# Next-generation techniques replacing legacy software tools

Larry Whiteside Jr.,

Founder, Whiteside Security

Co-Founder, ICMCP

"Your Partner for Success"
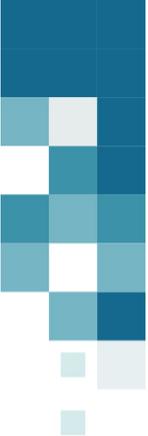
# Why do I care?

- Whiteside Security is focused on helping Security Executives be successful
- ICMCP (International Consortium Minority Cybersecurity Professionals) – helping to create diversity in cybersecurity by increasing women and minority representation in the career field
- Larry Whiteside Jr.
  - Over 20 years of experience as Security Executive
  - Advises a number of Executives in corporate and cybersecurity tech space
  - Recovering CSO/CISO in multiple verticals

# What's going on right now?

- Publicity following mega-breaches continues to push the cybersecurity spending button
- Despite the increase in spend now or the forecast of more spending, attacks and breaches remain as prevalent as ever.
- IoT is driving security decisions
  - No longer just user based devices
- Threats are increasing and # of available people are not

Source: Hackmageddon.com

# What are the changes in cybersecurity technology?

- Legacy solutions have lost effectiveness in detecting increasingly complex attacks.
  - Attack surface increase
    - IoT, Social Media, Phishing/Whaling, Hactivism, Geopolitical, DoS/DDoS, Socially engineered malware, MtM, Xsite, Session Hijacking, IAM, patching (or lack there of), etc, etc...
- Network architectures are also changing, as software-defined networking (SDN) and cloud computing create more complexity in security needs.
  - What worked yesterday doesn't work with today's innovations
- Organizations are now turning to complex security PLATFORMS
- Ability to DETECT and RESPOND are becoming paramount
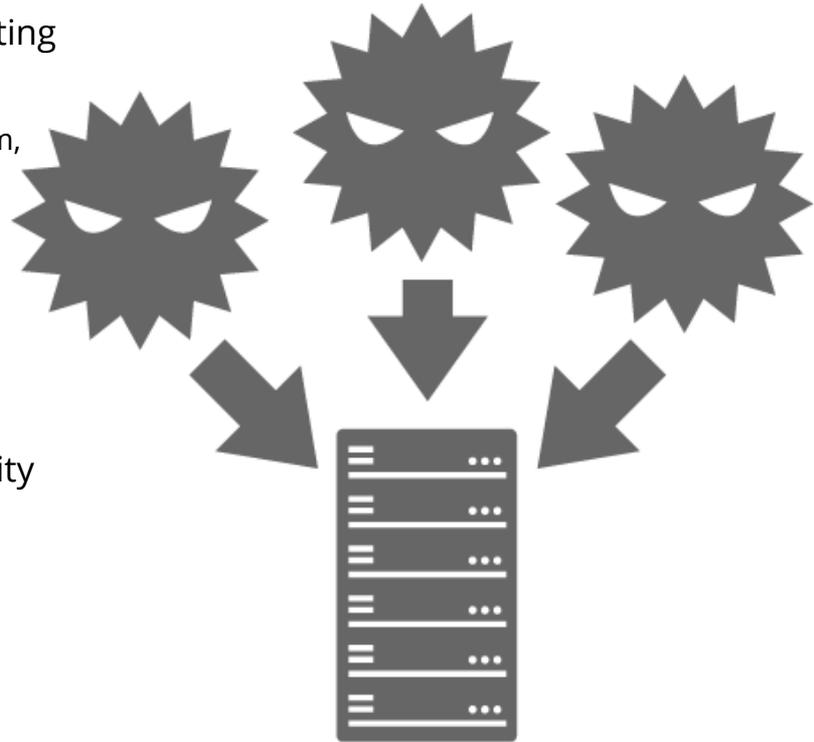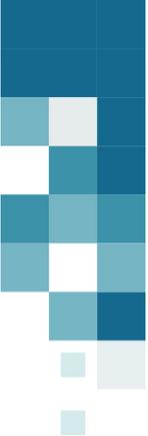
# What are the changes in cybersecurity technology?

- Virtualization and Cloud are forcing a re-evaluation of capabilities to protect corporate assets
- More integrated, automated, and complimentary tools are being sought and purchased
  - "Best of breed" versus "ease of management" was struggle
  - NOW – best of breed versus ease of management {coupled with meantime – to – detection}
- Detection and Response are outpacing Protection
  - Its not just about putting a better wall around things or isolating things MORE
  - Gartner says By 2020, 65% of worldwide managed security service providers (MSSPs) will offer managed detection and response (MDR)-type services. Driving security automation and orchestration
- Shortage of Security Expertise
  - Driving more MSS investment
  - Driving security automation and orchestration
- Compliance / Policy Enforcement
  - Not just with regulations
- IoT is creating new security points of infection
  - It used to be about how many devices each person had and how they connected
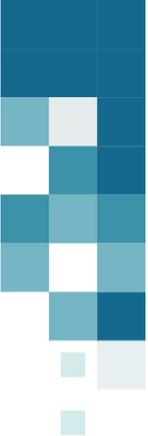
# Why are the changes necessary?

- Attacks are not going to stop!
  - Detect rather than protect
  - If you can't respond, nothing matters
- Policy means nothing if its not measured
  - Adherence to processes, compliance etc…
- Though more people are entering the field, the technical depth needed is not moving fast enough
  - Masters Degree level professionals
  - Non-technical business leaders
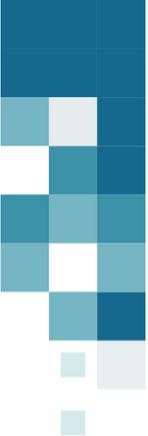
# Questions and Contact

Larry Whiteside Jr.

[Larry.Whiteside@whitesidesecurity.com](mailto:Larry.Whiteside@whitesidesecurity.com)

[www.whitesidesecurity.com](http://www.whitesidesecurity.com)

[www.icmcp.org](http://www.icmcp.org)

Twitter:

@LarryWhiteside

@WhitSec

@ICMCP_org

www.linkedin.com/LarryWhiteside

# Too Many Security Vendors, Not Enough Qualified Personnel



Percentage of respondents who say there is a shortage of cybersecurity professionals in their country
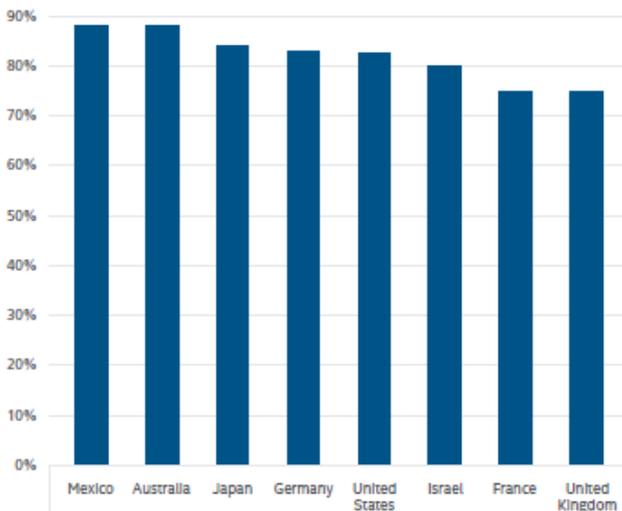
Figure 1. Cybersecurity workforce shortages by country and skillset.



Percentage of respondents whose company outsources cybersecurity services
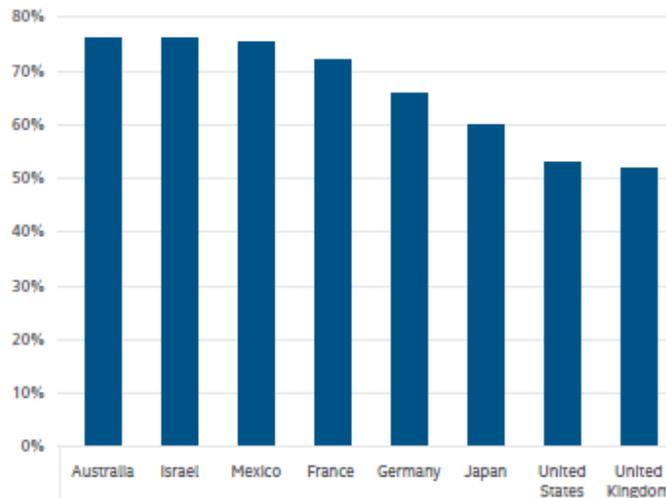
Figure 13. Outsourcing cybersecurity functions.

Source: "Hacking the Skills Shortage", Intel Security

# Abundance of Players in MSSP Game

Figure 1. Magic Quadrant for Managed Security Services, Worldwide