Cntium in partnership with tenable

Unified Exposure Management Platform:

Case Studies

Case Study:

Implementation of Tenable One Exposure Management Platform

Cantium Business Solutions (Cantium), works in partnership with both Public and Private Sector organisations to enhance their cybersecurity posture. One such initiative, is the implementation of the Tenable One Exposure Management platform. This general case study highlights the collaborative approach we take, the results achieved and the numerous benefits realised by organisations partnering with Cantium.

Background

Cantium Business Solutions

As a Local Authority owned trading organisation (LATCo), Cantium has over 35 years' experience supplying IT services. As such, we have developed a comprehensive managed service portfolio, built alongside a strong partner network, to support and complement the services we deliver in-house.

Our highly experienced and dedicated teams, consisting of over 300 ICT specialists, provide advice, guidance and support to over 33,000 users. With a customer base of over 700 organisations across the Public, Private and Education sectors, Cantium offers a range of ICT services tailored to our customers' individual needs.

Tenable

A globally trusted exposure management company, approximately 40,000 organisations around the globe rely on Tenable to understand and reduce their cyber risk. As the creator of Nessus®, Tenable has developed and extended its vulnerability expertise, creating the world's first platform to view and secure any digital asset on any computing platform. Working in collaboration to instil cybersecurity awareness and reduce external threats, Cantium has developed a strong partnership with Tenable to deliver value and security resilience to our customers.

Demonstrating our founding principles:

- ✓ **Fast**
- ✓ **Connected**
- ✓ **Insight-Driven**
- ✓ **Customer-Led**

A Partnership Approach

Adopting a proactive approach, Cantium focuses on continuous improvement for our customers, regularly seeking opportunities to increase service quality. By partnering with Tenable, Cantium offers an end-to-end solution, with our IT experts on hand to guide organisations through their cybersecurity improvements.

Objectives

Cantium collaborates with our customers to achieve objectives, such as:

- ✓ **Implementing the Tenable One Exposure Management platform to identify and prioritise vulnerabilities.**
- ✓ **Integrating the Tenable platform with existing ITSM systems.**
- ✓ **Streamlining vulnerability management processes and improving overall security posture.**
- ✓ **Enhancing communication and collaboration between security and IT teams.**
- ✓ **Improving incident response and remediation times.**

Solution

To enhance an organisation's vulnerability management, Cantium proposes the implementation of the Tenable One Exposure Management platform, a leading solution known for its comprehensive vulnerability scanning, identification and prioritisation capabilities. To ensure seamless integration with existing processes, Cantium also recommends integrating the Tenable platform with the existing ITSM system.

The implementation process consists of the following steps:

1 Assessment and Planning

Conducting a thorough assessment of the existing infrastructure, identifying potential integration points with the ITSM system and formulating a detailed implementation plan.

2 Tenable Deployment

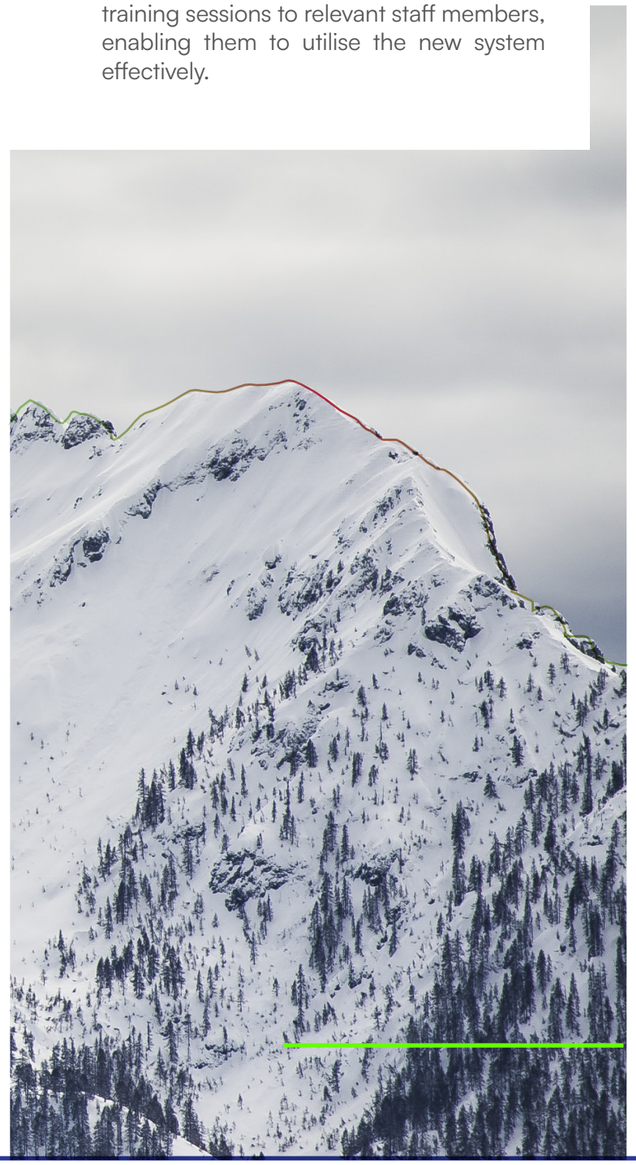
Deploying the Tenable One Exposure Management platform, configuring to meet the organisation's requirements and customising vulnerability scanning policies to align with the organisation's priorities.

3 Integration with the ITSM system

Developing and implementing a seamless integration between the Tenable platform and the ITSM system, allowing vulnerability data to flow automatically between the two systems.

4 Testing and Training

Conducting extensive testing to ensure full functionality of the integrated solution. Additionally, delivering comprehensive training sessions to relevant staff members, enabling them to utilise the new system effectively.



Benefits

Implementing the Tenable One Exposure Management platform and integrating it with the existing ITSM generates several benefits for organisations including:

Enhanced Vulnerability Management

- ✓ Improved visibility into an organisation's security posture through comprehensive vulnerability scanning and prioritisation.
- ✓ Streamlined vulnerability management processes, enabling efficient identification, tracking and remediation of vulnerabilities.
- ✓ Real-time monitoring and reporting on vulnerabilities, facilitating informed decision-making and resource allocation.

Improved Collaboration

- ✓ Seamless integration with the ITSM system improves collaboration between security and IT teams.
- ✓ Accelerated incident response and improved communication channels can be developed between different departments.
- ✓ Automated ticket creation in the ITSM system based on vulnerability scan results, ensuring prompt incident resolution.

Efficient Resource Utilisation

- ✓ Prioritised vulnerability data, integrated with the ITSM system can allow for better resource allocation and efficient mitigation of high-risk vulnerabilities.
- ✓ Reduced manual effort in vulnerability tracking and remediation can result in time and cost savings for organisations.

Compliance and Reporting

- ✓ Simplified compliance monitoring by leveraging the Tenable platform's reporting capabilities.
- ✓ Generation of comprehensive reports on vulnerability status, remediation progress and overall security posture for regulatory purposes.

Conclusion

With a focus on cybersecurity improvements at the centre of our collaborative projects, Cantium successfully implements solutions quickly and with minimal disruption.

Benefits to organisations who adopt our solutions include, enhanced vulnerability management, improved collaboration across the organisation and more efficient resource utilisation.

Case Study:

Implementation of Tenable Identity Exposure (formerly Tenable.ad) for a Local Authority

Tenable worked in partnership with a Local Authority (LA) organisation to implement an Identity Exposure solution to increase security for its Active Directory (AD) with a focus on identifying vulnerabilities, gaining visibility into AD architecture and monitoring security threats in real-time. This case study highlights the steps taken and the improvements made through adopting Tenable as the vulnerability management partner of choice.

Background

Tenable

A globally trusted exposure management company, approximately 40,000 organisations around the globe rely on Tenable to understand and reduce their cyber risk. As the creator of Nessus®, Tenable has developed and extended its vulnerability expertise, creating the world's first platform to view and secure any digital asset on any computing platform. Tenable's range of modular products allows organisations to tailor their security services to meet their specific needs.

The Customer

As a large Local Authority (LA) organisation, employing approximately 17,000 people and providing a full range of public services to its citizens, the customer recognised the paramount importance of data security.

As a public body, the LA understood how pivotal cybersecurity is to ensuring its personal data, including children and vulnerable adults, as well as sensitive commercial, third party and NHS data, remains safe.

In addition to compliance certification and data sharing agreements, the LA is subject to oversight by numerous regulatory bodies, including the Public Services Network (PSN), Office for Standards in Education, Children's Services and skills (Ofsted), the Department of Education (DfE), and the Information Commissioner's Office (ICO). It must also comply with GDPR, PCI DSS and the DSP toolkit for NHS data.

With the recent rise in cyberattacks, specifically targeting government websites and services, the LA was looking to increase security for its Active Directory (AD) to ensure domain control. Prior to Tenable's engagement, the LA was utilising a single forest AD structure with parent-child domains to control access to its internal servers and external facing services.

Objectives

Gaining Visibility into AD Security

The LA's enterprise architecture team consists of a security team (maintaining security policies and overseeing cybersecurity threat management) and an operations team (handling AD administration and vulnerability management). The security team were concerned by the rise in Government-targeted cyberattacks and were looking to secure their AD and address their critical priorities, including:

- ✓ **Identify existing vulnerability indicators early and take proactive**
- ✓ **Maintain security by gaining visibility into AD architecture.**
- ✓ **Receive real-time alerts when under attack.**

The team needed a single solution that would enable them to monitor AD security on an ongoing basis, indicating flaws as soon as they appear to enable remediation before any network impact occurs.

Solution

Real-time analytics and visibility to enable immediate response

The LA already had Tenable in place to help with its vulnerability management efforts. To secure AD, which is often the target of criminal attacks seeking valuable privileges and data, it added Tenable Identity Exposure (formerly known as Tenable.ad) to its security stack in 2021, shortly before the offices were closed for the end of August English Public Holiday.

The team implemented Tenable Identity Exposure on the LA's servers on the Wednesday, with all alerts enabled. On Friday morning, they discovered multiple Brute Force attacks [a trial and error method to systematically guess login credentials and encryption keys] on administrator accounts taking place, including one Golden Ticket attack [a method to target the access control privileges of a Windows AD environment, aiming to gain control of a domain], which was soon followed by many others. Over the next three days, Brute Force and Golden Ticket attacks continued to occur in a cycle.

According to the organisation's Enterprise Architect:

> **If we didn't have Tenable.ad [Identity Exposure], we would never have known. We would have come back from the long bank holiday weekend and been locked out of our network. We were very lucky to get Tenable.ad [Identity Exposure] in place.**

> **This is a solution you can't leave without, if we hadn't installed Tenable.ad, we would never have known about these attacks.**

Mitigating damage and identifying the source

With Tenable Identity Exposure alerting them to the attacks in real-time, the team was able to immediately disable the targeted accounts. The Enterprise Architect explains, "We were able to take charge of what was happening very quickly." The speed of response was critical to preventing further damage, including compromised access and data leaks.

Using the detailed information provided by the Identity Exposure alerts, the enterprise team was able to immediately specify which accounts needed to be disabled. However, with every attack which was shut down, another was initiated. The team realised this was not a singular attack and concluded that a user was on their network, exploiting these accounts. In addition to disabling accounts, the team also started physically removing devices from the network and reset the password of the Kerberos ticketing agent to prevent further Golden Ticket attacks. The attacks continued the next day and with the assistance of Identity Exposure, the team continue to resolve the threat.

> **Tenable.ad [Identity Exposure], told us very quickly who they were and we disabled those accounds very, very quickly.**

By leveraging Identity Exposure's real-time analytics and visibility, the team continued to disable IT network management accounts, pulling servers from the network and removing data centre servers from the cluster. By Sunday, they were able to verify that all infected servers had been taken offline.

Conclusion

Greater visibility, proactive response and a better security posture

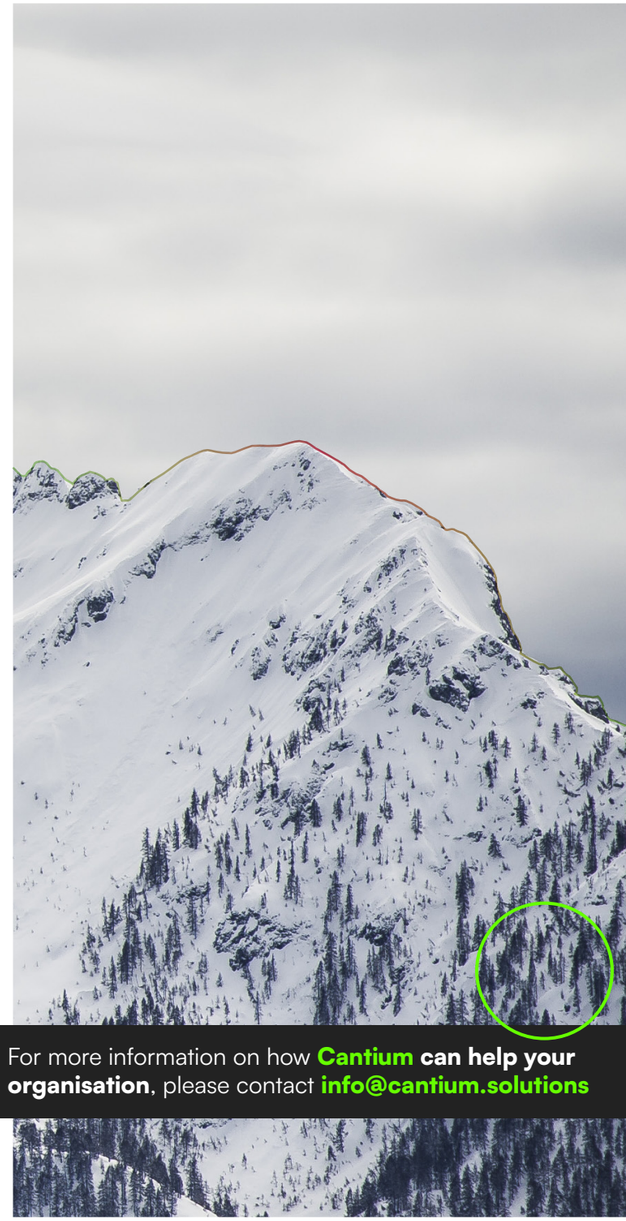
Tenable Identity Exposure was instrumental in negating cyclical Brute Force and Golden Ticket attacks over a period of 3 days. Without Identity Exposure installed, the attacks would have gone unnoticed which could have resulted in a costly security breach.

The Enterprise Architect stated,

> **The visibility we gained from Tenable.ad [Identity Exposure] not only allowed us to prevent a data leak and the damage that would have done to our reputation, it's brought security back to the forefront.**

Following on from their success with Identity Exposure, the LA introduced Tenable Vulnerability Management (formerly known as Tenable.io) as a management and reporting solution.

- ✓ **Real-time monitoring and attack alerts.**
- ✓ **Efficient installation and configuration.**
- ✓ **Targeted accounts disabled and attacks shut down swiftly.**
- ✓ **Able to trace attacks to a single server and taken offline.**
- ✓ **Prevented further damage and costly fines.**




Cantium
in partnership with
tenable