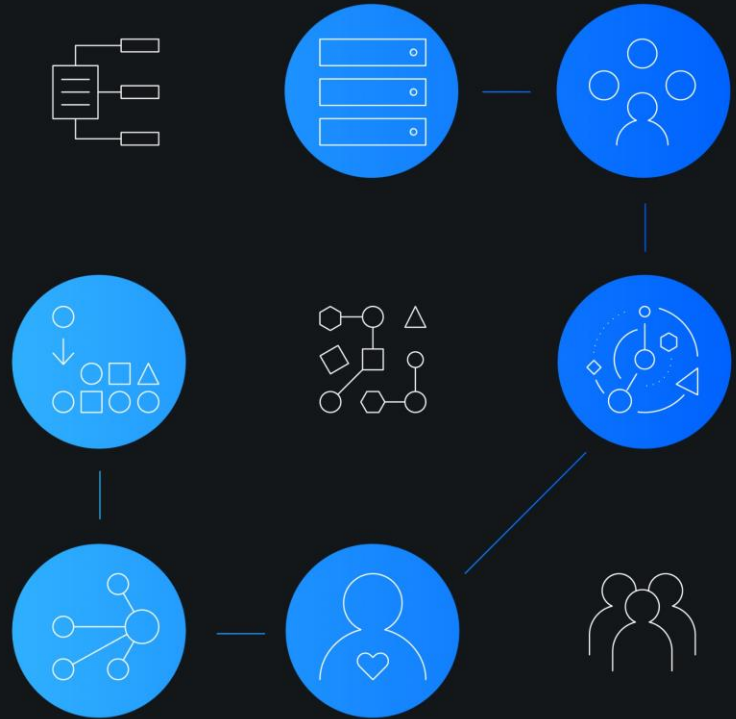


Welcome to

IBM Security Virtual User Group Day



IBM Security Trusteer

Protecting your remote workforce with actionable risk insights

Ayelet Avni – IBM Trusteer Offering Management Strategy Lead

May 2020

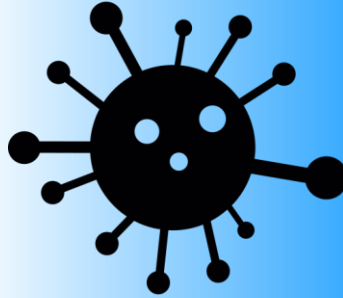
COVID-19 has changed the security landscape

14,000%

increase in COVID-19 related
spam and phishing

84%

increase in remote working tools since
the start of February

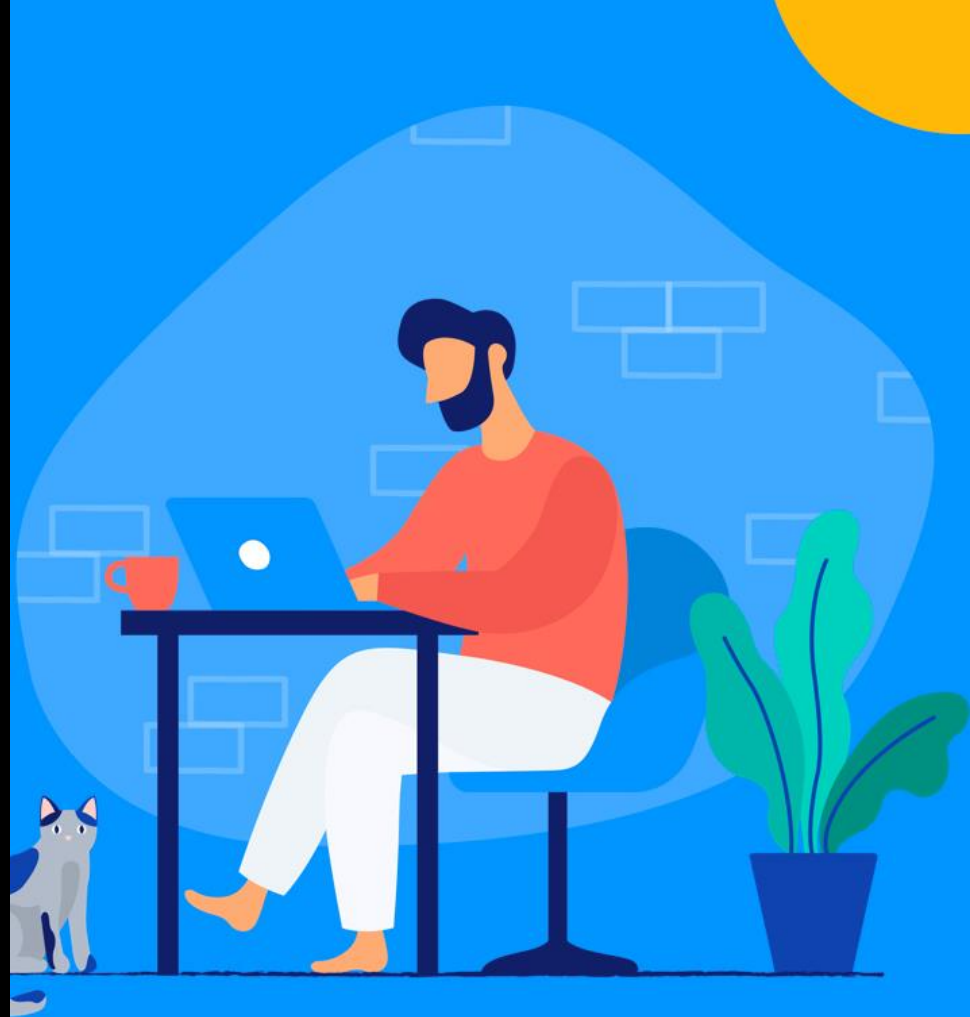


COVID-19



Office workforce		Remote workforce
Corporate owned and managed	Devices	Home / BYOD / Corporate
Secured by network and device controls	Access to corporate applications	Not at all / Not secured / Remote Desktop / VPN
Zero, but trust is in the other security controls	Risk visibility in the digital identity	Zero

A new digital channel
has emerged



New digital channel risks emerge when managing a remote workforce

27%

of breaches occur
due to compromised
credentials¹

With less control over who is accessing systems and from which device, password-based authentication and traditional MFA methods are even less secure than normal

10 billion

stolen credentials
on the dark web¹

Traditional assumptions of access from within the corporate network and using a known and trusted device are no longer valid

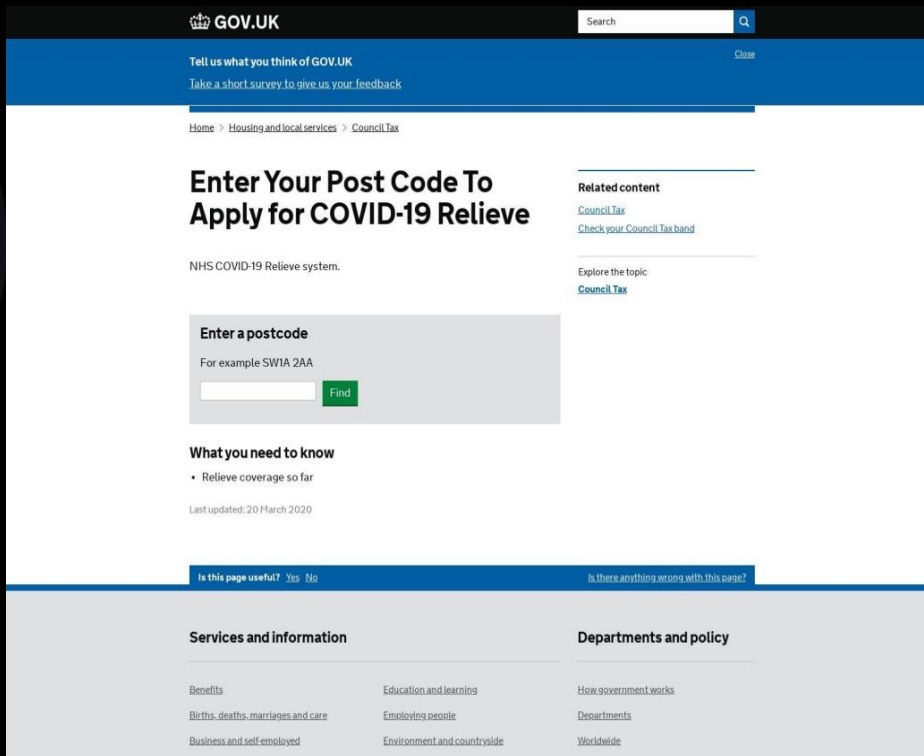
1 in 13

web requests
lead to malware
infection²

Business continuity requires immediate support for BYOD without the ability to fully manage a device, determine its health, control what is installed, or who is using it

Phishing for financial credentials

- Abuse of the compensation citizens should receive due to the COVID-19 outbreak
- Imitation of Government related institutions and financial organizations to steal the victim's information



GOV.UK

Search

Tell us what you think of GOV.UK
Take a short survey to give us your feedback

Close

Home > Housing and local services > Council Tax

Enter Your Post Code To Apply for COVID-19 Relieve

NHS COVID-19 Relieve system.

Enter a postcode
For example SW1A 2AA

Find

What you need to know

- Relieve coverage so far

Last updated: 20 March 2020

Is this page useful? Yes No

Is there anything wrong with this page?

Services and information

- Benefits
- Births, deaths, marriages and care
- Business and self-employed

Departments and policy

- Education and learning
- Employing people
- Environment and countryside

How government works

- Departments
- Worldwide

Workforce phishing

From: Service <no-reply-@support.com>
Subject: Your account access will be limited!
To: [redacted]

Cisco Security Advisory

Cisco CloudCenter Orchestrator Docker Engine

Critical

Advisory ID:	cisco-sa-20161221-cco	CVE-2016-9223
First Published:	2016 December 21 16:00 GMT	CWE-264
Last Updated:	2016 December 21 18:03 GMT	
Version 1.1:	Final	
Workarounds:	Yes	
CVSS Score:	Base 9.3, Temporal 8.1	

SUMMARY

The CVE-2016-9223 is a vulnerability in the Docker Engine Configuration in CCO. This could allow an unauthenticated user to inject arbitrary code into the container. To fix this error, we recommend that you update the Docker Engine to the latest version.

[JOIN](#)

From: Update on Corona for | [redacted] <maga@tus.tusdns.com>
Sent: March 30, 2020 12:56 PM
To: [redacted]
Subject: Staff Member Confirmed COVID 19 Positive ID:1871 Monday 03/30/2020

Dear Team,

We need to be extra vigilant now as we lost a colleague to the deadly Virus. Attached is a guideline on the next steps. Do not Ignore for your safety!!!

Regards,
Management

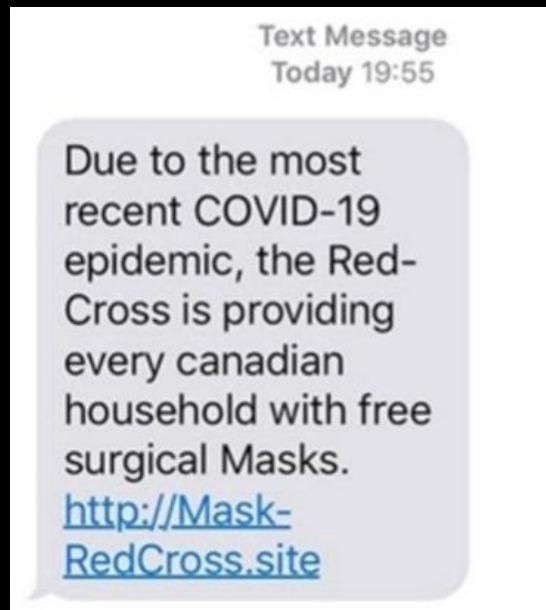
Sign in

Don't have a Microsoft account? Sign up

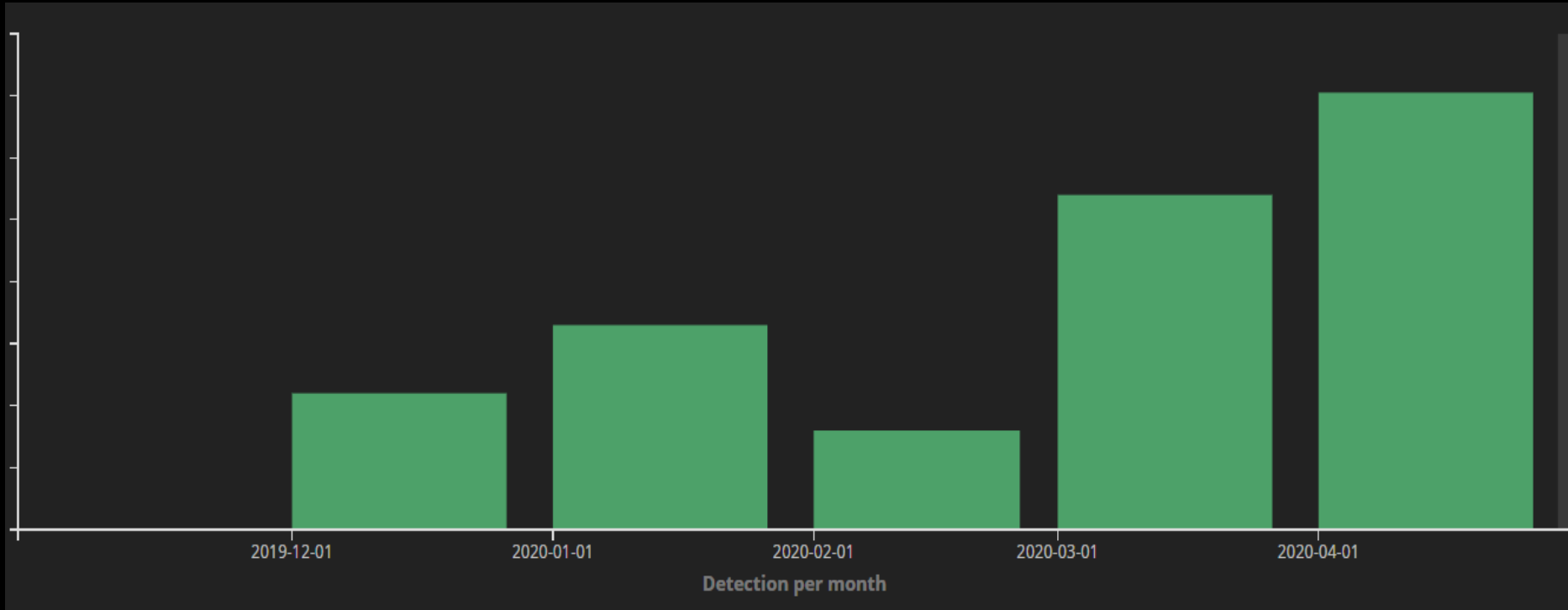
Office 365

Not signed in or password is incorrect. Please try again.

Increase in SMiShing & Vishing attacks



Malware infections



A sharp rise in March and April detections

Fake “Coronavirus Finder” App

Ginp Mobile Malware

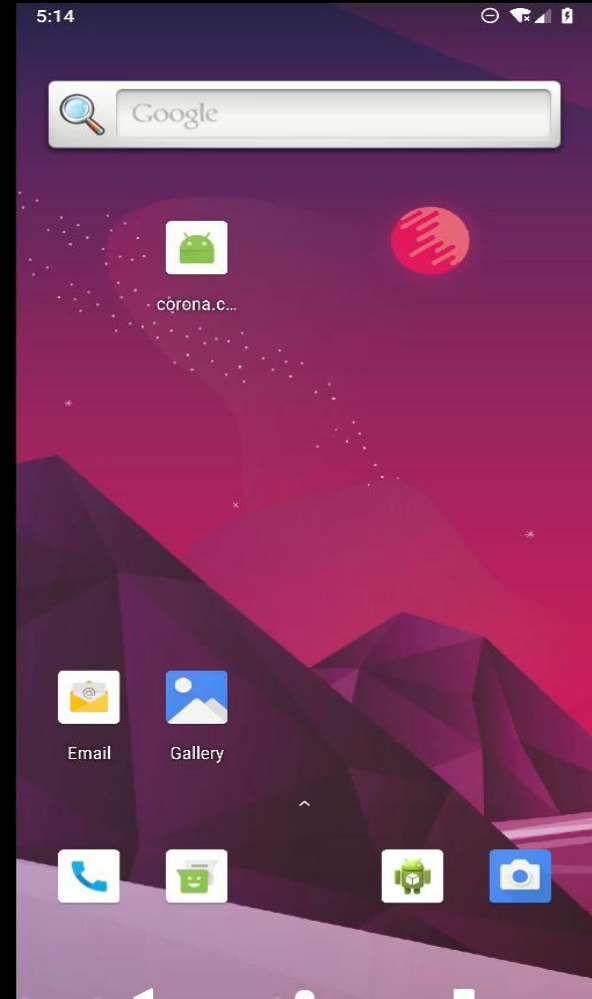
Started as an SMS stealer

Initially targeted Spain banking apps

Reused Anubis code after it leaked

Added advanced capabilities such as overlay screens and call forwarding

New version - expanding from Spain to additional countries and from banking to more industries



In these uncertain times, every organization needs to...



01

Help protect and enable your remote workforce

02

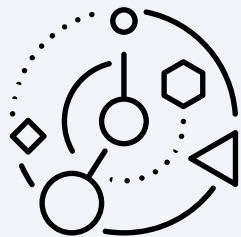
Help detect and respond to accelerating threats

03

Virtually extend your security team and quickly add expertise

Remote Workforce: Risk Increase

Compromised Devices



Remote access using an **unmanaged** personal device, at times **non-compliant**, may be infected with **malware**, at times **spoofed**, or has other **high-risk indicators**

Compromised Credentials



Malicious access using **account take over** : valid **credentials** that may have been **phished**, **acquired** (e.g. via **social engineering** scam) or otherwise **stolen**

Trusteer transparently validates multiple context domains to secure the user login

✓ **Device Intelligence**

Use of a new device, unmanaged infected or spoofed device attributes, virtual machine, or simply owned by malicious user that is attempting to access apps

✓ **User History**

Access from new device after the previous access was done from an infected device

✓ **Account Information**

Multiple users or devices are accessing the same account; or the same device is attempting access using different user credentials

✓ **Geographic Location**

The user attempted to login from different geographic locations during too short of a period of time

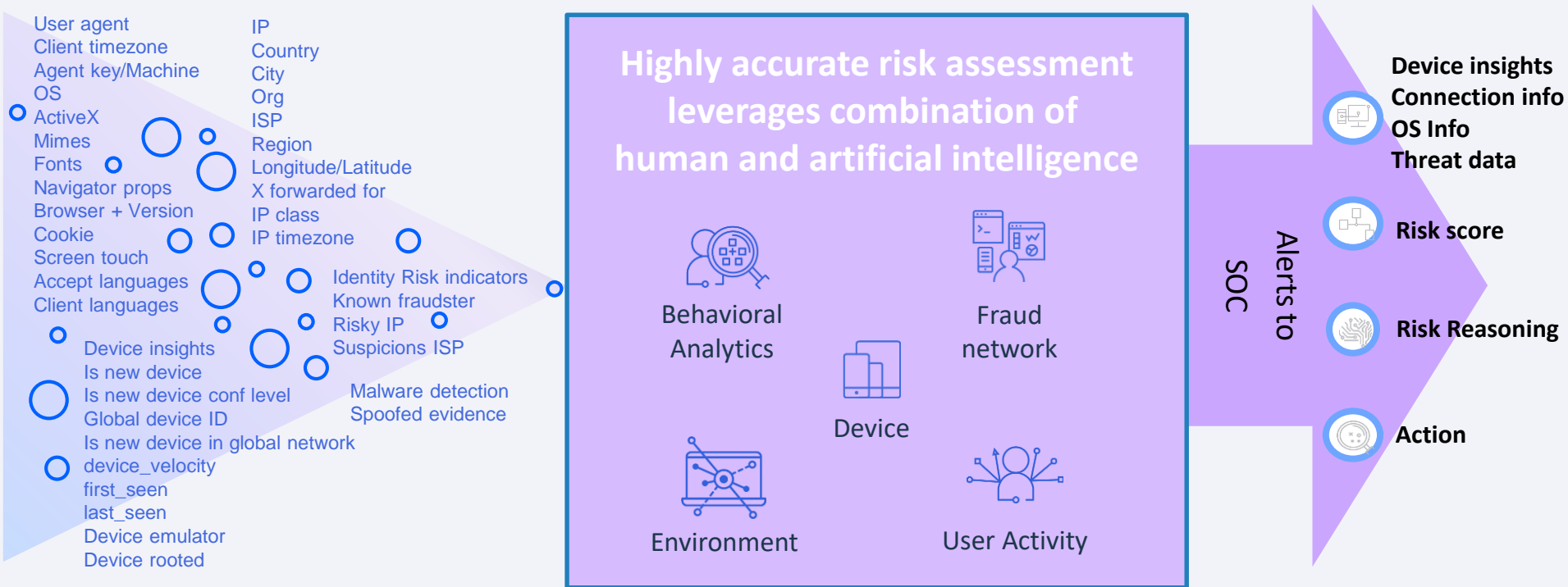
✓ **User Behavioral Analysis**

Detecting abnormal behavior for the user, access resources at an unusual time or from a new location or with suspicious or new browser configuration

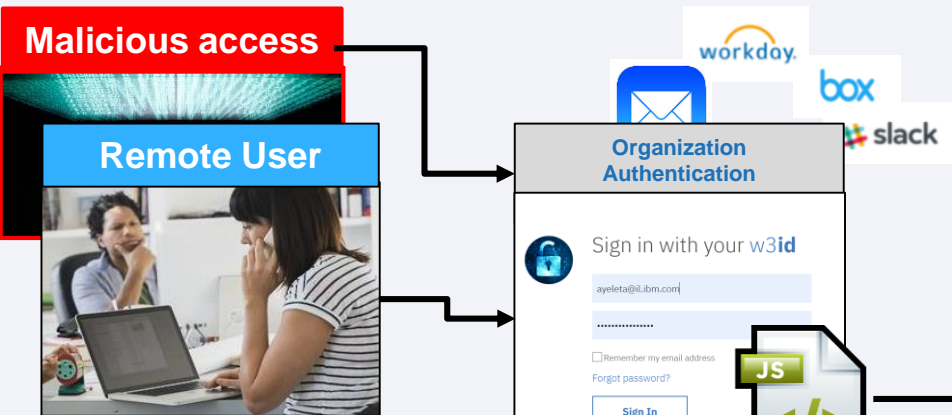
✓ **Known-bad consortium**

Access using known-bad characteristics: IP address, service provider (ISP), confirmed malicious device or device attributes

Hundreds of attributes are collected during login or single sign-on flow and fed to Trusteer for real-time risk analysis

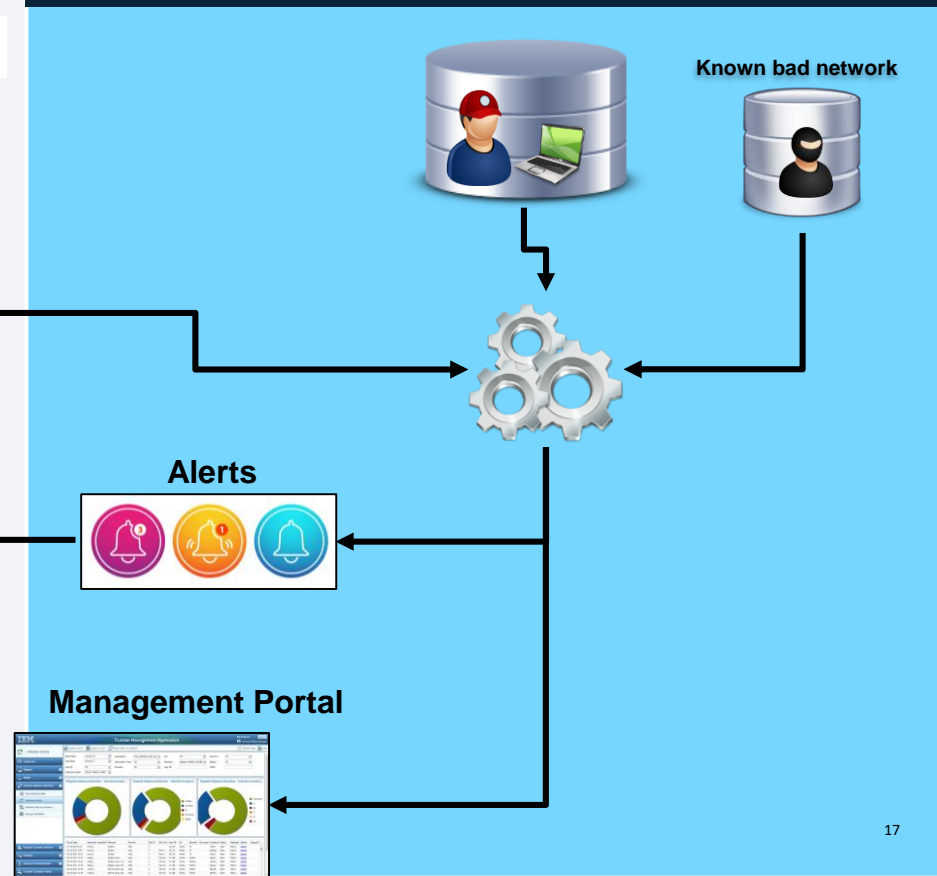


How does it work?



Integrate into existing SOC workflow:
(QRadar Integration)

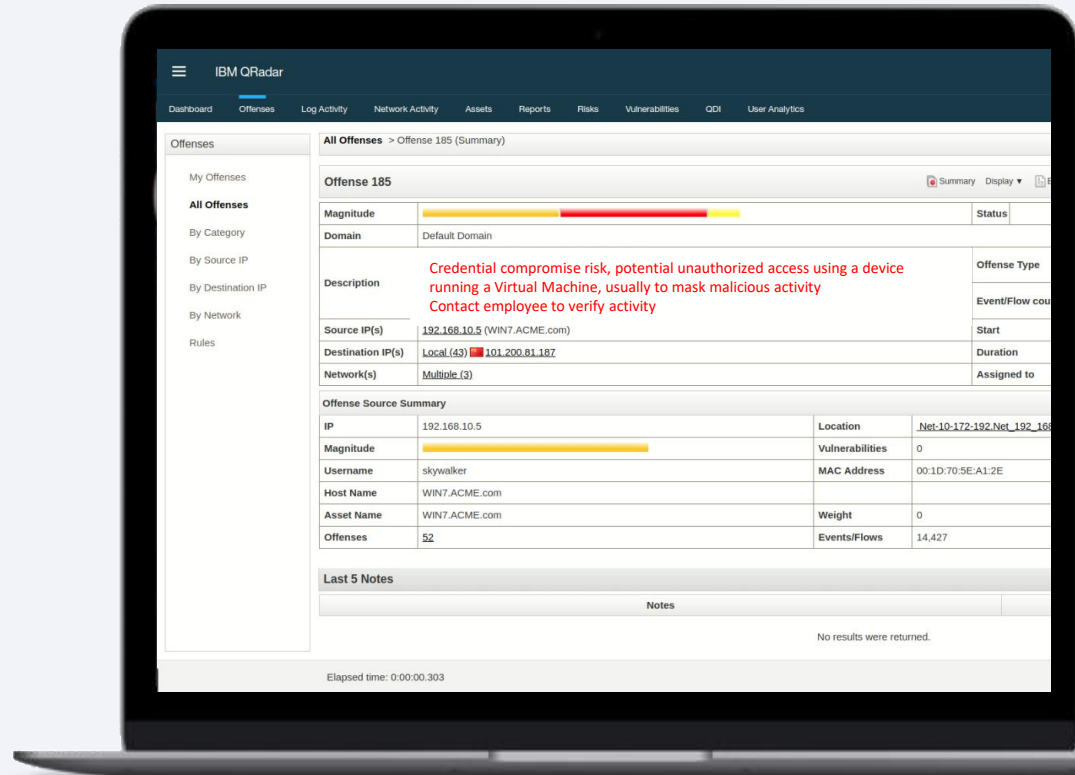
IBM Security Trusteer



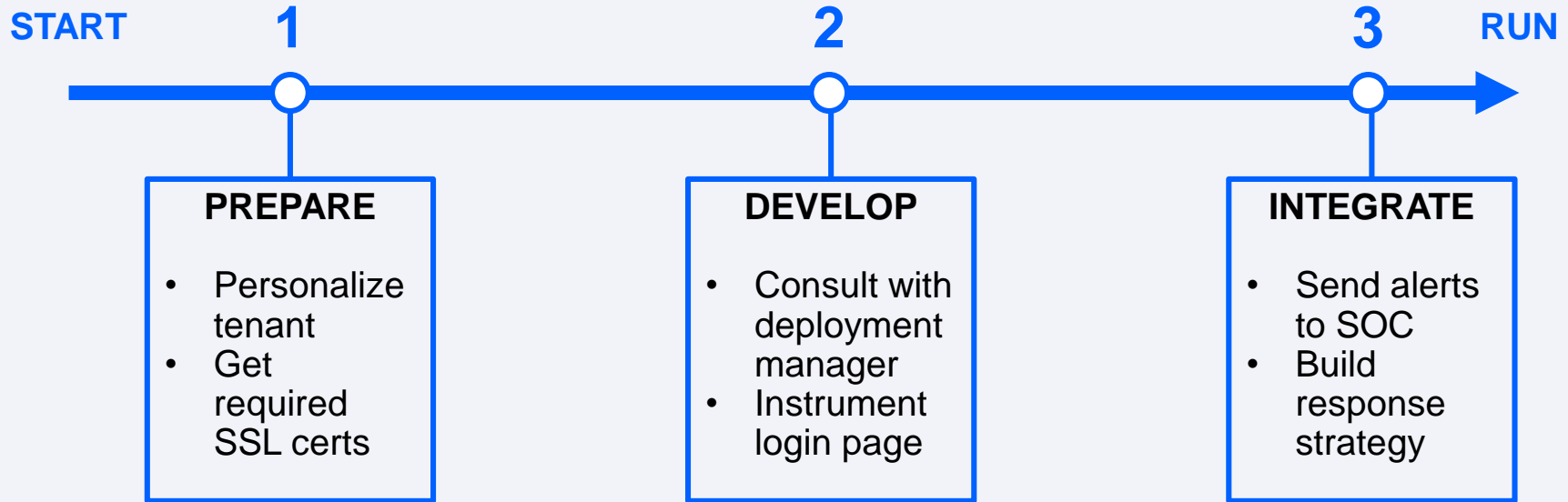
Easily integrate alerts into existing Threat Management workflow

1. **Integrate.** Alerts can be sent directly to SIEM, such as IBM QRadar.
2. **Orchestrate.** Automate remediating actions to protect critical resources using security platform, such as IBM Cloud Pak for Security.
3. **Respond.** Confirm malicious access in Trusteer dashboard to make the detection smarter.

Proof Point: European client was able to block more than 1500 cases of confirmed fraudulent access while alerting on only 0.04% of all transactions



Get up and running in a matter of weeks, not months



Transparently identify risk on workforce remote access

- ✓ **Nothing to install on the device:** Agentless solution means no need to install anything on the device and it is fully transparent to end users
- ✓ **Nothing to install in data center:** Remote, digital deployment through SaaS solution
- ✓ **Quick time to value:** Integrates into the existing organization's login page to protect hundreds of apps with no changes to backend identity system
- ✓ **Detect threats in near real-time:** Immediate visibility to all risky accesses from your remote workforce from either a managed or unmanaged device
- ✓ **Tie into existing SOC workflow:** SIEM integration allows for automated response to highly accurate alerts



Demo

Demo

Protect the remote workforce with actionable risk insights



Protecting more than **142 Million users** worldwide with **58 billion** data events processed every month



Full SaaS service, with unique combination of **machine learning** and **human intelligence**



Full **digital context**, with holistic view on the digital identity and the device remotely accessing your enterprise

IBM Security Community

8,000 Members Strong and Growing Every Day!

Sign up: <https://community.ibm.com/security>

User Group Day discussion: <https://ibm.biz/trusteer2-usergroupday> (share feedback, ask questions and continue the conversation after this session!)

Learn: The indispensable site where users come together to discover the latest product resources and insights — straight from the IBM experts.

Network: Connecting new IBM clients, veteran product users and the broader security audience through engagement and education.

Share: Giving YOU a platform to discuss shared challenges and solve business problems together.

IBM Security Community

Home Groups Local Groups Events Participate Resources All Communities

Learn, Network and Share in the IBM Security User Community

Collaboration is more important than ever before. In this user community of over 8000 members, we work together to tackle the challenges of cybersecurity.

Join the community

Tuesday 26 May	Guardium Virtual Users Group Monthly meeting for Guardium customers. To receive invitations to the VUG meetings, send an email to leila@us.ibm.com ■ Tue May 26, 2020 12:00 PM - 01:00 PM ET
Wednesday 27 May	Webinar: IT Security in the Post-Corona Threat Landscape It has become clear that the spread of the COVID-19 has also meant a spike in cybercrime. Fraudsters saw a golden opportunity to take advantage of a time when everyone was working from home and was vulnerable. ... ■ Wed May 27, 2020 08:30 AM - 11:15 AM GB
Wednesday 27 May	Virtual Cyber Threat Management PoT Event - May 27-28 As cyber threats (External and Insider), to your organization increase in number and sophistication, you need a balanced data management and threat analytics approach to handle Cyber Threat Management ... ■ Wed May 27, 2020 08:30 AM - Thu May 28, 2020 04:30 PM ET
Wednesday 27 May	Webinar: Identity & Access Management Capabilities to Support Remote Work Webinar Summary With the influx in remote work, your organization needs to ensure that the right people have the right to access the right systems and applications while working from home. Identity ... ■ Wed May 27, 2020 11:00 AM - 12:00 PM ET

Search Discussions

Term / Keyword / Phrase



1 to 50 of 152 threads (549 total posts)

Most Recently Updated

50 per page

Thread Subject	Replies	Last Post
Default python libraries...	1	19 minutes ago by BEN WILLIAMS Original post by Nathan Getty
Gadget or Python to send Email	0	11 hours ago by Sean Ebeling
Auto Close Tasks Based on Field Values	2	13 hours ago by Nick Mumaw
Generic Email Parsing Script-missing code	1	3 days ago by Nathan Getty Original post by Justin Shoemaker
Close Incidents with scripts	2	3 days ago by Nathan Getty

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

