A good DEFENSE never rests.

– F. Lee Bailey

Your security depends on the ability to detect and defend against the rapidly evolving threats to your cloud and on-premises environments. Todays hackers are highly sophisticated and very motivated to find ways into your network. Like most complex business issues, there's no magic bullet for identifying and protecting your business against these threats. That's why Appalachia offers a multi-layered approach to cybersecurity.

MANAGED THREAT DETECTED AND RESPONSE:

Many businesses have trouble keeping up with today's dynamic threat landscape. As a result, many are enlisting the help of a Managed Security Service Provider to protect their networks cost-effectively and reliably. When you outsource your security operations to Appalachia, you can realize the full benefits of complete threat detection without investing the time or resources required to deploy and maintain a complex SIEM solution. **Our NOC/SOC is staffed by all US-based, W-2 employees**.

Appalachia Technologies is SOC 2, Type II Audited SOC 2 audits are based on the AICPA's Trust Services Criteria. SOC 2 service auditor reports focus on a Service Organization's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system. "Appalachia Technologies delivers trust-based services to their clients, and by communicating the results of this audit, their clients can be assured of their reliance on Appalachia Technologies' controls."

Proactive Threat Detection

We monitor network traffic for suspicious activity or anomalous behavior.

Suspicious patterns are verified against known attack signatures and other indicators of compromise for early detection of active threats.

Threat Response

Our security analysts investigate events real-time to identify and alert you of potential threats in your environment.

Once confirmed, our team works quickly to isolate and eradicate threats before they can spread further within your environment, or worse… your clients.

Compliance

Stay ahead of compliance requirements and auditors with regular reports to show progress towards compliance as well as identify weak spots in your environment.

Appalachia's Protect+ service helps you meet compliance requirements such as PCI-DSS, NIST CSF, HIPAA, ISO 27001, CJIS, SOC 2, and more.

PROTECT YOUR BUSINESS FOR A STARTING PRICE LESS THAN HIRING A SINGLE SECURITY ANALYST.

Find
5012 Lenker Street, Mechanicsburg, PA 17050

Email
Info@appalachiatech.com

Call
888.277.8320

Visit
www.appalachiatech.com

How Our Security Operations Center Works

Appalachia's Security Operations Center (SOC) is staffed by highly-certified cybersecurity analysts who actively work to defend your business.

When you outsource your security operations to Appalachia, you can realize the full benefits of complete threat detection without investing the time or resources required to deploy and maintain a complex SIEM* solution.

Platform Components

Security Log Collection and Retention – Storing logs on a local device can be risky. Adversaries often cover their tracks by wiping local logs, and manipulating event data. Appalachia helps to mitigate these risks by storing logs on a segregated, secure system. These events are stored for a year to be reviewed, and have searchable retention of 30-days to cross reference events across multiple systems.

Standard Reports – Knowing when events happen in your environment is critical in building an appropriate response, which is why this is such an emphasized requirement in most compliance standards. Appalachia works with your specific requirements to get you the data you need to run your business, without having to spend the time doing the legwork. Receive regularly scheduled reports to stay in the know weekly, monthly, and quarterly. Report on key events like logins from your administrative accounts, detection of vulnerable protocols like TLS 1.0 or SSL 3.0, brute force login attempts, newly created privileged accounts, or additions/removals to administrative group memberships.

Network Intrusion Detection – Appalachia's skilled SOC technicians monitor traffic at key points in your network for known threat signatures as well as baselined traffic patterns. This data is leveraged to build a more complete picture of which applications are operating in your network, and when they are potentially being used against you.

Host Intrusion Detection – Unsecured or unmonitored privileged accounts are one of the most commonly exploited vulnerabilities in data breaches. Leveraging early warning signs, Appalachia quickly works with you to respond to potential threats before your data is in the wrong hands. We identify key security events like newly created privileged accounts, use of unapproved USB storage devices, and usage of default admin accounts to isolate active threats and shut down attack vectors.

Security Information and Event Management (SIEM) – Having logs collected to dig through after an event happens is helpful, but correlating those logs and identifying known attack patterns as they're happening can prevent incidents from escalating into breaches. Appalachia leverages the MITRE ATT&CK framework to identify network behavior early in the attack chain, and stop malicious actors before they can compromise your resources. Our goal is to keep your data where it belongs, and keep your company name from being the next security headline.

File Integrity Monitoring – Most configuration files don't change regularly, but making that assumption can be dangerous. Let Appalachia know which critical files should never change, and we regularly hash those files to identify if even 1 bit in the file has been altered. This is great to know if your web servers have been altered, or if someone changed an HR database. It is important to note that this does not replace the need to back up these files – always back up critical data!

Vulnerability Scans – Staying on top of the latest vulnerabilities can feel like a full-time job. With new threats emerging daily, most IT teams simply cannot keep up! Appalachia works with your company to conduct monthly vulnerability scans of all secured assets. These scans leverage the latest known vulnerabilities signatures and provide prioritized lists of risks to your company assets. Once the risks have been identified and prioritized, Appalachia works with your organization's risk management program to help build remediation plans to keep you safe and compliant.

Compliance Readiness – Even those who like surprises rarely want a surprise from a compliance auditor. Stay ahead of compliance requirements and changing standards with quarterly compliance reports from Appalachia's SOC. These reports highlight at-risk assets and non-compliant device configurations. While Appalachia cannot provide official audits or certifications, we can make your compliance roadmap much shorter!

LET US MANAGE YOUR IT SECURITY SO YOU CAN FOCUS ON YOUR BUSINESS.

Find
5012 Lenker Street, Mechanicsburg, PA 17050

Email
Info@appalachiatech.com

Call
888.277.8320

Visit
www.appalachiatech.com