


AVERTIUM CASE STUDY:

THE UNIVERSITY OF TENNESSEE[®] MEDICAL CENTER

 Have questions? Give us a call.
877-707-7997

 www.avertium.com

 Arizona • Tennessee



Copyright © 2023 Avertium

CONTENT



ABOUT THE UNIVERSITY OF TENNESSEE MEDICAL CENTER (UTMC)	3
THE CHALLENGES UTMC FACED	3
HOW AVERTIUM HELPED	4
THE IMPACT	6

ABOUT THE UNIVERSITY OF TENNESSEE MEDICAL CENTER (UTMC) ▼

Located in Knoxville, Tennessee, The University of Tennessee Medical Center (UTMC), has a rich history in the East Tennessee community of providing patient-centered care while remaining at the forefront of research, technology, and treatments. The hospital serves as a referral center for Eastern Tennessee, Southeastern Kentucky, and Western North Carolina. It is the region's academic medical center, Magnet® recognized hospital, and Level I Trauma Center, reinforcing its commitment to delivering top-notch healthcare and protection for its patients. UTMC's expectations were that its cybersecurity should be just as top-notch. With a small team, it was looking for a partner to help it continue to grow its cyber resilience while minimizing risk.



John Jeffries, CISO at UTMC

THE CHALLENGES UTMC FACED ▼

When UTMC CISO John Jeffries thinks back to 2018, when the medical center first engaged Avertium, what stands out in his memory is the hospital's booming growth – and the expanding cybersecurity challenges that accompanied it. He remembers saying, "The hospital is growing and so is the risk. We cannot be idle about it."

Regulatory compliance, a critical concern in healthcare, demands stringent data protection measures. John saw a need to continue UTMC's evolution to a proactive security framework in which threats were preemptively countered rather than responded to in a reactive manner.

But doing it without a "journey partner" was challenging due to:

- limited internal **resources**,
- a need for more in-depth cybersecurity **expertise in-house**, and
- a incomplete **approach delivered** a disjointed network of outside partners who did not provide the comprehensive support UTMC's team would most benefit from.

UTMC is committed to its goal of patient care with a strong emphasis on patient protection, reflecting a "your business is our business" mindset. It is not just a healthcare institution; it's a dedicated partner in ensuring the well-being and health of the community it serves.

While UTMC embraced the advantages of Microsoft Sentinel with their previous vendor, such as the absence of hardware procurement and equipment lifecycle management, John noticed there were a few drawbacks to this choice. Managing logs and storage proved to be a challenging task. And while UTMC aimed to streamline security operations through the use of Microsoft Sentinel, John felt they weren't fully harnessing its capabilities.

At the end of the day, **John did not want to settle for the status quo**, but he knew he needed organizational buy-in to get anything done. So he got to work doing just that – educating key stakeholders, driving internal alignment, and building advocacy. Once he got his organization behind him, John looked for outside partners to help him tackle the challenges in front of him. **This is when UTMC's partnership with Avertium began.**

We went from aimless to empowered.

"You really can't put a price on the impact – the value of the working relationship has been phenomenal. And it's evolving every day.

– John Jeffries, CISO at UTMC

HOW AVERTIUM HELPED



The Avertium team sat down with John to build a relationship and discuss the current state of UTMC's security program. After some initial conversations, it was determined that compliance was the best place to start building momentum. Because when done right, the security controls required by compliance mandates can serve as the foundation for greater cyber maturity.

This is where Avertium's cyber fusion approach of "Assess, Design, Protect" first came into play.

Step 1: Assess →

Before UTMC could have clarity on the path forward, the team needed to know where they stood. That's why the collaboration kicked off with an in-depth assessment phase, where Avertium's team dove into UTMC's existing infrastructure, evaluating current capabilities, the strength of its compliance, and opportunities for enhanced efficiencies. This phase was crucial, as these assessments gave John insight into how best to prioritize UTMC's cybersecurity maturity initiatives. It was a small step, sure, but it helped him build momentum.

Avertium started with a HIPAA baseline assessment and gap analysis. Once John began to see the value in the way Avertium approached these assessments, he enlisted Avertium to conduct a few other compliance and maturity assessments, including a PCI readiness assessment and penetration tests on UTMC's network.

Findings during Step 1: Assess



UTMC HIPAA Baseline Assessment:

The HIPAA baseline assessment recognized the need to mature the existing policies to better protect the organization and strengthen its security posture.



UTMC Penetration Test Report:

The UTMC penetration test revealed opportunities to mature the current vulnerability program, including by scanning all systems connected via the environments and making adjustments to its patching protocols.



PCI Readiness Assessment:

The PCI v4.0 readiness assessment highlighted the reporting and procedures that would need to be redesigned to qualify for a v4.0 certification. Some of these changes include modifications to the self-assessment practices as well as developing SLAs with current and future partners using UTMC resources for business use.

Step 2: Design →

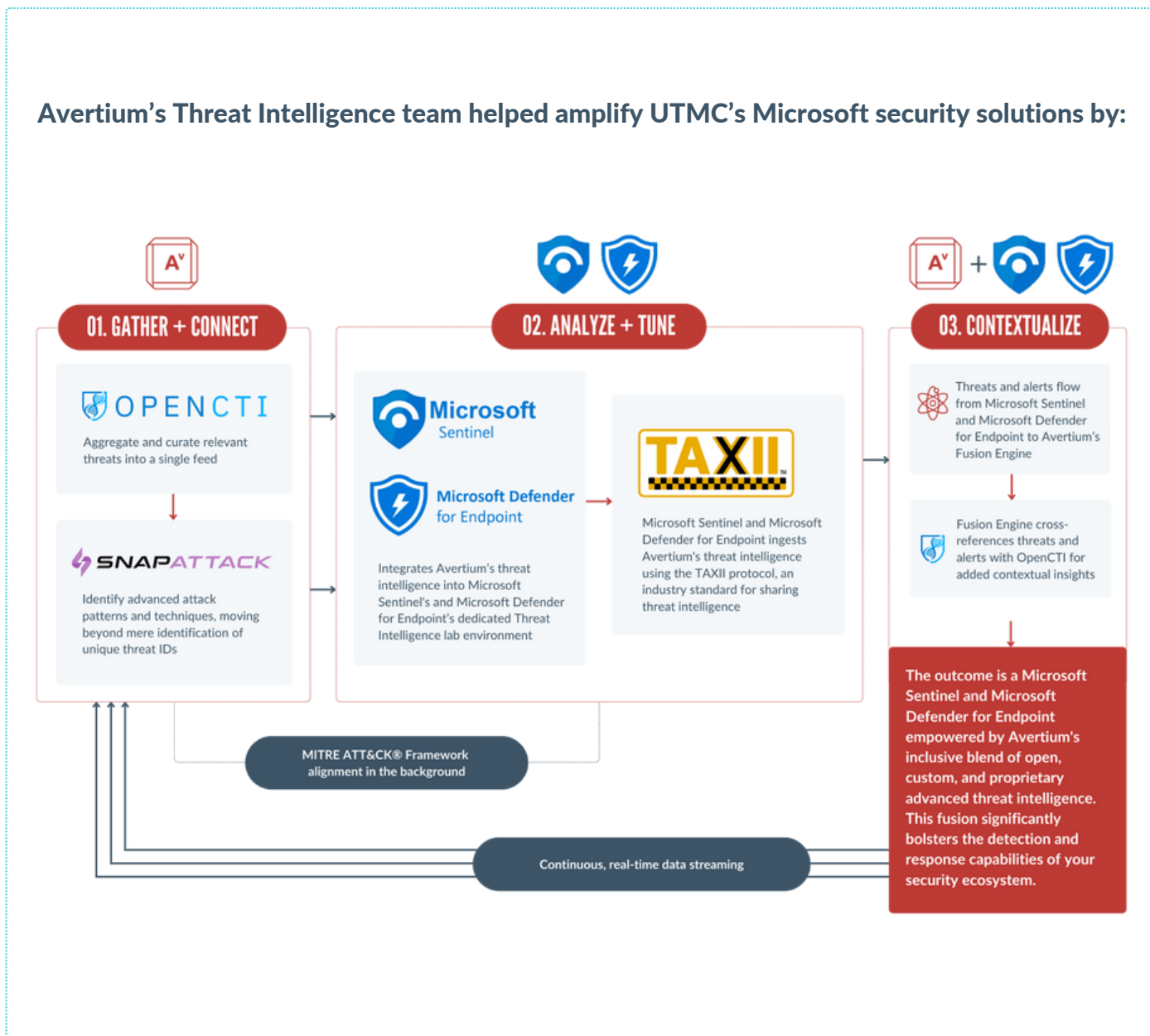
After the HIPAA assessment, Avertium assigned a Strategic Security Advisor – a security expert who works with client leadership to align assessment findings and the security roadmap with the goals of target organizations – to UTMC's account. Avertium's strategic security advisor worked closely with John to develop a pragmatic incident response plan – one that was best suited to UTMC's needs.

Once John saw first-hand how Avertium actually translated assessment insights into real action, John knew this partnership was different. From there, Avertium quickly became John's secret weapon.

Step 3: Protect →

When UTMC's contract came up for their previous managed services vendor, John began leveraging Avertium's team for the resetup and deployment of UTMC's Microsoft Sentinel technology.

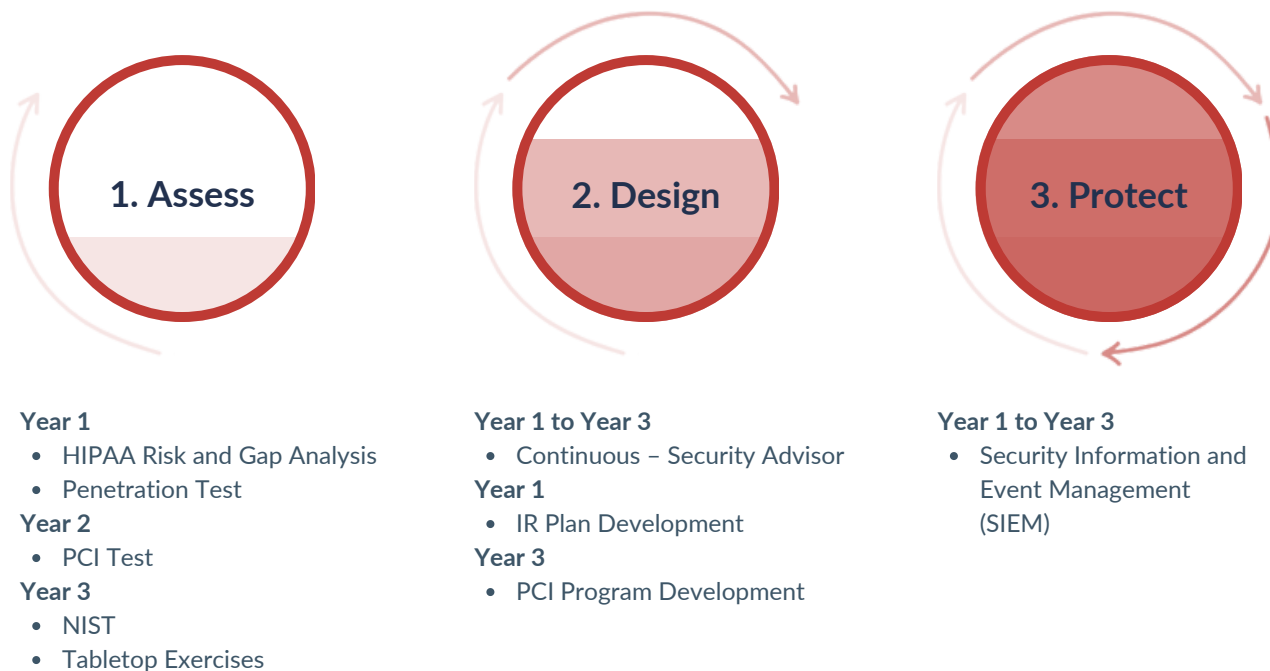
Together, Avertium and UTMC recognized that Microsoft's best-in-suite approach was best for UTMC's smaller team, offering a more consolidated and integrated solution. Building on the work already completed within the compliance space, the Avertium team understood UTMC's business and its threat landscape.



Avertium's service delivery team met with John's team weekly to review and incorporate risk assessment findings and implement remediation recommendations. By leveraging assessment insights to guide the security strategy and tactical management on the ground, Avertium's fusion-first approach offered more context and more clarity as John constructed a proactive cybersecurity strategy for UTMC from the ground up.

And that? That is the story. Avertium came in and solved a problem UTMC needed to solve, worked alongside the UTMC team, built trust, and got things done. And with each cybersecurity challenge that pops up, the cycle repeats.

UTMC x Avertium's "Assess - Design - Protect" Approach Over the Years



I trust that Avertium has a vested interest in our success.

“Other companies don’t have a vested interest in our success. I trust that Avertium does because I’ve seen it myself. That trust in Avertium enables me to be more productive and efficient. It enables me to get out of the weeds.”

– John Jeffries, CISO at UTMC

THE IMPACT

UTMC’s cybersecurity maturity has come a long way since the start of this partnership.

With Avertium’s fusion-first, assess-design-protect approach, organizations like UTMC are able to take two steps forward when they might otherwise only have taken one, accelerating the pace at which they can continue to mature their security posture.

Business-First Mindset →

With this integrated approach, UTMC is now getting more measurable value from their existing cybersecurity investment.

- **ROI Measurement** – UTMC can measure their progress because Avertium benchmarks, measures, and drives continuous improvement in the ROI of UTMC’s security investment.
- **Maximize Investment** – UTMC can now maximize the value of Microsoft Sentinel / existing security investments.

Cyber Fusion Engine →

UTMC adopted a more integrated, fusion-first cybersecurity strategy through Avertium's "Assess - Design - Protect" approach.

- **Assess** – Compliance is a high-value, connected exercise for UTMC. HIPAA and PCI compliance assessments are closely aligned to deduplicate efforts, and assessments are conducted on a continuous basis to prevent the annual compliance fire drill that so many organizations dread.
- **Design** – A dedicated Avertium Strategic Security Advisor works alongside John and his internal team to leverage assessment insights to inform the path toward a stronger cybersecurity strategy, infrastructure, and maturity. With Avertium, UTMC has easy access to a deep bench of trusted SMEs in virtually every cyber discipline – enabling them to punch above their weight from a security perspective.
- **Protect** – UTMC maintains a continuous, optimized approach to its processes and policies. The utilization of Avertium's 24/7 monitoring and threat response services, along with PHI integration and streamlined SIEM tasks, has resulted in an elevated level of security. By delegating SIEM responsibilities to the Avertium team, John's team can now concentrate on internal priorities, resulting in a significant enhancement in the signal-to-noise ratio. Then the cycle repeats. And that? That's the value of a cyber fusion-first approach. Not just seeing the Sentinel side, but all sides.

Human Element →

And finally, John has a partner he can truly count on.

- **Relationships** – John has cultivated a strong relationship with the Avertium team, who is making him a go-to resource for bouncing ideas and seeking recommendations. Avertium's team exemplifies a collaborative approach, consistently probing with the right questions to genuinely comprehend UTMC's priorities.
- **Communicative** – Avertium consistently maintains a proactive approach, conducting follow-up calls and emails while ensuring quarterly touchpoints for ongoing collaboration and alignment.
- **Expertise** – Avertium goes above and beyond by fostering a true partnership rather than just focusing on building reports. This commitment to providing extensive expertise is evident in UTMC's experience. With access to a multitude of subject matter experts (SMEs), UTMC has been able to leverage a diverse range of skill sets to address new challenges as they encounter them.

We have a great process in place with the Avertium team.

"Everything changes and we don't know what to expect tomorrow, but I feel like we have a great process in place with the Avertium team to deal with whatever comes along. It's stressful, sure, but I actually have confidence in our processes, tools, and people. We're not invincible, but we're equipped to handle whatever comes at us."

– John Jeffries, CISO at UTMC

While UTMC has come a long way, their team still seeks constant, consistent growth in their cyber program. And they always will. **Because building security maturity the right way is an endless cycle of assessing your current state, finding and designing solutions to fill your gaps, and shoring up your defenses with focused action.**

It is not static. **It is dynamic and ever-evolving.** But instead of reacting to the ever-evolving demands of the threat landscape, chasing the next shiny object, Avertium's methodical approach helps organizations find their agency and take back control of cybersecurity strategy – and do it with both clarity and confidence.

Level up your cybersecurity posture and contact an Avertium expert today >

ABOUT AVERTIUM

Avertium is a cyber fusion company with a programmatic approach to measurable cyber maturity outcomes. Organizations turn to Avertium for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and Threat Intelligence, Avertium delivers a more comprehensive approach to cybersecurity.

That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

📞 Have questions? Give us a call.
877-707-7997

🖱️ www.avertium.com

📍 Arizona • Tennessee



Copyright © 2023 Avertium