at what times
- Workstation and device usage statistics
- Other corporate IT security policy monitoring

Performs correlations with data sources within the enterprise infrastructure such as:

- Firewalls, VPNs
- Directory Servers
- File Servers
- Cloud Services, O365, AWS
- Mailing Systems

There are up to 20 Use-Cases that can be utilized in a SOC, which includes both alarms and detections.

Our solution is based on Microsoft Windows Sysinternals Sysmon and Linux auditd, for which we provide advanced configuration and support with continuous monitoring.

4. Why Trust Us?

Black Cell was founded in 2010 in Hungary. Our team of highly skilled cybersecurity professionals possess all the relevant knowledge and experience, to successfully develop and maintain a Cybersecurity Operations Center, which is substantiated by our numerous domestic and international references. A strict service level agreement (SLA) governs our operations and we have liability insurance for $1 million. We operate a 24/7 live monitoring and alerting center every day of the year for our domestic and foreign customers.

Our Computer Emergency Response Team (CERT) has been certified by Carnegie Mellon University. The team consists of engineers from four different IT security disciplines who serve in the SOC simultaneously. The specializations are offensive security (ethical hacking), defensive security (log analysis), threat hunting and cyber intelligence (CTI). Additionally, our network security and product-specific support staff are always available.

5. Our Certifications