Recent Trends in Incident Response and Digital Forensics – Investigations Matter

Jennifer Lynn

Director, Cybersecurity and Investigations

jennifer.lynn@kroll.com

I am a passionate practitioner…

- 19 years experience Digital Forensics and Incident Response
- Case studies and examples of the difference in approach in the US in comparison to the GCC
- Make you reflect on your own organization
- Investigations are valuable and necessary
- Need to shift the mindset in the region

Set the Stage…

Independent energy trading and shipping company

Small by the number of employees

The incident(s) that finally forced the call for help

The consulting engagement…

Typical third-party or consulting engagement gets X number of hours when asked to respond

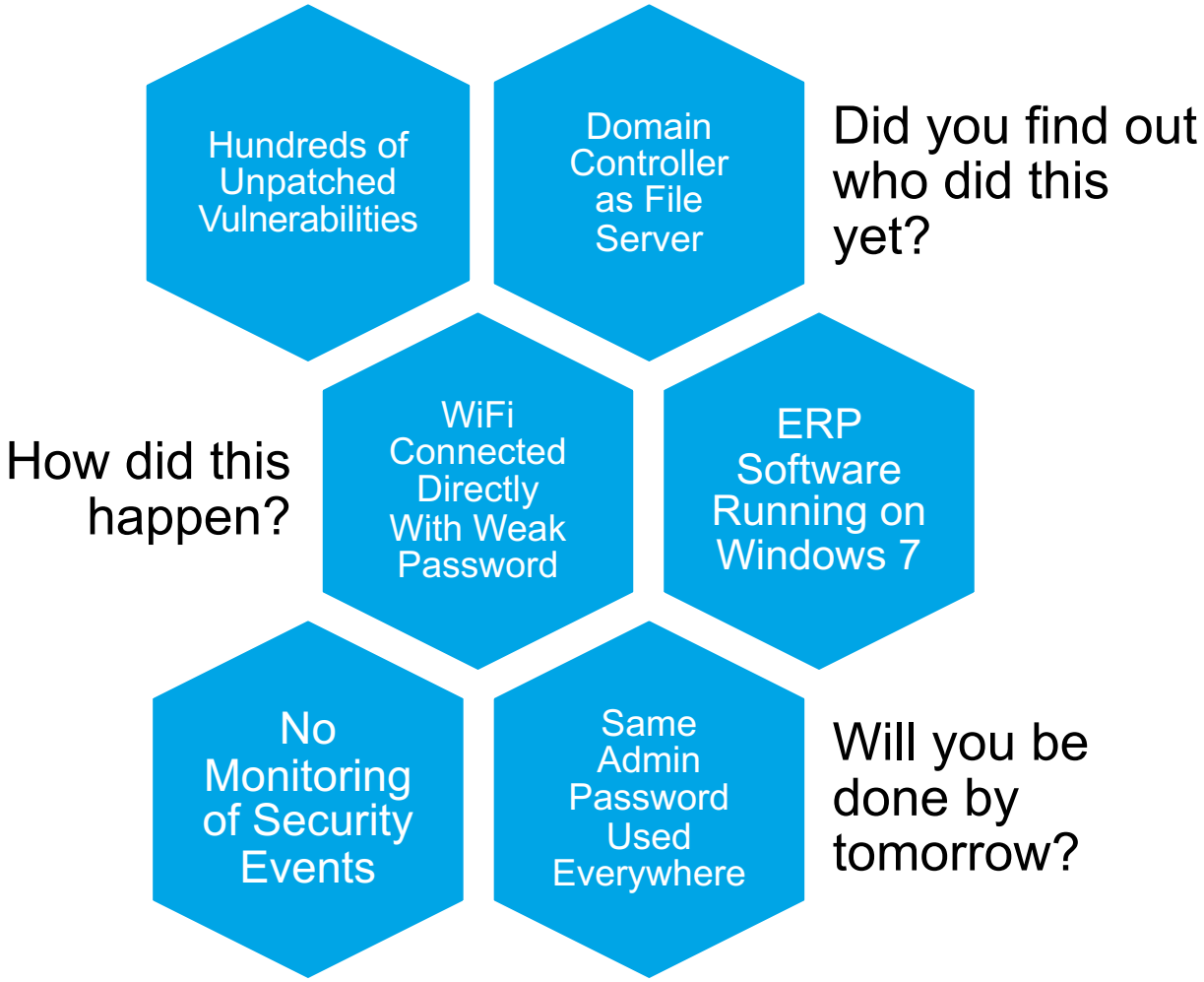
Day 1 Fire Fighting

Data collection of available logs, network traffic, memory captures, hard drive images

Overall Information Gathering Through Interviews and Technical Assessments

End of Day Meeting

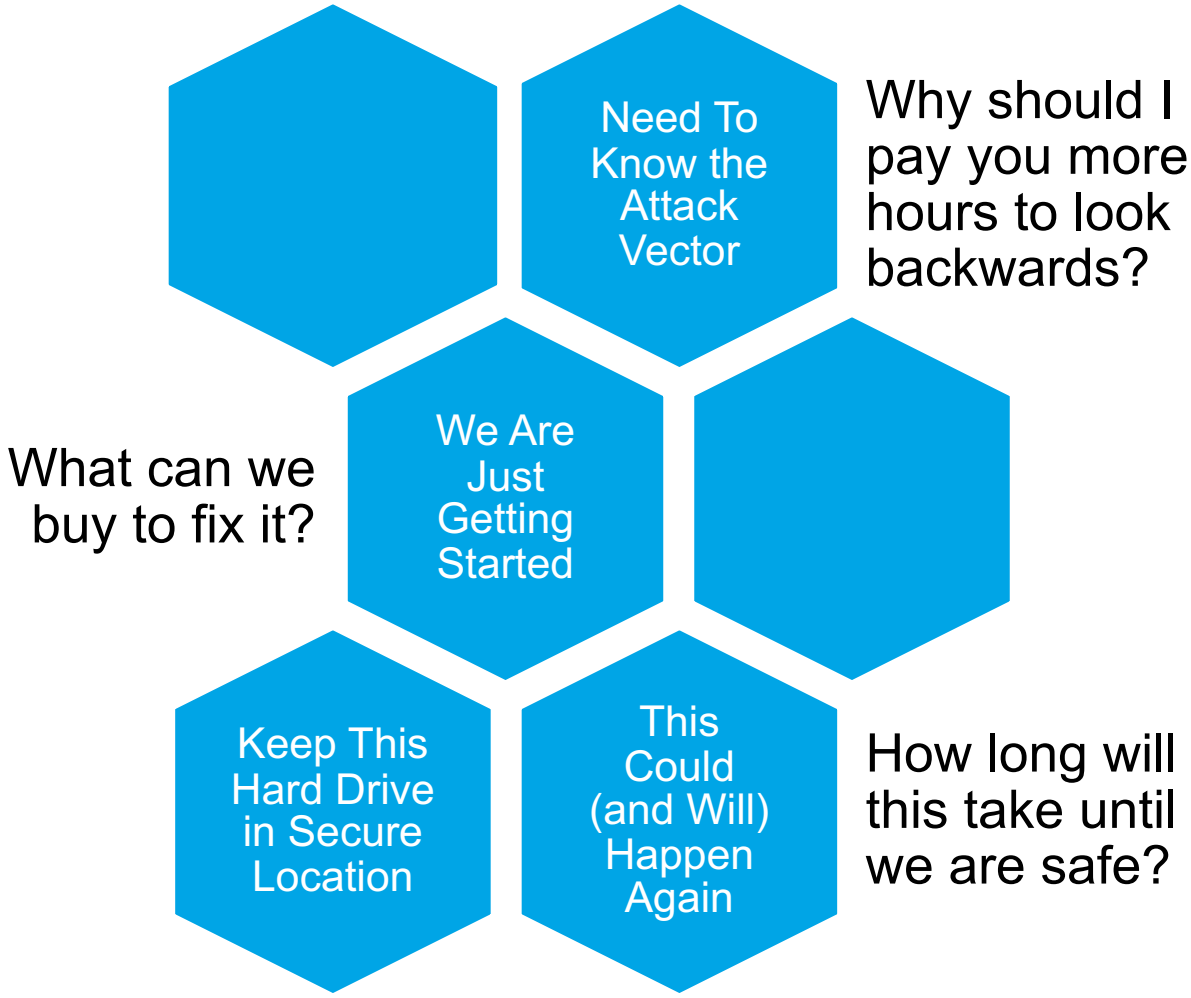
Stakeholders Meeting…End of Day Status



Day 1 Over…

What do you think happened next?

Investigation Stops…Remediation Mode



The consulting engagement completed…

90 Page Report of Vulnerabilities and Recommendations

New Security Road Map

We Declined Implementation and Returned for Health Check

About 9 Months Later…

It Happened Again…

Had Become Personal Friends with CEO and Staff

Forensics Found Web Browser History of Known Fake Malicious Office 365 Site

IT Manager was Victim of O365 Phishing Attack

Would he been left in the same position of trust if the investigation was completed the first time?

What is this was a technically sophisticated attack originally by a state actor who valued the company's intellectual property more than the cash out?

Culture of remediation…post consulting

UAE Company with 15,000 Users working in the CSOC

Minor incidents identified a file and we would be notified and remediation at the end point

The story of a trusted hardware vendor

Key reflections…

- Have we had an incident that was not fully investigated?
- Do we fully know what happened?
- How will we change out mindset and culture for the future?
- Did we report it to someone like DESC because we all love the UAE and want to help build a strong cyber defense community?

Thank You - Please Investigate!