THALES CYBER HEALTH CHECK

Case Studies
## Client Situation

Thales and Williams (F1?) formed a technical partnership in July 2016 to provide assistance to Williams in securing the high-tech data that it produces in both the Williams Martini Racing and Williams Advanced Engineering businesses. As part of an on-going digital transformation the relationship is helping to identify and secure immediate threats as well as ensuring that a cost-effective cyber-security programme is progressing.

## Task Description and Approach

At the outset of the partnership a cyber-healthcheck was conducted in order to ascertain the overall condition of Williams’ security posture, and identify the areas in which improvement would be beneficial, and those where investments were proving valuable. The two fundamental questions that the project needed to answer were “How mature are our cyber-security capabilities compared to industry best-practice?” and “How effective have changes to our infrastructure been?”

The chosen format of the healthcheck was a combination of cyber-security maturity review, a technical vulnerability assessment, and a cyber-physical assessment. Other modules of the healthcheck, such as Human Factors assessment, and a Phishing test were considered for inclusion in later work after the high-level picture of the organisation was understood.

## Project Result and Performance Assessment

The combination of the different modules created an incredibly useful set of data that provided insight into the current security posture of Williams. At the corporate level it was identified that a corporate wide policy and security programme would be required to allow all business functions to strive for alignment with Williams’ mission and objectives.

From a technical perspective it was possible to see the different maturity levels that were in place across the business functions – and for risk management that type of information is critical to understanding where best to place resources and effort.

- What was the result of the project / What was the value gained?
- Holistic view of security posture;
- Gap analysis outlining short falls in security controls;
- Better understanding of the organisation Cyber risk profile and threats facing the business;

## Man Days

<How long did this Take> Mike to update

## Staff

Mike Westmacott
Trent Holmes

---

<table>
<thead>
<tr>
<th>Name of Example</th>
<th>Williams F1 Cyber Health Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Williams F1 (F1)</td>
</tr>
<tr>
<td>Client Situation</td>
<td>Thales and Williams (F1?) formed a technical partnership in July 2016 to provide assistance to Williams in securing the high-tech data that it produces in both the Williams Martini Racing and Williams Advanced Engineering businesses. As part of an on-going digital transformation the relationship is helping to identify and secure immediate threats as well as ensuring that a cost-effective cyber-security programme is progressing.</td>
</tr>
<tr>
<td>Task Description and Approach</td>
<td>At the outset of the partnership a cyber-healthcheck was conducted in order to ascertain the overall condition of Williams’ security posture, and identify the areas in which improvement would be beneficial, and those where investments were proving valuable. The two fundamental questions that the project needed to answer were “How mature are our cyber-security capabilities compared to industry best-practice?” and “How effective have changes to our infrastructure been?” The chosen format of the healthcheck was a combination of cyber-security maturity review, a technical vulnerability assessment, and a cyber-physical assessment. Other modules of the healthcheck, such as Human Factors assessment, and a Phishing test were considered for inclusion in later work after the high-level picture of the organisation was understood.</td>
</tr>
<tr>
<td>Project Result and Performance Assessment</td>
<td>The combination of the different modules created an incredibly useful set of data that provided insight into the current security posture of Williams. At the corporate level it was identified that a corporate wide policy and security programme would be required to allow all business functions to strive for alignment with Williams’ mission and objectives. From a technical perspective it was possible to see the different maturity levels that were in place across the business functions – and for risk management that type of information is critical to understanding where best to place resources and effort.</td>
</tr>
<tr>
<td>Man Days</td>
<td>&lt;How long did this Take&gt; Mike to update</td>
</tr>
</tbody>
</table>
| Staff | Mike Westmacott
Trent Holmes |