CASE STUDY

Harnessing Innovation for Active Directory Security

- Industry: Commercial Blasting
- Country: Australia (HQ) & +100 countries
- Revenue: AUD 5.9B (2019)

KPIs

- 3 domain
- 1 forest

Orica Stakeholders

- 2 Engineers
- 1 Security Manager
- IT Infrastructure Manager and CISO

Tenable.ad Dedicated Team

- 1 Technical Account Manager
- 1 Engineer

Integration Plan Insights

- Integration into managed security service

Founded in 1874 and headquartered in Australia, Orica is the world's largest provider of commercial explosives and blasting systems for mining, quarrying, construction, oil and gas sectors. Employing around 11,500 people, Orica has a global manufacturing footprint and supply chain that delivers product and services to customers in over 100 countries.

Challenges

While Active Directory is part-and-parcel of Orica's IT infrastructure, this core component was not front of mind as a potential security point of failure for the organisation's operations. Management of AD by the in-house IT team was focused on maintaining availability of services and minimising service disruption. Against these competing work priorities, security control gaps emerged. Also, while the in-house Security Operations Centre (SOC) operated 'defense in depth', there was limited visibility of what activity was occurring within AD itself.

Prioritizing Mindsets

Through an Tenable.ad POC, Orica was able to get real-life insights into the current AD security posture. It highlighted weaknesses that could potentially lead to compromise of accounts and the domains. The ability to see such vulnerabilities, enabled the security and infrastructure team to re-align their focus and reignited the importance of securing Active Directory across the wider IT team.

Tenable.ad also helped address gaps in AD subject matter expertise. Most IT teams rely on generalist system administrators to maintain their domains and therefore even when issues are known, additional information is required before it can be remediated. Tenable.ad provided the IT team and the SOC with information on the complexity of the issue, what to prioritise and importantly, what steps the team could take to fix the issue. This empowered the IT team to focus on fixing issues, rather than simply identifying them.

Addressing a Lack of Visibility

Following the POC, the IT team accepted the need for continuous monitoring and the ability to track changes in real-time on the most critical parts of the directory. The initial discovery was followed with the instant-on deployment of the agentless, non-intrusive Tenable.ad for AD solution. Ingesting the Tenable.ad alerts into their Security Operations Centre enables Orica to continuously monitor for suspicious activity on AD, adding an additional layer of detection. Visibility was also missing for IT management. The POC, and then the production deployment, provides management with an overview of the AD security posture and the rate in which improvements are being made.

Solutions

The incoming CISO identified four needs that Tenable.ad could satisfy.

1. Insight to the security posture of AD – This allows identification of potentially dangerous configurations– as changes take place daily within an AD, continuous monitoring and resolving of misconfigurations and attack pathways became paramount.
2. Guidance to the in-house team on how to remediate – With a shortage of Active Directory security expertise internally, the power of Tenable.ad was used to empower the IT teams to make the security-specific changes within the domain.
3. Provide alerting on suspicious activities occurring on the domains – The SOC needs to know as soon as possible when suspicious activity is taking place. Tenable.ad's trail flow and indicators of exposure provide alerts with high levels of confidence, on activities that require further investigation by the SOC.
4. Provide continuous monitoring of the AD configuration – As well as the infrastructure and security teams, IT management gained visibility into a critical part of Orica's technology ecosystem. This has ensured an ongoing focus to ensure AD is maintained in a secure state.

“Tenable.ad is the answer to the two questions every CISO should be constantly asking – Are my domains adequately secured? and How can I independently prove it?”

Result

- Reduction in number of critical and high exposures with AD
- Trailflow alerts sent to SOC for actioning
- Monthly reporting on security state of AD as part of IT KPIs