Validate the Efficacy of Your Security Controls
Can You Validate Your Security Controls In a WFH Environment?
Agenda

01
Validating Security Controls with SafeBreach

02
Top 5 Remote Workforce Risks
- Email
- Endpoint
- VPN
- Segmentation
- Data Leakage

03
Demo
How to easily validate relevant security controls
How do you provide value and efficacy of your security practice?
Breach and Attack Simulation - For Security Control Validation

Many Enterprises today …

- Implement security tools / technologies based on Frameworks (HIPAA, PCI, ISO 2700x, NIST, etc. = Controls-based)
- Don’t validate that the controls are working
- Don’t prioritize initiatives based on greatest risk to the organization
- Are not able to demonstrate return on investment AND reduction in risk
Breach and Attack Simulation - For Security Control Validation

What if there was a way to …

Get more from your existing security
Minimize security exposure
Ensure you are meeting compliance requirements
Test your Incident Response Plan
Prioritize initiatives based on actual Risk
Rationalize your cyber investments and demonstrate performance
Online Poll

Do You Validate Security Controls?

1. No
2. Yes, with annual Pen-Test
3. Yes, with RED TEAM exercises
4. Yes, with automated Breach Attack Simulation
97% of breaches are at companies which have already deployed the right controls.

99% of attacks are known and have been for years.

95% of firewall breaches are due to misconfiguration.
Stop a Breach Before it happens

Validate your controls without the risk

Simulate TTPs to test your defenses

Visualize exposures with data-driven results

Holistically remediate to defend your enterprise

Proving the value and efficacy of your security practice
Simulate attacks

**Safely and continuously** run thousands of known threat indicators and attack behaviors to validate and improve your security controls.

- Content: 12,000+ Methods
- Tactics, Techniques and Procedures
- Malware Types
- Custom Build Attacks
- Threat Groups
Visualize Your Posture

- MITRE ATT&CK Heat Map
- Risk Score
- Explorer View of Kill Chain
- Executive Reporting
Remediate Holistically

- Actionable prioritized remediation by business impact
- Aggregate and share remediation data to Network, Endpoint and SIEM solutions
- Ability to drill down to individual results for security control validation
Top 5 Security Validations for a Remote Workforce
Fox Kitten – Widespread Iranian Espionage-Offensive Campaign

Posted on February 16, 2020

During the last quarter of 2019, ClearSky research team has uncovered a widespread Iranian offensive campaign which we call “Fox Kitten Campaign”. This campaign is being conducted in the last three years against dozens of companies and organizations in Israel and around the world.

Read the full Report: Fox Kitten – Widespread Iranian Espionage-Offensive Campaign

Though the campaign, the attackers succeeded in gaining access and persistent foothold in the networks of numerous companies and organizations from the IT, Telecommunication, Oil and Gas, Aviation, Government, and Security sectors around the world.

A botnet is brute-forcing over 1.5 million RDP servers all over the world

Furthermore, statistics show that despite BlueKeep, most RDP attacks today are brute-force attempts.

A Chinese APT is now going after Pulse Secure and Fortinet VPN servers

Security researchers spot Chinese state-sponsored hackers going after high-end enterprise VPN servers.

APT Groups Exploiting Flaws in Unpatched VPNs, Officials Warn

MARCH 12, 2020 • INSIKT GROUP®

Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide
Alert (AA20-099A)
COVID-19 Exploited by Malicious Cyber Actors

Original release date: April 08, 2020

Summary
This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom’s National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IoCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails. This alert provides an overview of COVID-19-related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IoCs provided within the accompanying .csv and .stix files of this alert are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this alert does not seek to catalogue all COVID-19-related malicious cyber activity. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

Technical Details
Phishing Email

Dear Families,

The Coronavirus (Covid-19) is wreaking havoc around the world. But if you know the "Virus-Proof Your Life" you can prevent this invasive pathogen from getting past your natural defenses, developed using the latest, cutting edge research from major coalitions and institutions across the globe.

Please go through this video and check what it’s trying to tell you!

Thanks
Dr. Christopher Kawa, DC

P.S. I’ve been in practice for almost 24 years and every day I’m researching the latest scientific evidence on health so that I can teach my patients to function better and avoid disease. This special, one-of-a-kind e-book contains the latest, essential factors that lead to a strong immune system; one that can fight off bacteria and viruses with the God-given tools that we all have inside of us. I want to share this wisdom with you so that you and your family can all live happy, healthy lives.
How can you ensure your extended remote workforce is secure?

- **Email**
  - Malicious Attachments
  - Malicious Links
  - Social Engineering

- **Endpoint**
  - Phishing Attacks
  - Drive by Downloads
  - Browser Exploits

- **VPNs**
  - Exploit VPN Vulnerabilities
  - Brute Force Attacks
  - Phishing VPN Credentials

- **Networks**
  - Brute Force Attacks
  - Malware Propagation
  - Remote Exploitation

- **Data Leakage**
  - Data Exfiltration
  - Improper Permissions
  - Unencrypted Communication
DEMO
### Relevant Attacker Techniques to watch

- **Infiltration techniques** - Monitor email and network for email, drive by and other download of malicious content
- **Host infection techniques** - file and fileless malware, malware execution
- **Host actions** - Monitor filesystem, registry and process dynamics for suspicious activities

### Relevant Attacker Techniques to watch

- **Brute Force** - Monitor network activity for authentication attempts over common protocols internally available
- **Malware propagation** - Monitor network activity for the propagation of known malware
- **Remote Exploitation** - Monitor internal network activity for vulnerability exploitation and exploit delivery

### Relevant Attacker Techniques to watch

- **Exploitation** - Monitor network activity for vulnerability exploitation attempts

### Relevant Attacker Techniques to watch

- **Data Exfiltration** - Monitor network activity for sensitive content over a variety of protocols and channels
- **C&C Communication** - Monitor outbound communication for known C2 domains and C2 communication behavior
Validate your Security Controls!

Top 5 Security Validations for a Remote Workforce

Contact ASMGi for more information:
sales@asmgi.com

Special Offer for Attendees
Q & A
Thank you!