



ISSA

Information Systems Security Association
International

www.issa.org

ISSA International Webinar

Security Professionals Dilemma

November 27, 2018

Today's web conference is generously sponsored by:

Infoblox
CONTROL YOUR NETWORK



Infoblox

<https://www.infoblox.com/>



Moderator

Mark Kadrich, Principal, Kadrich InfoSec Consulting Services

For the past 30+ years, Mark Kadrich has worked in the security community, building knowledge, and contributing solutions. His strengths are in architecture level design and review, solution design and efficacy, policy generation, endpoint security, and risk management. Mr. Kadrich is the author of the book Endpoint Security published by Addison Wesley. Mr Kadrich holds degrees in Management Information Systems, Computer Engineering and Electrical Engineering. He was a contributing author in publications such as Healthcare Technology Online, Health IT Outcomes, TCP Unleashed, ISSA Journal, Publish Magazine, Planet IT, RSA, CSI, SANS and The Black Hat Briefings. Mark Kadrich is a well- known speaker and evangelist on network security matters at technical conferences and security events. He was the program manager and chair for Cornerstones of Trust for 3 years.

Mr. Kadrich has been a CISO, CSO, CEO, Chief Scientist, Corporate Minion, and Security Slave. He is presently a Free Range CISO helping customers create and manage security IT environments.



Speaker

Geoff Horne, Distinguished Engineer and Senior Manager of SMEs, Infoblox Inc

Geoff is an Architect, Systems Analyst, and Threat Intelligence Consultant. He has been involved in the design and integration of next generation computing and communications systems for more than two decades and is currently a Distinguished Engineer and Senior Manager of SMEs for Infoblox Inc. There he is responsible for design, development, and securing of systems for large scale network intelligence infrastructures for fortune 500 companies.

Geoff draws on a diverse background that began with a Masters degree in physics, a post graduate career in research computing at the University of Sydney, digital film production including visual effects for such films as 'The Matrix', and the Technology Director for News Corporation's News Interactive where he managed the design and development of five of Australia's top ten websites.



Speaker

Karen Worstell, CEO, W Risk Group

Karen Worstell is the CEO of W Risk Group and founder of MOJO Maker for Women in Tech. Ms. Worstell has over 30 years of information security experience including tenure as the Chief Information Security Officer (CISO) at Microsoft Corporation, AT&T Wireless and Russell Investments. As leader of the W Risk Group Ms. Worstell provides customized guidance to help companies develop their information security programs demonstrate due diligence to a defensible standard of care (D4SC) and via the MOJO Maker program Ms. Worstell provides leadership development for mid-career women in tech. Her experience as a chaplain in regional medical centers and the VA led her to recognize the issues of moral distress and burnout in the workplace and she returned to the workplace to address this need. She is the author of "Governance and Internal Controls for Cutting Edge IT" published by ITG Publishing, contributing author to the 6th Edition of the Information Security Handbook by Wiley on "The Role of the CISO" and co-author of "Evaluating the Electronic Discovery Capabilities of Outside Law Firms" by Pike and Fisher. Her newest publication is "Your Amazing Itty Bitty® Personal Data Protection Book: 15 Keys to Minimize Your Exposure to Cybercrime Using These Essential Steps". She holds Bachelor of Science degrees in Chemistry and Molecular Biology from the University of Washington, and a Master of Science in Computer Science from Pacific Lutheran University. Her theology MA degree is from MJTI.



Speaker

Geoff Horne, Distinguished Engineer and Senior Manager of SMEs, Infoblox Inc

Geoff is an Architect, Systems Analyst, and Threat Intelligence Consultant. He has been involved in the design and integration of next generation computing and communications systems for more than two decades and is currently a Distinguished Engineer and Senior Manager of SMEs for Infoblox Inc. There he is responsible for design, development, and securing of systems for large scale network intelligence infrastructures for fortune 500 companies.

Geoff draws on a diverse background that began with a Masters degree in physics, a post graduate career in research computing at the University of Sydney, digital film production including visual effects for such films as 'The Matrix', and the Technology Director for News Corporation's News Interactive where he managed the design and development of five of Australia's top ten websites.

Cybercrime Growing in Complexity and Scale



- \$600 billion (~1% of global GDP) lost to cybercrime per year¹
- Breach victims often hire expensive forensic firms, law firms



- Each breach results in millions of records stolen
- Breach victim's future business jeopardized

Today's Security Landscape



Security in virtual environments

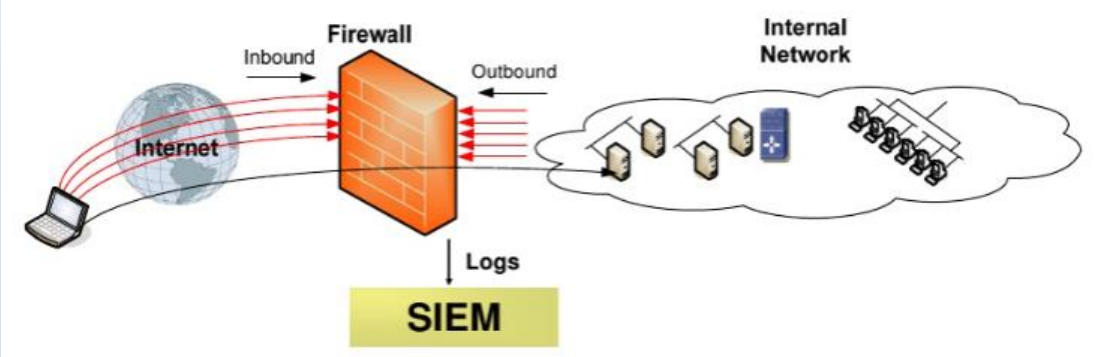
- DevOps security, is code review enough?
- Have you 'locked the doors' to your SaaS accounts?
- Do you have control plane, SDN security?
- Who has rights and access to provision more infrastructure?



Traditional Defense Mechanisms Insufficient



- DLP (Data Loss Prevention) solutions don't have visibility into virtual conversations and do not cover DNS
- Firewall doesn't always have control plane visibility.
- SIEM license could be costly if you put all the DNS query/response data into it.



Do you really need more tools?



Or do you just need better tools?

Do you already have right coverage in place today?

Is your Threat Intelligence house in order?

Security Teams Cannot Respond to Incidents Fast Enough

REQUIRES MULTIPLE STAKEHOLDERS, BETTER INFORMATION AND PROCESSES



- Breach response must follow GDPR's 72 hr. notification timeline
- Not all organizations have necessary tools and automation to correlate data from multiple systems
- Expensive security personnel / lack of skilled resources add to operational issues

Customer A

- Found that he had a lot of data to analyze and decided to outsource SOC operations because they couldn't analyze it themselves



Customer B

- Didn't know all the places in the network where they were using threat intel and failed to operationalize on it

Leading to...



Poor Security Posture

- Infected end not isolated
- Risk of lateral infection
- Data at risk



Inefficient Operations

- Manual incident search
- Manual threat intel research
- Slow isolation/disinfection



Lack of Agility

- Manual DNS, DHCP & IPAM operations
- Multiple teams handover

Ideal Solution: Security Automation at Scale



Increased SOC maturity

Automated processes, integrated tools within SOC



Combined DDI, threat intel and context

External & internal threat intelligence automatically shared with security ecosystem to accelerate & prioritize response



Better agility

Automated IT workflows for better agility and manageability across next generation data center environments



Single pane of glass visibility

Centralized visibility across on-prem, virtual and cloud deployments including VMWare, AWS, Azure, Cisco ACI, OpenStack

Using IPAM – The motherload of data



✓ Event Correlation

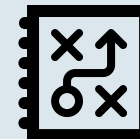
DHCP servers responsible for allocating IP addresses that can be used to track infected devices

DHCP correlates disparate events related to the same device under investigation especially in dynamic environments



✓ Incident Response/Scope of Breach

Discovery and Config Management enable operations teams to accurately identify compromised machines and gain visibility into what resources that client has been accessing



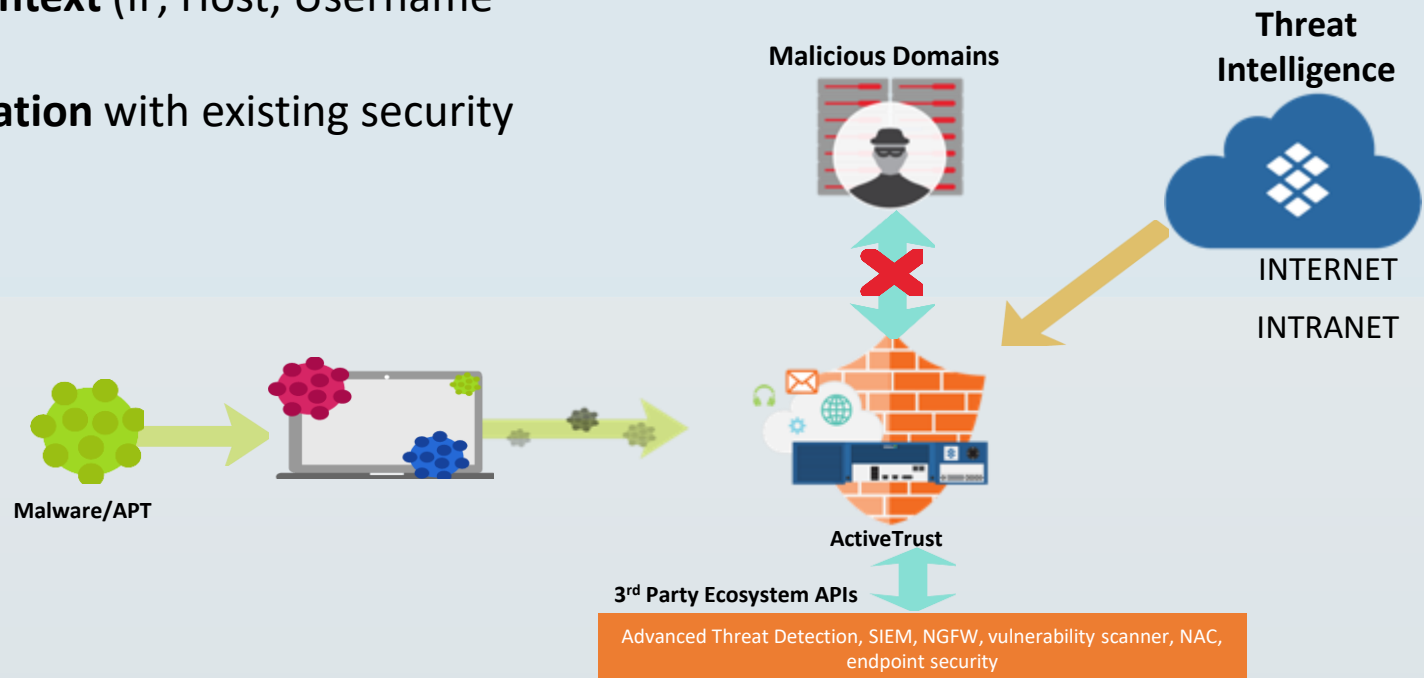
✓ Threat Actor Investigation

Public pDNS (passive DNS) and domain registration data help to fully understand scope of adversaries' malicious infrastructure and link events

DNS and Domain registration data are key data sets in making threat intelligence actionable

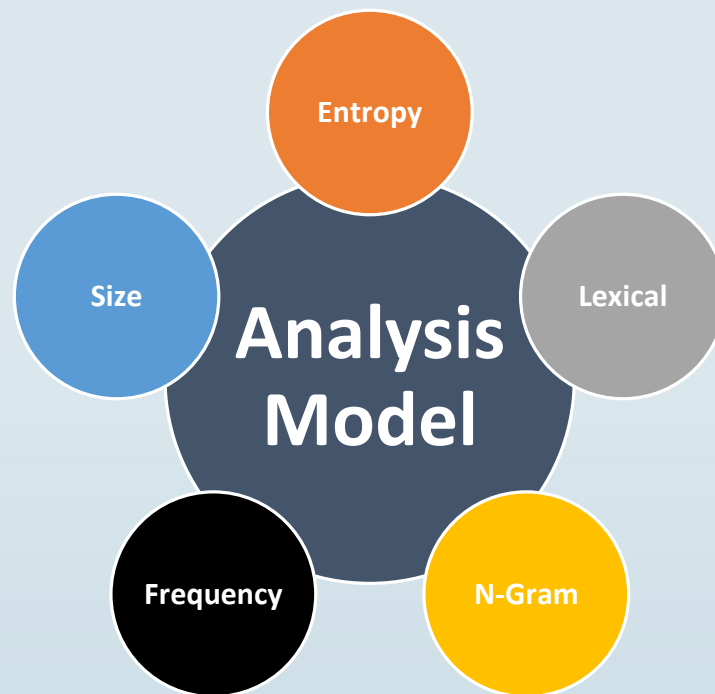
Make DNS Your First Line of Defense

- Scalable Threat Protection using **Response Policy Zones (RPZ)**
- Leverage existing infrastructure (DNS) and **operationalize** billions of **threat indicators**
- Access to **data context** (IP, Host, Username mapping)
- **Exchange information** with existing security infrastructure





Use Analytics to Detect and Block DNS-based Data Exfiltration





- **Detect** data exfiltration with DNS-based analytics
 - Includes those that don't have well known signatures (zero-day)
 - Looks at TXT records, A, AAAA records
- Feed threat intel data to **block** data exfiltration in near real time
 - Put domains associated with data exfiltration in RPZ feed to block infected devices from connecting to them

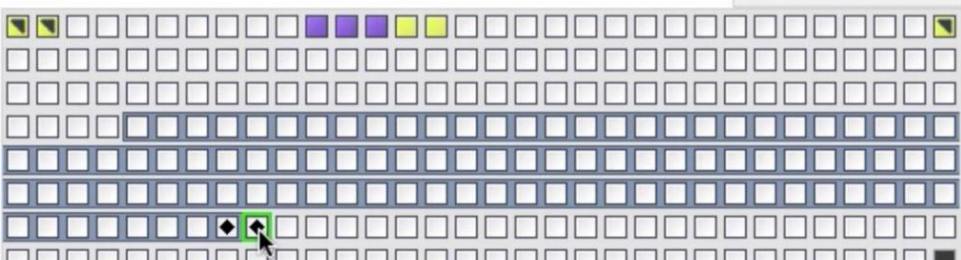


Get IPAM visibility

IPAM Home
10.60.136.0/24 IPv4 Network   [Go to DHCP View](#)

IP Map List


Go to    



Toggle Basic View

- Unused
- Conflict
- Used
- Pending
- Unmanaged
- Fixed Address / Reservation
- DNS Object
- Host Not In DNS/DHCP
- Device
- Active Lease
- Selected IP Address
- DHCP Range
- DHCP Exclusion Range
- Reserved Range

IP Address: 10.60.136.200
Status: Used
Usage: DNS,DHCP
Type: A Record,Lease,IPv4 DHCP Range
Lease state: Active
Range: 10.60.136.100-10.60.136.200
DHCP Fingerprint: Microsoft Windows 8 or 8.1 (Version 6.2)
Active Users: 1
Device Type(s): Windows

10.60.136.200 

Type:	A Record, Lease, IPv4 DHCP Range	MAC Address:	74:e6:e2:e0:c8:7b
Comment:		Name:	tmelab-pc001.test.com, tmelab-pc001
		DHCP Fingerprint:	Microsoft Windows 8 or 8.1 (Version 6.2)

Discovered Data

NetBIOS Name:	TMELAB-PC001	OS:	
Discovered MAC Address:	74:e6:e2:e0:c8:7b	Last Discovered:	2016-09-22 08:45:31 BST
Attached Device Name:	cisco-p4r3-34	Attached Device Vendor:	Cisco
Attached Device Port Description:	FastEthernet0/2	Attached Device Model:	catalyst3560v248ps

Get endpoint visibility



Search Dossier



Resources

Export JSON

microos.jumpingcrab.com

For additional information try searching [jumpingcrab.com](#)

Reported by Infoblox, and ThreatTrackSecurity

First Reported on 11/11/2014 by Infoblox

Last Reported on 4/1/2018 by ThreatTrackSecurity

DNS Count: 1
Domain/Subdomain Count: 1
IP Count: 14
Positive URL Detections: 3

CATEGORIZATIONS

Infoblox	APT_MalwareC2
ThreatTrackSecurity	MalwareDownload_Generic
Forcepoint ThreatSeeker	bot networks. advanced malware com...
Dr.Web	
Websense Threatseeker	

WHOIS



Created:	11/22/2005
Updated:	11/7/2017
Expires:	11/22/2018

Indicator Information

Export

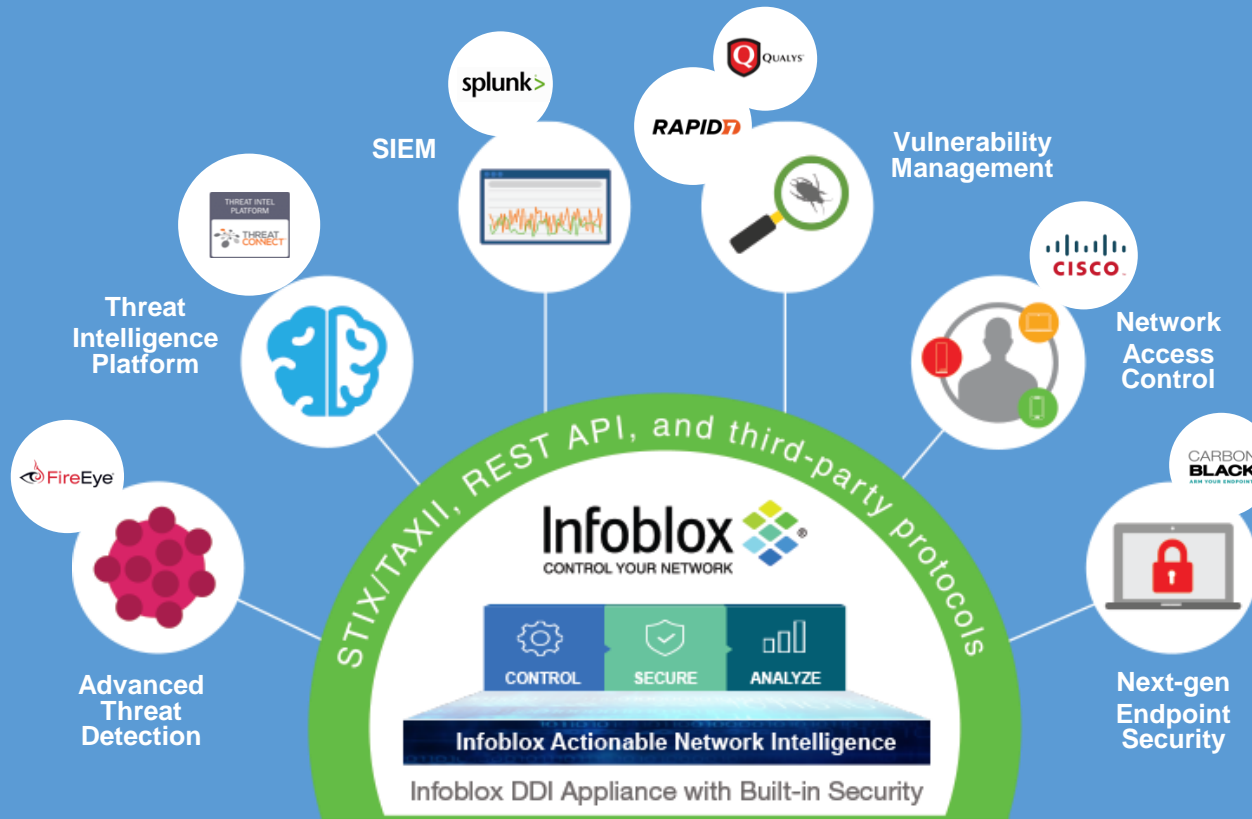
DATA PROVIDER	PROPERTY	FIRST REPORTED...	LAST REPORT...	EXPIRATION DATE	STATUS	FEED NAME
ThreatTrackSecurity	MalwareDownload...	3/29/2018	4/1/2018	5/31/2018	Active	
Infoblox	APT_MalwareC2	11/11/2014	11/11/2014	1/19/2038	Active	Base

Timeline

Export

DATE	EVENT	IP	SOURCE
11/22/2018	WHOIS Expires		WHOIS
4/1/2018	Last Detected as MalwareDownload...		ThreatTrackSecurity
3/29/2018	First Detected as MalwareDownload...		ThreatTrackSecurity

Security Orchestration and Automation





ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?



Speaker

Karen Worstell, CEO, W Risk Group

Karen Worstell is the CEO of W Risk Group and founder of MOJO Maker for Women in Tech. Ms. Worstell has over 30 years of information security experience including tenure as the Chief Information Security Officer (CISO) at Microsoft Corporation, AT&T Wireless and Russell Investments. As leader of the W Risk Group Ms. Worstell provides customized guidance to help companies develop their information security programs demonstrate due diligence to a defensible standard of care (D4SC) and via the MOJO Maker program Ms. Worstell provides leadership development for mid-career women in tech. Her experience as a chaplain in regional medical centers and the VA led her to recognize the issues of moral distress and burnout in the workplace and she returned to the workplace to address this need. She is the author of "Governance and Internal Controls for Cutting Edge IT" published by ITG Publishing, contributing author to the 6th Edition of the Information Security Handbook by Wiley on "The Role of the CISO" and co-author of "Evaluating the Electronic Discovery Capabilities of Outside Law Firms" by Pike and Fisher. Her newest publication is "Your Amazing Itty Bitty® Personal Data Protection Book: 15 Keys to Minimize Your Exposure to Cybercrime Using These Essential Steps". She holds Bachelor of Science degrees in Chemistry and Molecular Biology from the University of Washington, and a Master of Science in Computer Science from Pacific Lutheran University. Her theology MA degree is from MJTI.

What I know about you

➤ You thrive on:

- Personal Growth
- Variety & Change
- Contribution
- Curiosity
- Integrity

➤ For the long haul, you likely need more of:

- Love & Connection
- Resilience skills
- Greens and Water
- Exercise
- Burnout awareness**

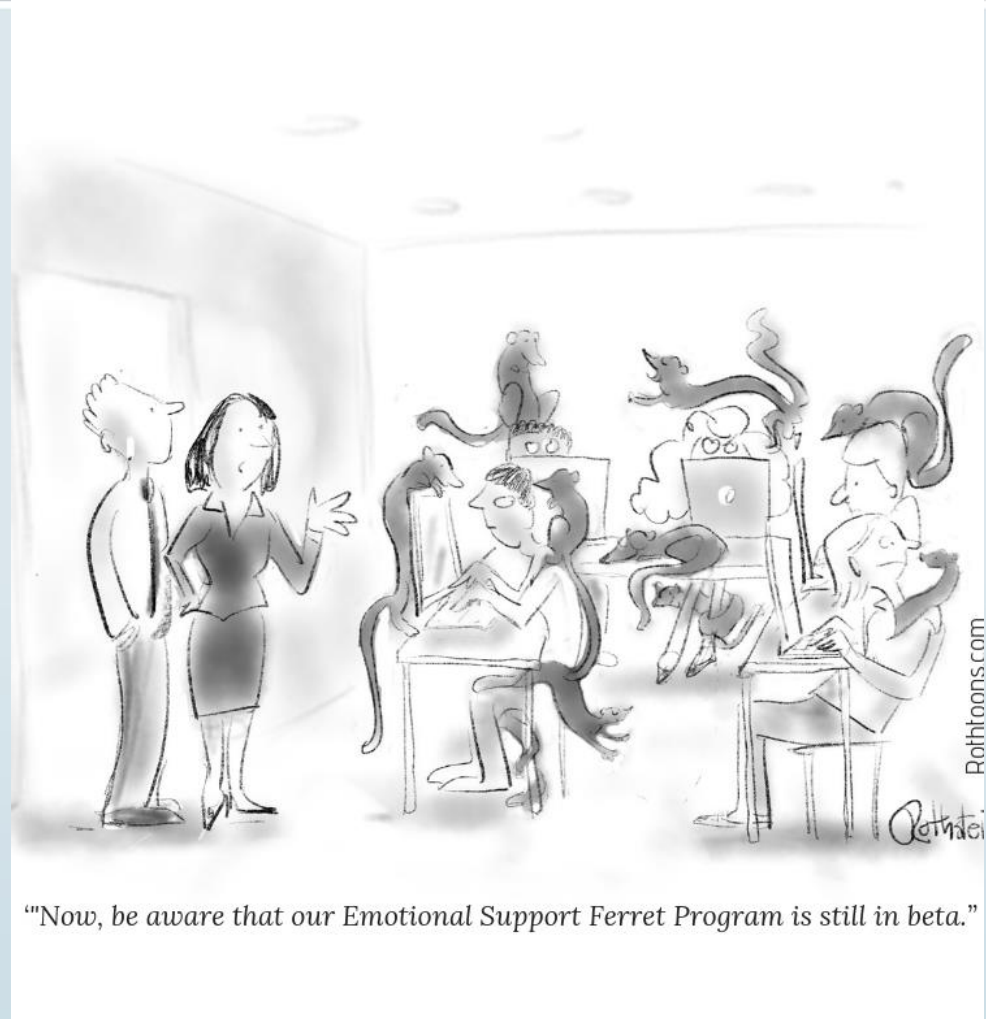
Burnout: tech's dirty little secret

In a global study, 80% of people reporting burnout cited work-related issues as contributing and 39% reported that work was the *only* reason.

57.16 % of 11,500 tech employees responded YES to the BLIND survey question: "Are you currently suffering from burnout?"

Different burnout scales:

- Depersonalization/Detachment
- Emotional Exhaustion
- Professional efficacy



If Cybercrime were a nation state
It would be the 13th largest GDP in the world

The Perfect Storm

Hypervigilance

Chronic lack of resources
necessary to meet
the threat

High responsibility
+ Low authority



The high cost to organizations



Attention to detail and follow-through decrease

Creative thinking, collaboration and innovation decrease

The willingness of your best people to speak up decreases

Presenteeism cuts productivity by 30%

Absenteeism costs \$2650 per year per salaried employee

Morale tanks

Turnover skyrockets



‘We’ve got beer on tap and a company hot tub. With perks like that, we don’t have to worry about a cyber talent shortage, do we?’

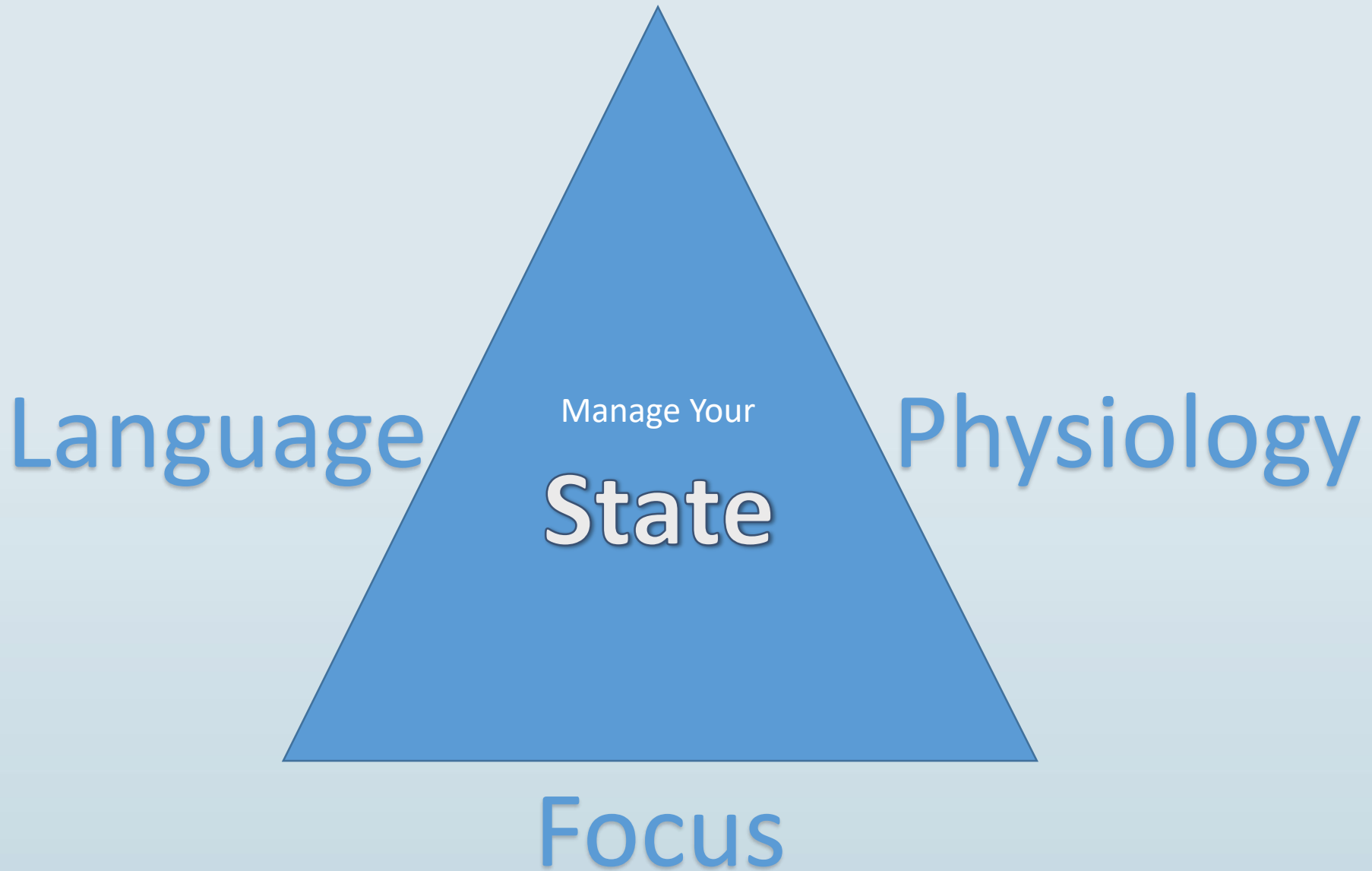
Adversity and pain in life are a given.

Suffering is optional.

Be aware

- You may be on the verge of burnout if you notice any or all of these symptoms:
 - Chronic fatigue: feeling physically and emotionally depleted, and waking up dreading the day.
 - [Insomnia](#): as exhausted as you are, you still can't [sleep](#).
 - Forgetfulness or impaired [concentration](#) and attention.
 - Physical symptoms that can include chest pain, heart palpitations, shortness of breath, gastrointestinal pain, dizziness, fainting, and/or headaches (be sure to seek medical help for any of these if chronic).
 - Getting sick more often. With your immune system becomes weakened, you're more vulnerable to infections, colds, flu, and more.
 - Loss of [appetite](#) and weight loss
 - Anxiety and/or [Depression](#).
 - [Anger](#). You're irritable and your fuse is only getting shorter.

What you can do now – for you



More info & resources



- March 4th, 2019 Talent Seminar at RSA Conference
- karenworstell.com/rsac/
- karenworstell.com/mojo-maker
- If there is a specific question or topic you want us to cover on cybersecurity culture and burnout, please email me: karen@wriskgroupllc.com.



ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?