

Building a secure healthcare network:

A hospital's immune system in action

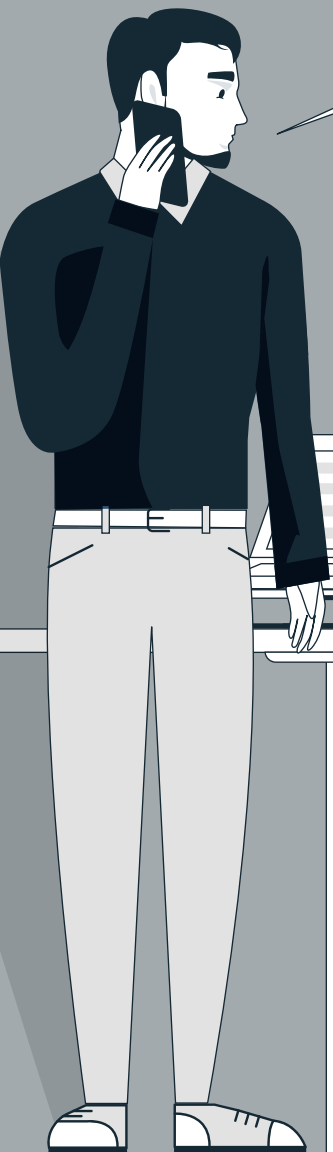


Chapter 1

It was a typical day at Sun Valley Health.



Meghan, the CISO, was looking over the morning IT infrastructure risk assessment reports, when a call came in from Alex, a member of her security team.



Meghan, remember when you asked me to keep an eye on Dr. Froth's online account? He's the doctor at that new physician network we acquired last month.

Yes, of course, I remember. What did you see?

His risk score has been increasing over the past month. We've seen multiple logins on his account from different offices. Activity across Europe at odd hours of the day.

That's not good. Have you reviewed the endpoints that have logged into that account? Also, do we know the data that account has access to?

That's exactly what I'm working to find out.

Good. I need you to prioritize this investigation and determine what's happened. I'll have to update Jack about this in our quarterly meeting next week.



Two days later...



Meghan is at the meeting with Jack, the CEO, in his office.

How long has your team known about this?

We noticed a possible attack about a month ago; we've been monitoring the situation very closely. We need your support to do the investigation.

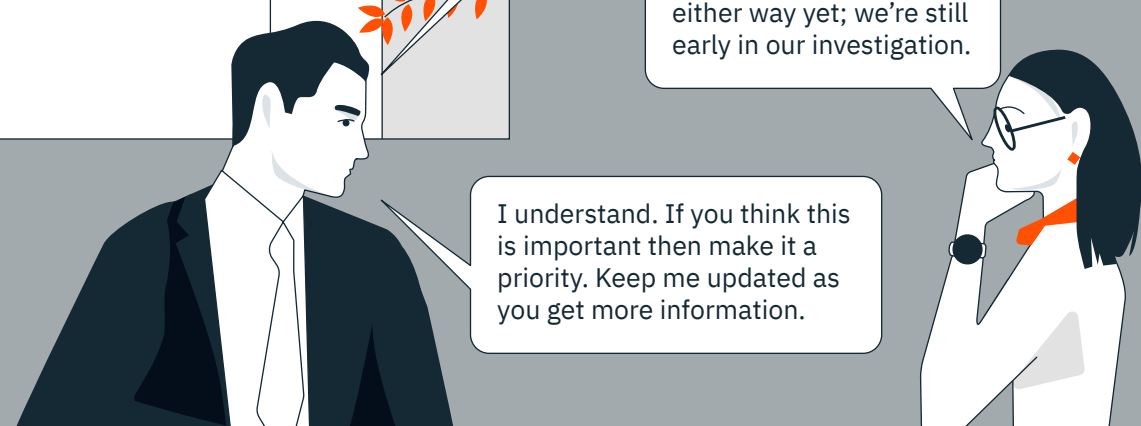
Of course. Do we have an idea of who or what the threat could be?

My bet is it's one of the organized criminal gangs in Eastern Europe. They've been responsible for numerous breaches in the industry.

Do we know if they've stolen patient data?

We can't say for certain either way yet; we're still early in our investigation.

I understand. If you think this is important then make it a priority. Keep me updated as you get more information.



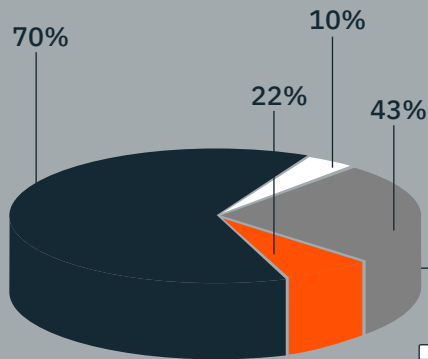
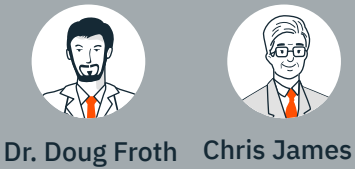
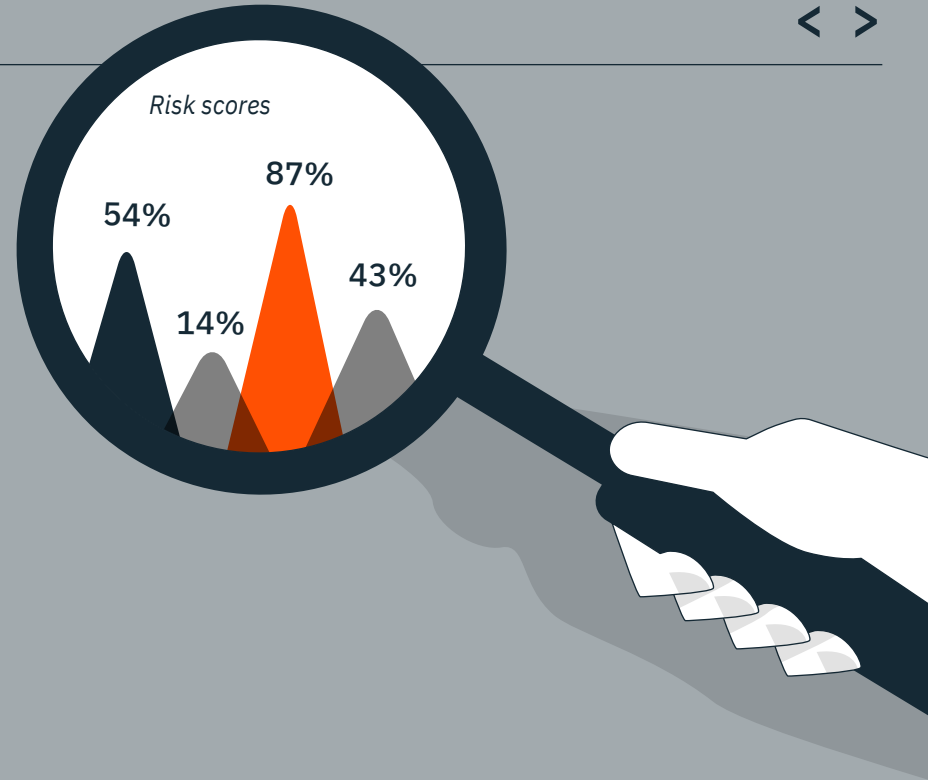
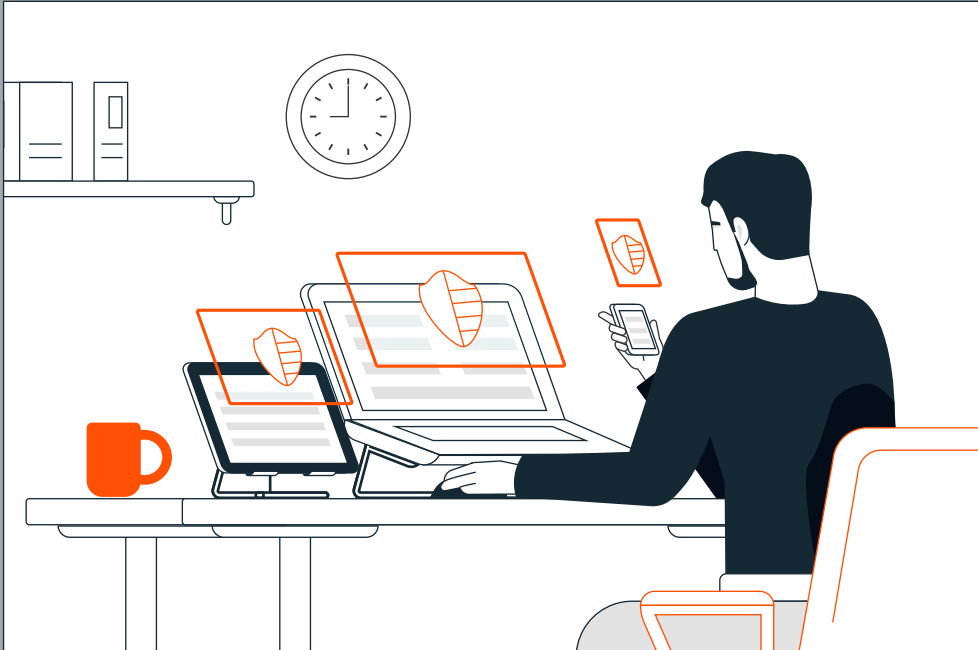
As Meghan leaves the office Jack thanks her for the work she's done so far.



Chapter 2



The pressure is mounting on Meghan's team to identify exactly what has happened and ensure that patient data hasn't been breached. The security operations center is feverishly investigating the abnormal spike in the risk score of privileged users Chris James, Dr. Froth and others.



One week later Alex tells Meghan they found something. Meghan is hopeful, yet cautious. Alex presents some key findings from his analysis to Meghan using IBM QRadar Advisor with Watson. He tracked the attack back to legacy software that was used by the physician network.

Meghan, we found something in our investigation. Here's our knowledge graph and a timeline of the kill chain so far.

The attacker got into the physician network using a Facebook message. They were in there for three months before we finalized the acquisition.

The M&A team must have been in such haste that they overlooked making sure the network was secure before connecting accounts.

Do we know who it is?

Exactly. The attacker escalated their privilege and was able to access our corporate network.

We compared IPs with information from IBMs X-Force team and tracked it back to a cell in the Balkans responsible for other attacks on US health systems.

Alex tells Meghan that the attacker was able to access a few other accounts within the physician network.

They were probably looking for a door into our patient data. Did they get access?

We investigated if these accounts accessed our sensitive data or if there was any other strange activity.

We don't have any reason to believe they stole patient data, but we're still looking. They got access to a few other user accounts, which we've already quarantined.

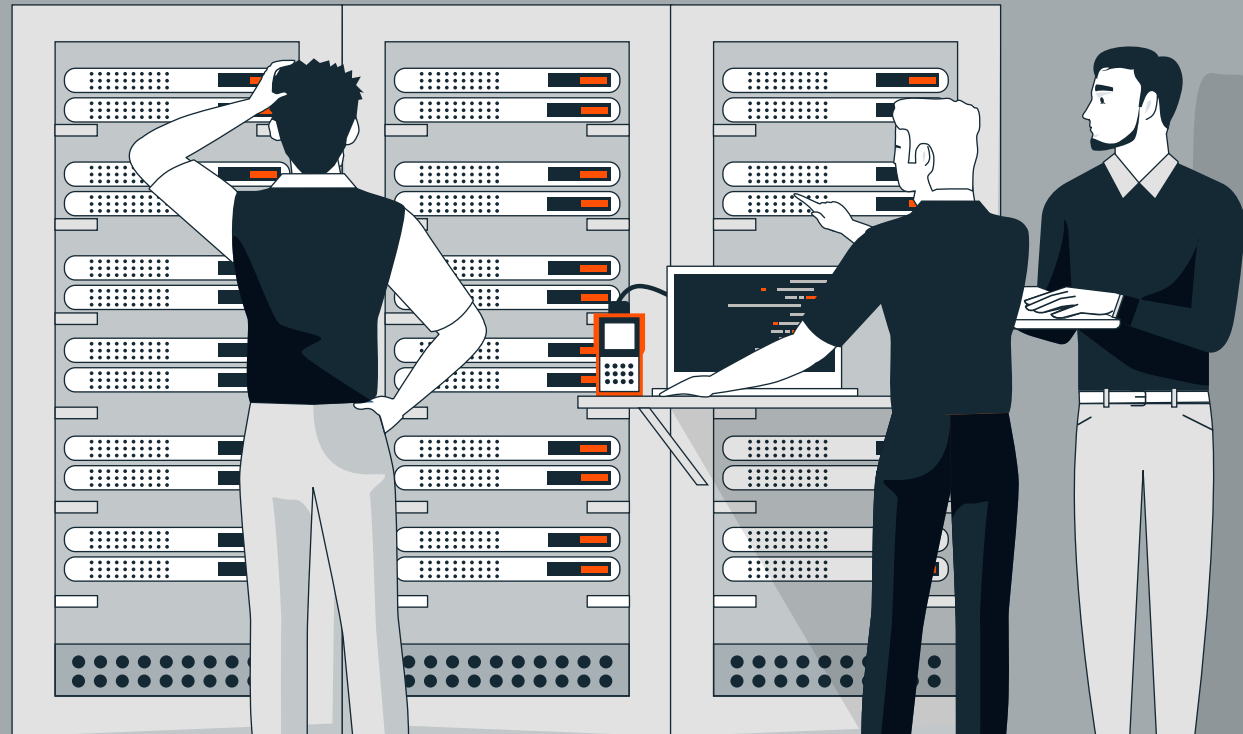
I'll give Jack a quick update. He'll want to know if we've been breached. Review all the infrastructure and accounts used, as well as places other than servers where there's patient data.

Of course. We're on it.

Login Succeeded	Login Date and Time	Logout Date and Time	Host Name	Remote Address	#
1	2018-01-22 01:55:11		vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1
1			vx39	9.55.150.194	1



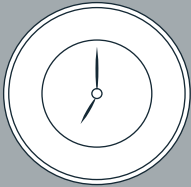
Five weeks go by...



Susan Fisher, Chief Legal Counsel, joins Meghan's meeting with Jack.

Susan, nice to see you again. Always wish we could see each other under different circumstances.

CONFERENCE ROOM B



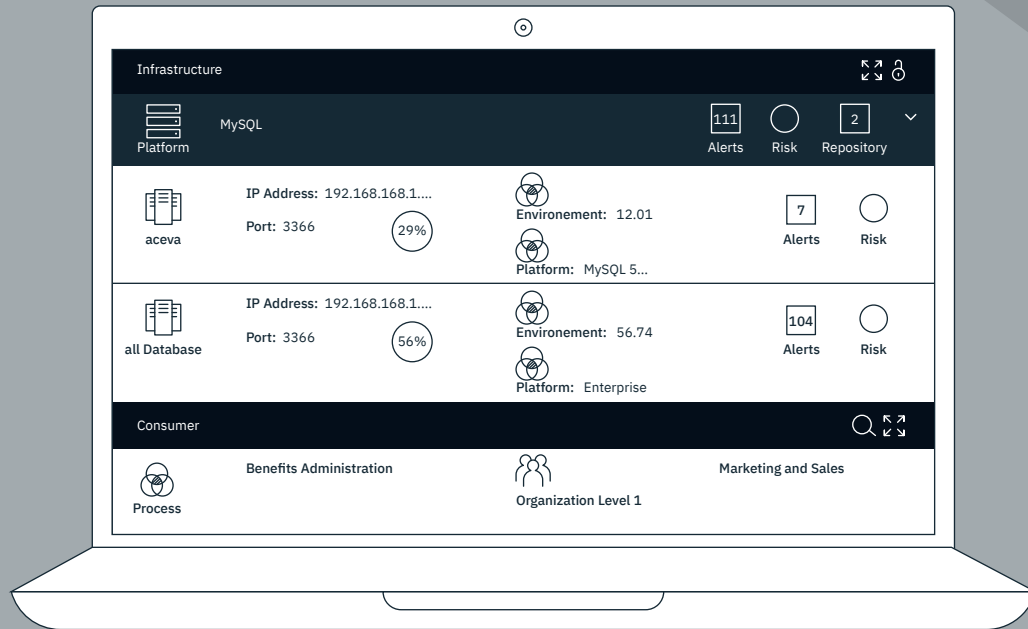
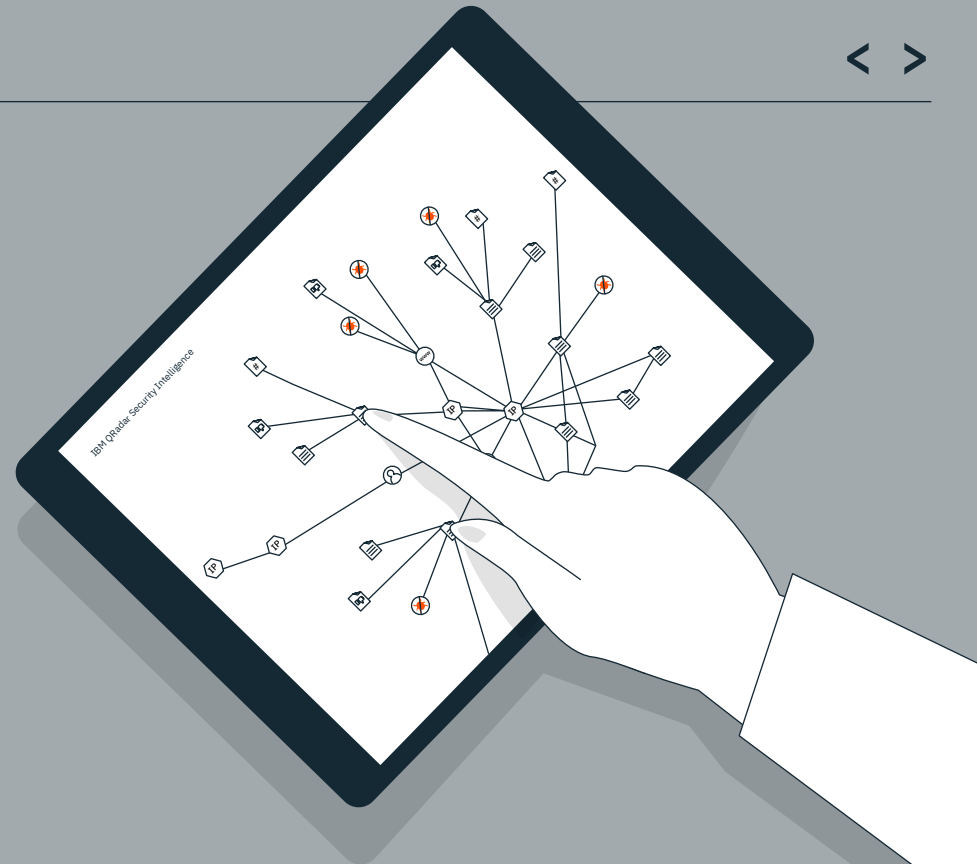
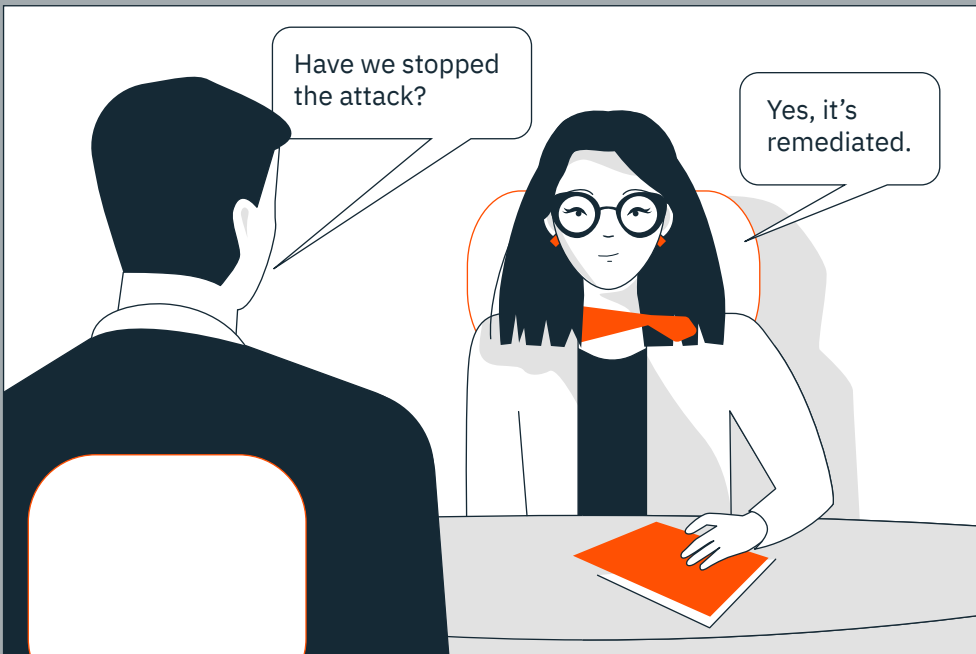
Meghan, you know how much I love these meetings. Feels like every day I read about more attacks in our industry. Let's get right to it. What did you find?

Because of the investments made and processes followed by our staff, we identified all our locations for patient data and confirmed there wasn't any breach. But they got close.

But how do we know for sure?

With good visibility into the end points, logs and infrastructure used we could see the whole attack.

The meeting with Jack.



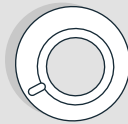
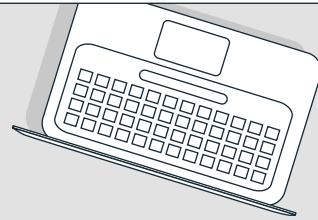
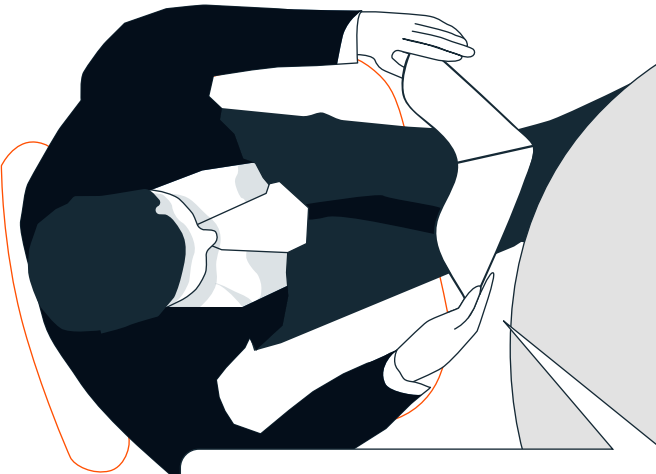
Meeting conclusion.

Thank you and please thank your team. This was good work. We had luck on our side too, given how close they got. Are we doing anything to improve how we protect ourselves and respond?



Thank you. We've already patched the legacy software. And we worked with Chris to update our M&A policies to ensure new acquisitions are up to our security standard before we connect with them.

Good. Let's also make sure our staff get smarter with their Facebook use. And Meghan, a win for us is another day where nothing happens. A lot of people don't appreciate that, but thank you.



IBM at work in healthcare:

Discover how Concord Hospital deployed a comprehensive security solution from IBM to secure endpoints and better detect and respond to threats across the organization.

www.ibm.com/industries/healthcare



© Copyright IBM Corporation 2018. IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.