quorum

☎ 0131 652 3954 marketing@qnrl.com qnrl.com

CASE STUDY:

Security - Legacy Protocols

CLIENT:

A Leading Banking Organisation

Despite the efforts large Enterprises put into protecting their infrastructure, one critical area is frequently overlooked is the phasing out of legacy protocols. Failure to remove legacy protocols could leave systems exposed and vulnerable to attack.

As a leader in the financial industry, security is top priority for our client. Quorum have been instrumental in a multi-year cyber security programme of work with the client.

One of these projects is responsible for improving and maintaining the security posture of the on-premises Active Directory Domain Services environment and the client sought to identify and remediate 'legacy protocols' from the environment.

Most legacy protocols were designed and built before modern enterprise security requirements were clear (or even existed!) - legacy protocol exposure can quickly lead to vulnerable access points.

The project scope was to highlight the use of legacy and encryption protocols within the client's environment which had been identified by an audit. These instances were then traced back to the originating application and a risk assigned to the appropriate owner where relevant protocols were identified.

Our previous work with the client provided us with a unique understanding of their environment, issues, options, and, most importantly, how to integrate with the current client team.

A senior stakeholder at the client gave this feedback: *"[We were] extremely impressed with the team...[we] worked against very tight milestones, shifting workloads around to ensure all deliverables were met."*

The benefits of using Quorum for this project included:

1. Strong relationship with the client & knowledge of their environment.

2. Microsoft security and identity experts.

3. Vast experience in highly regulated industries.

Scenario – and the team Quorum deployed to address it:

The project scope was to identify occurrences of 12 legacy authentication and encryption protocols within the client's environment and trace them back to the originating application to assign a risk to the appropriate owner whenever relevant protocols were identified.

Splunk and Stealthwatch Netflow were among the 'individual' technology-based solutions previously presented to the client, but these could not fully address the issue. The client chose Quorum because of our expertise. Our proposed solution took a tailored approach to each protocol and used the most appropriate tooling to capture and analyse the data.

The team comprised of:

Project Manager:

Oversaw the project and reported to stakeholders.

Technical lead:

Investigated and defined the capture process and was responsible for leading the engineering and determining the testing process.

Technical Engineer:

Responsible for the capture process, including scripts and configurations and performing testing and production implementation.

Data Analyst:

Produced a summary report for protocols, source devices and technology and/or business mapping reports.

It's vital that we work well with the internal teams of our clients to make these projects a success and in this situation, we got on fantastically well, becoming an extension of each other's teams, which was greatly appreciated by all. The client commented that, "*[We] had fantastic team ethic and camaraderie – working well together as a distinct unit and with the Project Team.*"

Solution – 12 diverse issues to be addressed in 1 project:

Each of the 12 Legacy Protocols, as specified by the client, was investigated, and then categorised into protocol types:

- Authentication
- Networking/Communication
- Encryption

This allowed the team to formalise a data collection strategy while grouping comparable protocols for faster processing.

Internal stakeholders and the Active Directory Services team discussed all infrastructure needs as well as data gathering tooling. A large volume of authentication and encryption traffic must be recorded and analysed to do this.

Quorum provided a cost-effective, customised data recovery solution using only standard Native Tooling, such as Event Log Forwarding, decreasing the resourcing footprint necessary when engaging teams other than the internal support team.

Thoughts and Outcomes:

This project was carried out in response to an audit point, which made it extremely crucial to our client. Rather than engage contractors to augment their internal team and run it as a BAU task, our client chose to onboard Quorum as a team to manage this delivery. We made this an easy choice for them based on our previous successful work within their Active Directory system.

Quorum has discovered all relevant occurrences of the 12-legacy authentication and encryption protocols within the client's environment, and the project is now complete. Here are key statistics from the project:

Runbooks

No of Runbooks produced:	10
No of document pages overall:	800

Data Analysis Reports

No of Data Reports produced:	7
No of document pages written:	179
No of Data spreadsheets produced:	10

Data Results

Legacy Protocols Investigated:	12
No of Protocols identified in use:	9
No of protocols identified as not-in-use:	2
No of protocols with capture issues:	1

Overall, around **1000** pages of information published.

The client can move on with an aggressive remediation plan to eliminate the protocols from the estate. Quorum's runbooks can be used on a regular basis to ensure that these protocols have been successfully removed.

Quorum continues to collaborate closely with the client and, through our current knowledge and close working relationship with them, is effectively positioned to quickly mobilise specialist resources as the business requires them to ensure they stay current, secure, and efficient.