ACHIEVING CMMC LEVEL 3 AND BEYOND TO MITIGATE INSIDER THREATS IN GOVERNMENT

How Zero Trust Provides the Key to Success

archTIS

TABLE OF CONTENTS

INSIDER THREAT FACTS

95%

of cybersecurity breaches are caused by human error

207 DAYS

The average time to identify a breach in 2020

280 DAYS

The average lifecycle of a breach was from identification to containment

<13% IN 30 DAYS

Only 13% of insider incidents were contained in less than 30 days

EXECUTIVE SUMMARY

With so many technologies available to mitigate cyberthreats including SIEM, SOAR, IPS/IDS, Predictive Analytics, AI and Machine Learning, organizations are still getting breached. Zero Trust is gaining momentum as the new standard for defending networks in the Government and the Defense Industrial Base (DIB). Case in point, Defense Information Systems Agency (DISA), is now building out a new reference architecture for zero trust.

With third parties being an attractive attack vector, all DIB players, from the largest Systems Integrators to the small “mom & pop” machine shops in the Defense Supply Chain (i.e. parts for the F-35), must now meet the requirements and audits for CMMC (Cyber Security Maturity Model Certification) to get and maintain government contracts.

All of this is being done to address the multiple threats that are targeting the networks and the data. However, one of the biggest threats is hiding in plain sight—trusted insiders. Known as ‘insider threats’ these incidents encompass negligent employees and contractors, malicious employees possibly working for nation-states or looking for personal gain. Insider threats have quickly become just as big a threat as those from external hackers and other outside influences – and they are even harder to detect.

A couple of statistics to note:

- 95% of cybersecurity breaches are caused by human error. (Cybint)
- The average time to identify a breach in 2020 was 207 days. (IBM)
- The average life cycle of a breach was 280 days from identification to containment. (IBM)
- Only 13% of insider incidents were contained in less than 30 days. (Observe IT)

With the migration to the Cloud, BYOD, and COVID19 creating a world-wide remote workforce, there truly is no perimeter anymore. Now more than ever, we need a seamless way to adapt our cyber defenses to also look towards the inside and proactively secure data. Systems that are designed using Zero Trust principals should be better positioned to address existing threats but transitioning to such a system requires careful planning to avoid weakening the security posture along the way, as they replace the traditional security model. The solution also has to scale to meet the demands of both the DOD and the critical infrastructure players and map to critical controls laid out in NIST 800-171, 800-53, and CMMC – primarily CMMC Levels 3-5.

In this White Paper, we will discuss the problem and then show how to defend and mitigate against threats coming from inside of your trusted network by applying the zero trust methodology to the data layer using Attribute Based Access Control (ABAC).

CYBER SECURITY HEADLINES

"Watchdog finds the Pentagon is behind on several cybersecurity initiatives…"

April 13, 2020, Fifthdomain.com

"Given the increased telework demand, we've seen a tremendous increase on the network. Unprecedented demand just over the last weekend or so, raising worries about cyber-attack" Essye Miller, said.

March 24, 2020, Military & Aerospace

"Cyber-attack on DISA results in data breach that may have affected as many as 200,000 computer system users."

Feb 27, 2020, Military & Aerospace

SITUATIONAL ANALYSIS

Today's media is flooded with stories of new and increasingly severe cyber-attacks such as, SolarWinds, and the Microsoft Exchange Data Breach. These high-profile cases have prompted senior official resignations as well as a loss of public confidence in some industries due to data exfiltration of personal information (social security, driver's license, and credit card information).

To that end, according to a recent report privileged IT users and admins have been identified as posing the biggest security risk, however only a small proportion (22%) of organizations feel that they are effective in managing user privileges.[1] This suggests that privilege management should become a higher organizational priority and a component of the zero trust model. There is also a substantial long-term impact on the security of the United States, our critical infrastructure, and our intellectual property, due to these insider threats (Snowden and Manning to name a few).

Most of these breaches stem from known vulnerabilities in existing network security architectures. These vulnerabilities, which vary in sophistication, could be as simple as using weak passwords (e.g., default value, simple number strings or the word "password" itself). Slightly more sophisticated attacks that leverage phishing attempts through e-mail or social engineering are designed to elicit unsafe action or information that would allow adversaries access using a trusted user's stolen credentials.

These successful cyberattacks highlight the fact that disciplined cyber hygiene is necessary, but not sufficient to prevent all potential attacks and the difficultly in ensuring DOD cyber hygiene policies can keep pace with constantly evolving threats. Systems are simply becoming too complex to defer application and data security to the supporting network's defense appliances and infrastructure. All of our agencies are already stretched to the limit from a resource perspective for all of their NOC/SOC and IA infrastructure teams.

An April 13, 2020 report from Government Accountability Office, titled "DOD Needs to Take Decisive Actions to Improve Cyber Hygiene," warned that the Pentagon faces increased cybersecurity risk because the department hasn't implemented basic cybersecurity practices. DOD teams are having to take on more cyber requirements and responsibilities but are not scaling up the budgeting to properly address the situation. This is not just a DOD problem, this is an inherent problem with the DIB and commercial sector as well.

The Problem

Remember TCP/IP is always on, and when you connect to the network, you are by default on the network. In a nutshell, with all of the "defense in depth" cyber security models and deployments that have been done, the networks, IP-based control systems and data are still at risk. The old notion of defense in depth has been touted by leading security organizations over the past decade, which relies on the National Institute of Standards (NIST) as the basis upon which a security framework can be developed to safeguard our networks. The "depth" includes both physical security protections (walls, gates, locks, guards, and computer cages) and logical security measures, including NGFW, IPS/IDS, SEIM/SOAR, etc.

So, no matter how many layers of network perimeter protection are employed (including AI tools), adversaries continue to overcome defenses through using a variety of countermoves or by exploiting poor cybersecurity practices. The whole mindset here is still to first recognize that something bad is happening, and then try to react to the situation – after the breach. This approach is also designed to protect against outside threats, not threats coming from trusted users.

[1] https://info.nucleuscyber.com/2019-insider-threat-report

The basic premise of zero-trust is trust no one. Do not automatically trust anything inside or outside of your organization's perimeters. Instead, you must verify anything and everything trying to connect to your systems before granting access. The key to proactive security is granting authenticated users the bare minimum access to information while still enabling them to do their job. Too much access and you get data loss; too little and you get frustrated users spinning up rogue clouds – which is a major security problem.

Not only are the DOD/Federal networks at risk, but the 12 identified critical infrastructures and the Defense Industrial Base (DIB) are also principal targets for insider threats and nation state threats perpetrated by insiders. The United States has lost billions of dollars in intellectual property, revenue, and corporate creditability, due to network breaches at some of our most prestigious and notable companies, infrastructure companies, and defense contractors. The tech industry, Congress and NIST have all struggled with how best to address these issues.

The Insider Threat—Our Achilles Heel

An insider threat is when someone close to an organization with authorized access to data and systems misuses that access—negligently or maliciously—to negatively impact the organization's critical information or systems. It's not just employees that pose a risk; third party vendors, contractors, and partners with access can pose a threat as well.

Overall, there are three common types of insider threats:

1. **Negligent insiders** who inadvertently compromise data. For example, if an employee misplaces a laptop or incorrectly sends an email, or clicks on a phishing email, compromising their system.
2. **Malicious insiders** who commit acts such as data and IP theft, fraud, sabotage, and espionage.
3. **Compromised insiders** whose credentials are stolen by a bad actor.

The Insider Threat Report from Cybersecurity Insiders,[2] a 500,000-member community for information security professionals, explored how organizations are responding to the evolving security threats in the cloud. A majority of organizations consider themselves only somewhat effective or worse (58%) when it comes to monitoring, detecting and responding to insider threats both in the Cloud and on-premises.

Their Key findings include:

- 68% of organizations feel moderately to extremely vulnerable to insider attacks
- 70% of organizations confirm insider attacks are becoming more frequent
- 56% of organizations believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud
- 85% of organizations find it moderately difficult to very difficult to determine the actual damage of an insider attack
- 39% identified cloud storage and file sharing apps as the most vulnerable to insider attacks

At a recent 'Insider Threat Conference', the principal focus for the first day and a half, was on the persona of the potential insider threat actor, not the acts themselves. In the example given, a large public safety Governmental agency stated that the average insider threat "dwell time" (time that an insider is in the network before being identified) was well over 170 days before being contained.

[2] https://info.nucleuscyber.com/2019-insider-threat-report

THREE KEY SOURCES OF INSIDER THREATS:

1. Negligent insiders who inadvertently compromise data.
2. Malicious insiders who commit acts such as data and IP theft, fraud, sabotage, and espionage.
3. Compromised insiders whose credentials are stolen by a bad actor.

Even if a person is deemed a potential threat, it all has to be documented and a case built. All of this takes valuable time and resources. By the time they build a case, it's too late. Furthermore, insiders with privileged access (such as Snowden, Pvt. Manning, and others) have a much better chance of successful data exfiltration due to their unlimited network privileges and may not show up as a risk until the damage has been done. It then becomes a forensics exercise in assessing the damage.

Another critical area for DOD/Federal environments, are the legacy systems that now leverage middleware to connect to newer IP networks and DOD systems that are certified and built on older, non-supported operating systems and other coding types, but are in full production networks and need to be protected. Existing security methodologies will not address these critical issues and without OS support from the manufacturer, it is nearly impossible to "harden" these critical systems any further. In addition, as the new NIST requirements are put in place, the CUI and FCI requirements for tagging the data is critical for moving forward. Per DOD 5200.48:

For federal systems, IS storing information identified as CUI must meet the minimum network security standard in Part 2002 of Title 32, CFR. For nonfederal systems, IS must meet the standards in the NIST SP 800-171, when established by contract.

When DoD legacy information is incorporated into, or cited in, another document or material, it must be reviewed for CUI and marked in accordance with this issuance.

CMMC: ESTABLISHING MINIMUM SECURITY STANDARDS TO COMBAT CYBER THREATS

In order to address growing cyber threats, the US Department of Defense and NIST released the much-anticipated Rev 2 of SP 800-171 and the working draft of supplement SP 800-171B. As the core part of the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirements, SP 800-171 focuses on protecting controlled unclassified information (CUI) for Department of Defense contractors. For some contractor information systems managers, these are the minimum-security standards and for some, SP 800-171 is bringing the organization up to adequate security to secure DOD contracts.

Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) is a new requirement for existing DoD contractors, replacing the self-attestation model and moving to third-party certification. This new certification is intended to tighten cybersecurity within the defense industrial base (DIB). CMMC consists of five levels to measure cybersecurity practices of contractors. The level of CMMC a DIB organization will need depends on the type of information in its IT system.

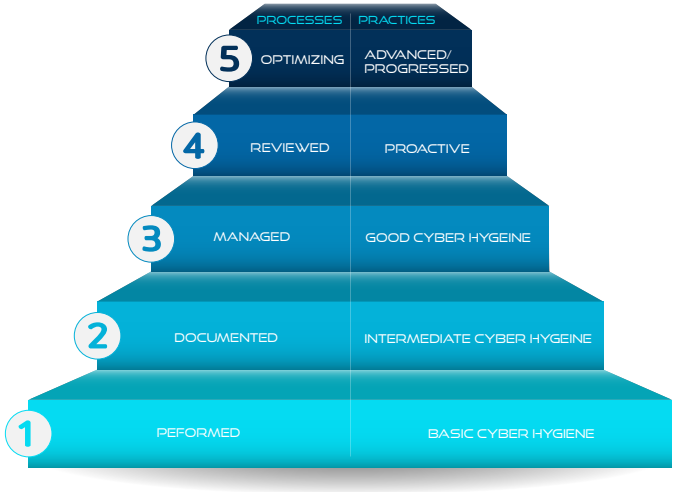
When you reach CMMC Level 3, you also have to meet the requirements for DOD INSTRUCTION 5200.48:

- **Federal Control Information (FCI)** – information provided by or generated for the government under contract not intended for public release.
- **Controlled Unclassified Information (CUI)** – information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.

CMMC Capabilities and Maturity Levels:

- **Level 1 Safeguard Federal Contract Information** focuses on "basic cyber hygiene" practices such as using anti-virus software and regularly changing passwords. Basically, follows FAR 52.204-21.
- **Level 2 Transition Step to Protecting Controlled Unclassified Information (CUI):** Requires "intermediate cyber hygiene" and serves as a stepping stone to Level 3.
- **Level 3 Protect CUI** is what the Pentagon expects a plurality of the defense industrial base to achieve. NIST SP-800-171 Rev2 compliant.
- **Level 4 Protect CUI / Reduce Risk of Advanced Persistent Threats (APT) and Level 5 Protect CUI / Reduce Risk of APTs** are even more stringent and will be imposed on "very critical technology companies" working with the most sensitive information.

THE CMMC MATURITY MODEL



The Impact of CMMC

DoD expects CMMC to take five years to fully roll out and will really get going in 2021. DoD expects the third-party assessors to certify about 1,500 vendors in 2021, 7,500 more in 2022 and 25,000 more by 2023. By fiscal year 2026, all new Defense Department contracts will contain CMMC requirements that companies must meet to win the award.

As we now look at this new evolving operational environment that's being tailored for the DOD, in this case, the Cyber Domain, it significantly impacts all other Warfighting Domains, and now relies heavily on secure cloud, intranets (SIPRNet/NIPRNet), collaboration portals and COTS-based network technologies, services, and applications to service the needs of the warfighter, air assets, Coalition partners and tactical communication across the battlespace. This may include the Battle Command systems, down to the soldier and weapons platforms.

There are additional moves to implement multi-domain operations/environments which will additionally impact various "Cyber AORs," to include the Air Force Information Environment (AFIE), the Enterprise Battle Management Command and Control Systems, JADC2 (Joint All-Domain Command and Control), along with manned/unmanned (UAS/UAV/UUV) assets, along with how and what information will be shared in a multi-coalition environment.

There has also been a lot of discussion and interest in permitting unclassified users to use the SECRET High Tactical Internet to access unclassified computers connected to the commercial Internet. This capability is of particular importance to certain users, who typically use unclassified applications and data, and need to communicate in a split-based mode with large computer systems. This will inherently create even greater operational cyber risks and an even greater need for not only zero trust network solutions, but a way to extend this same level of control to application and data access.

THE PROBLEM WITH EXISTING SOLUTIONS

How About Machine Learning and AI?

To mitigate insider threats, some experts suggest that enterprises develop their own risk algorithms by coupling machine learning capabilities with behavioral analytics to understand discrepancies in employee activities, which was a topic at the Insider Threat conference referenced earlier.

While the increasing volume of insider threats has caused cybersecurity professionals to take more proactive steps and deploy User Behavior Analytics (UBA) tools to detect, classify and alert anomalous behavior, the threats are still in the network.

While this sounds like a good strategy, it is reactive. These systems detected a problem after the fact and the damage is already done. There is also a significant time delay in consolidating the data and then, flagging a threat.

Organizations also rely on user training (51%), information security governance programs (41%), user activity monitoring (36%), background checks (36%), and native OS security features (20%).[3]

Many CISO's recommend that HR data is key to building out risk models. Taking contextual employee data and online activity to create risk algorithms. You still have to refine and contextualize the data in order to correctly identify potential threats and it only considers legitimate employees. It does not address a compromised endpoint by a contractor or an active sophisticated hack.

SEIM, SOAR, and Deception Solutions?

Firewalls, network appliances and intrusion detection systems generate huge amounts of event-related data—more data (log files) than security teams can reasonably expect to interpret. A SIEM makes sense of all of this data by collecting and aggregating and then identifying, categorizing, and analyzing incidents and events. This is often done using machine learning, specialized analytics software, and dedicated sensors. The SIEM examines the log data from all of the devices (firewalls, IPS/IDS, etc.) for patterns that could indicate a cyberattack, then correlates event information between devices to identify potentially anomalous activity and finally, issues alerts accordingly. What about the data?

The SIEM approach remains reactive, it can only detect a breach or suspicious activity after the fact. Furthermore, the need for regular tuning leads to security analysts and engineers wasting precious time on making the tool work for them instead of triaging the constant influx of data. It's no surprise that not having enough resources to operate and manage SIEM tools are some of the biggest bottlenecks to more effective use of the platform (31%). This is followed by being overwhelmed by too many false positive alerts (22%) and not being able to detect unknown threats (18%)[4]. SIEMs do nothing for the data.

Like SIEM, SOAR is a reactive tool designed to help security teams manage and respond to endless alarms at machine speeds. SOAR integrates all of the tools,

[3] https://info.nucleuscyber.com/2019-insider-threat-report

[4] 2020 Insider Threat Report Cybersecurity Insiders

systems and applications within an organization's security toolset and then enables the SecOps team to automate incident response workflows. A SOAR's main benefit to a SOC is that it automates and orchestrates time-consuming, manual tasks, including opening a ticket in a tracking system, such as Jira, without requiring any human intervention—which allows engineers and analysts to better use their specialized skills. Again, the data remains at great risk.

Where do we go?

Solving the problems posed by insider threats, and protecting the data, requires a different information security approach. Traditional informational security is designed to focus predominantly on outside threats like hackers or unauthorized user access and is no longer enough. SIEMS, SOARs and other solutions are reactive and don't do anything to prevent the initial loss of data—they are focused on the actions of the attacker and not on the data. Re-purposing tools created to detect threats from outside is not sufficient to provide the level of proactive data security and metadata tagging required to battle the types of threats that come from the inside and are harder and will take longer to detect even with these tools in place. Extending zero trust to information security provides a solution.

ZERO TRUST INFORMATION SECURITY

There is a fundamental flaw with most existing security software solutions and with many security policies that are making data more vulnerable: the login process is not robust enough to guarantee that the logged in user is who they say they are, with no attribution at the user level. So, if someone logs in with stolen credentials, they can use the access and privileges of the compromised account to navigate systems and data, stealing as they go. In this case, the security lies within the permissions of the logged in user only.

Systems that are designed using Zero Trust principals should be better positioned to address existing threats, if done properly. Transitioning to this new reference architecture will require careful planning to avoid weakening the security posture along the way. For the providers that are trying to migrate to this zero-trust environment, they need to understand that it will require continuous verification of the operational picture via real-time information.

This new data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing, or denying access to resources. A model that is just "allow" or "deny" will not be sufficient to meet zero trust needs. Access must also be provided using various/different levels of control (secure reader, encrypt to audience, DLP, redaction, trimming). Remember that all of the zero trust players bringing their solutions still do not focus on the data, they focus on the network and the user – not the data.

A data-centric policy-based approach based on 'Zero Trust' is a far more effective methodology to ensure data remains secure. This modern approach does not automatically trust any user inside or outside your perimeters, instead you must verify anyone trying to connect to any systems, applications, or individual data files before granting access to them. Attribute-based access control (ABAC) is a Zero Trust security model that evaluates attributes (or characteristics of data and/or users), rather than roles, to determine access. It uses a data-centric security approach that evaluates each file's attributes including security classification and permissions, as well as user attributes such as security clearance, time of day, location, and device to determine who is able access, as well edit and download files.

This will give agencies granular, real-time control over the access of information by adjusting security in real-time to determine whether the user should be given access to the requested information based on all of these parameters at that point in time. If the user scenario does not match, or appears suspicious, then access is denied, or a restricted view of the data is provided. For example, if an authenticated user is trying to access a sensitive file they own, but it is outside of business hours and they are using a BYOD device in another country, file access will be denied – effectively thwarting a hacker using stolen credentials.

Meet and Enforce Key CMMC Capabilities with ABAC

The NC Protect solution provides dynamic data-centric security to automatically find, classify and secure unstructured data on-premises, in the cloud and in hybrid environments. NC Protect dynamically adjusts data access and protection based on real-time comparison of data and user attributes to make sure that users view, use, and share files according to your agency's regulations and policies.

The platform is fully integrated with Microsoft 365 apps including SharePoint, Teams, Yammer, OneDrive, Exchange, as well as Nutanix Files, Dropbox and Windows files shares to centrally secure your collaboration to meet and enforce CMMC requirements.

We are in a world of information sharing, and collaboration that leverages the full Microsoft stack for almost all Federal and DOD environments, including our coalition partners. Using a solution like NC Protect that utilizes attribute based access and control (ABAC) policies has many benefits and affords granular data security to not only ensure compliance with CMMC capabilities to meet Level 3-5 requirements but also ensure operational security by delivering a seamless ABAC solution to deliver and share information to our coalition partners.

The key to this, is NC Protect's ability to scan the Microsoft environment, add metadata tagging to the documents or leverage MIP sensitivity labels, it then evaluates both data and user attributes against policies to determine appropriate access, usage and sharing rights. A complete audit trail of all document access is logged and can be reported on using Azure Sentinel or Splunk. This level of granular control is the key to attaining CMMC Level 3 – 5.

HOW NC PROTECT HELPS WITH CMMC COMPLIANCE

Access Control (AC)

- Apply user specific encryption and DLP – Secure information every time a file is opened using security policies that are specific to each user. For example, ensure each user opens their own encrypted copy of the original document. Lock down functions such as print, save as, copy, paste based on the sensitivity of the document.
- Provide Time limited access. For example, if a user opens a file for editing, you can set a limit on the time they have to perform the editing before the file can be saved back to its origin. Outside of this window, access can be denied to the authenticated user.
- Enforce Secure Read Only Access to force viewing in an in-app secure reader rather than the standard editor, for users that only need read only access.
- Dynamically apply secure personalized watermarks that incorporate user attributes such as name, date, time, etc. and cannot be edited or removed to track chain of custody of printed materials and to deter photographing, an easy way to bypass security measures.
- Reduce the attack surface by forcing users to access a single source, master document. Document proliferation is an unpleasant side effect of many collaboration platforms. When a user adds a file to a chat message, sends an email or uses a cloud based editor, copies of the document are left lying around – often in locations far less secure than the source document.

Audit & Accountability (AU)

- Track access to sensitive data, ensuring transparency and accountability.
- Report on the number of issues identified by classification level and allow policy officers to review the results and rescan, reclassify, or reapply permissions if needed.
- Integrate user activity and protection logs with SIEM tools like Splunk and Microsoft Sentinel for further analysis and downstream actions.

System & Information Integrity (SI)

- Identify and manage information flaws to assess if sensitive information being stored in the wrong place or allowing incorrect user access.
- Implement advanced email protections to prevent users from accidentally emailing sensitive data, sending it to the wrong recipient or stealing data via email.
- Replace attachments with a link to a secure web viewer or file URL that requires additional authentication and verification.
- Prevent admins from viewing documents in the sent mail folders of other users or collaboration tools: SharePoint, OneDrive and Microsoft Teams.

Federal Control Information (FCI)

Tag and manage information provided by or generated for the government under contract not intended for public release.

Controlled Unclassified Information (CUI)

Tag and manage information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.

A ZERO TRUST SECURITY MODEL IS THE WAY FORWARD

Today organizations must assume they will be compromised by a bad actor, disgruntled employee, or malicious software. We can no longer afford to settle for after the fact detection and user behavior analysis to detect a breach, an approach that attempts to limit rather than prevent damage.

The solution is a Zero Trust approach that is not just employed for system and application access, but also extends to file access and sharing controls to help ensure the standards set by CMMC around the collaboration of FUI and CUI are met.

Only by using real-time data security that leverage ABAC policies which take into consideration content and context, can you prevent both negligent and malicious data loss.

NC Protect provides this level of advanced information protect that's simple, fast and scalable to protect sensitive information across the Microsoft collaboration stack. To learn more visit www.archtis.com.

"Secure collaboration is always top priority for our customers, and archTIS' integrations can help customers with highly sensitive data to ensure it remains protected as it is shared through the collaboration life cycle."

—Ryan McGee

Security Product Marketing, Microsoft Corp

archTIS

Microsoft Partner

Member of Microsoft Intelligent Security Association

Microsoft

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files and Windows file shares. For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS

archTIS.com | info@archtis.com

Australia | United States | United Kingdom