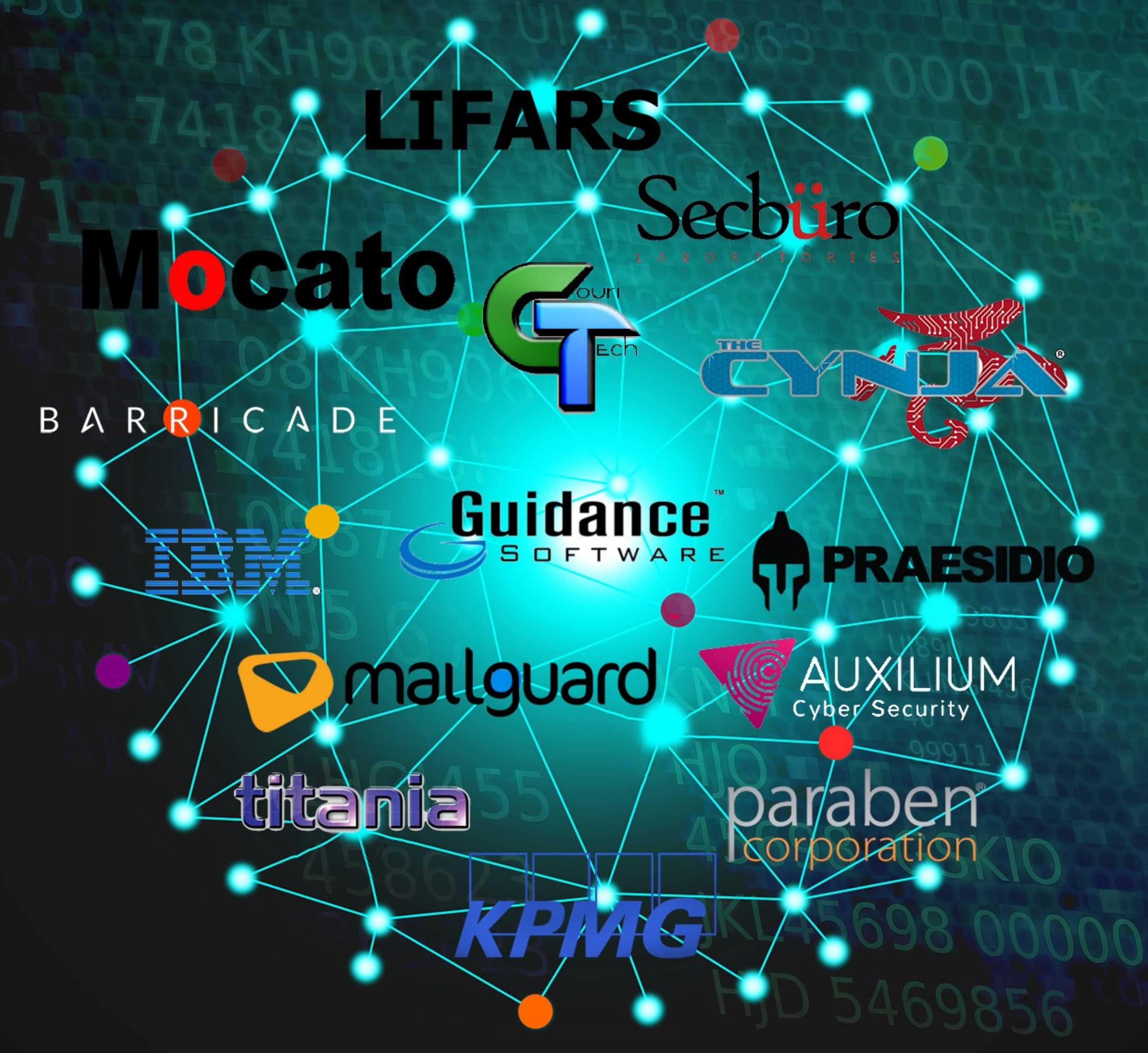
Hakin9
PRACTICAL PROTECTION
IT SECURITY MAGAZINE

eForensics Magazine

PREDICTIONS FOR CYBER SECURITY IN 2016



and more...

WHO IS WHO

[redacted]

[redacted]

[redacted]

Przemek Radzikowski
Secbüro Labs
Chief Security Researcher

Przemek (Shem) is the Chief Security Researcher at Secbüro Labs. For over two decades he has worked on key assignments with government, military, telecommunications, banking, finance and large multinational clients across the Americas, Middle East, Africa, Europe and Asia Pacific, where he headed the technical delivery and governance of highly complex Cloud, Data Center and Security projects worth in excess of $65 million.

CYBERSECURITY 2015 TOP EVENTS

What were the most important things that happened this year?

[redacted]

Przemek (Shem) Radzikowski, Secbüro: Labs: Ashley Madison Hack • Black Hat USA • First 400+ Gbps NTP reflection DDoS attack • APT28 • TalkTalk hack by 15yo.

[redacted]

RECRUITMENT

What will change in the talent pool?

[redacted]

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: Given the immediate requirement for cyber security professionals, many people will try to reskill and transfer from their existing professions to fill the gap.

[redacted]

RECRUITMENT

Will talent shortage in the industry continue to grow?

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: For the foreseeable future, the talent shortage will continue to grow for another two to three years (the average length of an undergraduate degree). Unfortunately, the ripple effect from the shortage may persist for a longer period while professionals gain industry experience.

[redacted]

RECRUITMENT

What new challenges will recruiters have to face in 2016?

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: Recruiters will find it tough to sift through a torrent of opportunistic but relatively unskilled candidates who want to jump aboard the rise in pay commanded by quality security experts.

[redacted]

[redacted]

RECRUITMENT

What new challenges will people looking for work in cyber security have to face?

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: There is no substitute for experience. Be prepared to work hard and learn fast because the security ecosystem is changing far more quickly than other sectors.

[redacted]

TRAINING

What role will formal education play in 2016?

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: It is difficult to see formal education disappearing completely, but in general, it has been slow to incorporate cybersecurity trends within their curricula. It’s not uncommon for university curricula to remain static for many years because of their reliance on published textbooks.

[redacted]

TRAINING

Will certification keep its role as the main tool to confirm skill and expertise?

[redacted]

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: I've met many highly-certified people who have turned out to know very little. All too frequently, certifications only test knowledge but not the candidate's ability to apply the concepts in real world situations.

[redacted]

TRAINING

Will we see a more unified standardization of education and skills?

[redacted]

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: The security ecosystem is becoming highly specialized and new niche areas are emerging each year. If anything, we will see further fragmentation of education.

[redacted]

TRAINING

Will online courses influence the level of education in security field?

Przemek (Shem) Radzikowski, Secbüro Labs: Although I have a number of formal credentials, I think online courses provide a tremendous service to the industry by making security education easily and cheaply obtainable to anyone who wants it. That's a positive. The negative aspect of online courses lies with their clumsy way of proving that the student has passed the material – it still hinges on an honours system.

THREATS

What threats that emerged in 2015 will remain relevant in the next year?

[redacted]

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: We saw some interesting reflection and amplification DDoS attacks this year, in particular those using Simple Service Discovery Protocol (SSDP). The SSDP attack vector was possible as a result of millions of unsecured home-based Internet-connected devices which use Universal Plug and Play (UPnP). These were used as SSDP reflectors. Their sheer scale of numbers and passive availability will likely continue through 2016.

[redacted]

THREATS

Which threat group will see the biggest growth in 2016?

[redacted]

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: I think it's worth keeping in mind that 300+ Gbps DDoS attacks will become the norm and may start to see sustained 500+ Gbps attacks. We should also be prepared to see a rise in DDoS attacks which act as a smokescreen for the "real" or "secondary" attack and ultimate exfiltration of data.

THREATS

Can you see any old and forgotten threat coming back in the next year?

Przemek (Shem) Radzikowski, Secbüro Labs: Brute force attacks have virtually disappeared, but with the proliferation of cloud applications, "Low and Slow" Brute Force attacks have been gaining popularity. The dispersed nature and scale of cloud resources makes possible their use to launch distributed "low and slow" brute force attacks without triggering alert thresholds.

[redacted]

[redacted]

TOOLS OF THE TRADE

What new technology will make an impact on cyber security the most?

[redacted]

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: Attackers and criminal organizations have been cooperating together for many years, and in many respects are a decade ahead of the rest in terms of their effectiveness. However, the adoption of cloud technologies has had a positive effect on our threat intelligence. By funnelling large data segments through relatively few cloud platforms, we have been able to collect valuable intelligence on the techniques, attack vectors and origin of attacks. Correlating these across regional and organizational boundaries gives us even more intelligence. This plus a push from industry players to share such intel freely, will only improve our ability to deploy proactive countermeasures.

[redacted]

THE INDUSTRY

In which industry will we observe the biggest demand for cyber security services?

[redacted]

Przemek (Shem) Radzikowski, Secbüro Labs: Akami's statistics for 2015 show that Media & Entertainment (48%), High Technology (11%), Retail (9%) and Public Sector (5%) collectively accounted for 65% of attacks. I'd put my money on this trend and say that these four segments will drive demand.

[redacted]

CONTRIBUTING COMPANIES

AUXILIUM
Cyber Security

BARRICADE

BLUSTOR™

BROADTECHSEC

Gouri Tech

CUJO

Mocato

MYDIGITALSHIELD

din's eye
Knowledge without sacrifice

paraben®
corporation

PRAESIDIO

RE-SEC®
Redefining Security

Secbüro
LABORATORIES

cybereason
malops protection

THE CYNJA®

cytegic

EH Academy

Guidance
SOFTWARE

GUIDEPOST SOLUTIONS LLC

IBM®