WIND™

ElectronicDesign

WHY YOUR COMPANY NEEDS TO CREATE A SECURITY POLICY BEFORE IMPLEMENTING A SECURITY PROGRAM

Security is a critical concern across a wide spectrum of industries. Ensuring security on embedded devices is a key element of an enterprise's overall security strategy. In this white paper we'll review research findings from a recent security study, interpret those findings, and make suggestions on how to implement a valuable security plan.

I INTRO

It is broadly understood that in today's connected world, everyone's data is at risk. In the embedded world, security goes well beyond data. If an embedded device is not secure, it cannot be safe, which means your entire system is not safe. We are not talking about server failures due to software hacking; we're talking about specific device security. Attacks can come from a lot of areas, including active side-channel attacks, memory and bus attacks, cold boot attacks, and, of course, network attacks. Cybersecurity is a worldwide issue with every connected device being a potential attack vector, or entry point, for an attack.

IdentityForce®[1] has reported that between January and September of 2019, there were over 7.9 billion data records exposed—a 33 percent increase from the same time in 2018. According to their website, "Although hackers are obvious culprits in uncovering this data, oftentimes they had a helping hand from human error resulting in a data breach." In a recent TechCrunch[2] article, a newly discovered hacking group was targeting energy and telecom companies where it targets devices, firmware, and telecommunications networks. And, according to a recent article in United States Cybersecurity Magazine[3],

"CYBERSECURITY REPORTS BY CISCO SHOW THAT THIRTY-ONE PERCENT OF ORGANIZATIONS HAVE AT SOME POINT ENCOUNTERED CYBER-ATTACKS ON THEIR OPERATIONS TECHNOLOGY."

Make no mistake, security is important.

Cyberattacks can disrupt businesses, compromise intellectual property, or wreak financial and reputational damage. The Internet of Things (IoT) opens up game-changing new opportunities from increased connectivity and the ability to better leverage data-driven insights, but it also ushers in unprecedented risks. With the proliferation of connected devices, the potential for new vulnerabilities is staggering. With the stakes higher than ever, it is ever more important to act now.

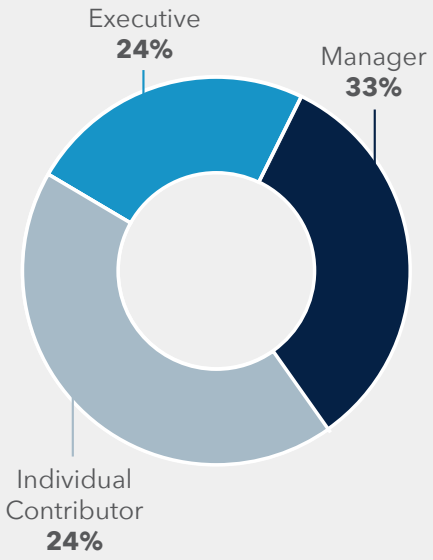


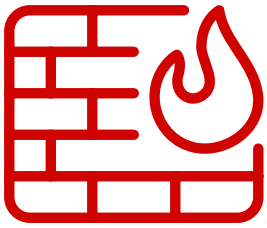
Figure 1: Breakdown of respondents.

RESEARCH SURVEY RESULTS

Sponsored research conducted by Electronic Design magazine found that security for embedded systems used in industry is an important, yet challenging, subject to understand and implement. In their 2020 research, they heard from embedded system engineers who were involved with both software and hardware development, as well as each expertise separately. The research focused on executives at 24 percent return, managers at 33 percent return, and individual contributors to the security team at 43 percent return (**see Figure 1**). What's important to note from the research is that a large percentage, 31 percent, were from industrial companies, 10 percent from medical manufacturers, 10 percent from defense, 9 percent from automotive, and a smattering of others from aerospace, telecom, energy, and robotics. With such a broad and significant return, researchers were able to find clear answers to important questions.

Respondents considered the biggest security threat to be device failure or takeover. In fact, 63 percent of managers and 59 percent of individual contributors have this concern at top-of-mind. The executive team appears, at 40 percent, to be more concerned with stolen credentials. Attack vectors into the enterprise has a 24 percent concern from individual contributors but much lower from managers and executives. Other concerns, such as zero-day vulnerabilities, counterfeit parts, and internal user failures have a much lower percentage rate at less than 20 percent.

So, where do security requirements come from? According to the survey, companies are paying attention to industry recommendations as the primary requirements source. This is especially true according to the executives surveyed. In house recommendations come in second, then the suggestions from government agencies. Others mentioned included a company's own IT department and customer requirements. Although a high percentage (46 percent) of executives believe their company is spending between 10 and 24 percent of its focus on security features and common vulnerabilities and exposure (CVE), 40 percent of individual contributors say that their focus on security features and CVE are less than 9 percent. Managers appear to be split between these two, while leaning slightly toward the executive understanding. This is a surprising gap between perception at the executive level and the reality at the engineering level. A recent report from CISO Economic Times[4] stated that over 375 new cyber threats per minute was seen by McAfee during 2020Q1.



Here's where the research survey gets interesting. In support with what responders believe about the biggest security threats, access control, authentication, data integrity, and IP protection are the most important design-in security considerations. Two more aspects of security—protecting data in motion and protecting data at rest—were at the lowest end of the spectrum. This disparity will be discussed in the next section, but it should be noted that this response was across all three categories of respondent. Laws such as the European Union's General Data Protection Regulation (GDPR) enables extremely punitive damages in the case of unauthorized disclosure of personally identifiable information (PII).

The number one roadblock to security, according to the survey results, was in determining how far to secure an asset—indicating either the lack of a security policy or the need for better understanding what is at stake. The second most common roadblock mentioned was the overall complexity of implementing security, followed by limited in-house expertise and budget restrictions.

Considering complexity and limited expertise, it's clear why they show up together. If a company lacks in-house expertise, it is natural that they would consider the problem was due to complexity. This is why embedded software experts like Wind River offer a security assessment service to companies designing a product. Implementation assistance is also offered once the assessment has been completed.

When survey respondents were asked which phase of the device lifecycle their team spends the most time on related to security, the responses varied greatly. This indicates some disconnect between the executives, managers, and individual contributors. For example, 35 percent of executives felt that the team spent most of its time on design and only 18 percent on maintenance. Managers felt that 29 percent of time was spent on implementation and another 27 percent on maintenance. The individual contributors were much closer to the executive responses and showed that 30 percent of their time was spent on design, 29 percent on implementation, 24 percent on requirements, and only 16 percent on maintenance. The reality is, security is a full lifecycle exercise, from inception to deployment. A solid security strategy starts with a written and agreed upon security policy, which we'll cover more thoroughly later in this paper.

43%
of executives

40%
of managers

29%
of individual contributors

didn't know they had a breach until their end customer discovered it and alerted them to the fact.

When asked what security practices from the IT world were most relevant for embedded system development, the majority of respondents from all three levels of organizational roles selected monitoring security events from the device—all in the 60 to 66 percent range. Although a large number of executives (57) percent felt that actively monitoring vulnerability announcements is important while only 32 percent of individual contributors felt that was necessary.

Half of respondents felt that device integrity (maintaining the content of the device) was most important to their project a small percentage of them (less than 26 percent) believed that maintaining the privacy of the device was important. Less than 30 percent believed that availability—maintaining access to the device—was important to their project.

Security breach detection is what we started with in this white paper. It's important that we understand and communicate that this is important. The shocking data to come from the question of how security breaches are being detected in deployed devices shows how misunderstood security in embedded systems can get. Forty percent of executive as well as 40 percent of individual contributors believe they have never had a breach. Further, 43 percent of executives, 40 percent of managers, and 29 percent of individual contributors responded that they didn't know they had a breach until their end customer discovered it and alerted them to the fact. Even though 60 percent of executives believe that breaches are detected by using simulated threat tests in a lab, only 26 percent—less than half—of individual contributors say that is happening.

So, what compliance documentation do respondents want to see from their software supplier? Simulated penetration testing results and other test artifacts was the number one response, with executives at 73 percent, managers at 68 percent, and individual contributors at 59 percent **(see Figure 2)**. Coming in second was third party certification and evaluations, while a full bill of materials of all software components in the device came in last.

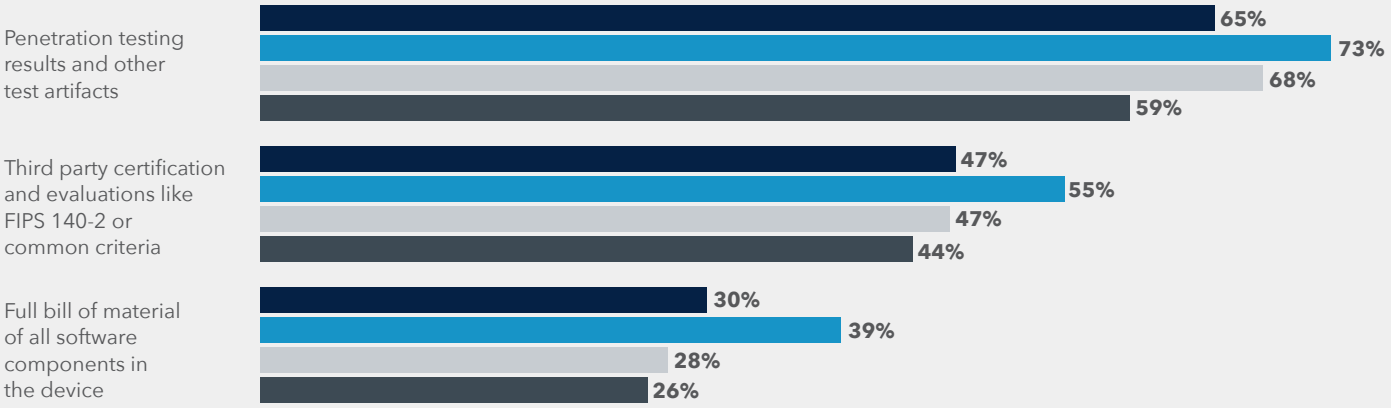


Figure 2: Compliance documentation expectations.

Other mentions included debugging documents and full lab tests as to vulnerabilities and mitigation strategies.

Along the lines of testing, nearly two-thirds of executive level respondents say they test an embedded device for security risks through the use of simulation tools. Forty percent say that their team of engineers do a hackathon before deployment. A smaller, less than 25 percent of respondents say they hire a third party to perform testing. The number one average response was that their company does limited testing for threats at all. In fact, 58 percent of individual contributors and 50 percent of managers stated they do limited testing.

Maintenance is a highly regarded and organized operation in most industrial and manufacturing companies as well as utility and energy, oil and gas, and medical and aerospace facilities. Yet, when it comes to ongoing security maintenance, updates, and patches for embedded security devices over ten percent of respondents say they don't do any. An average of 45 percent perform updates over the air, and an average of 61 percent say they do updates manually. The concern here is that manual updates are much more expensive and time consuming versus over the air updates.

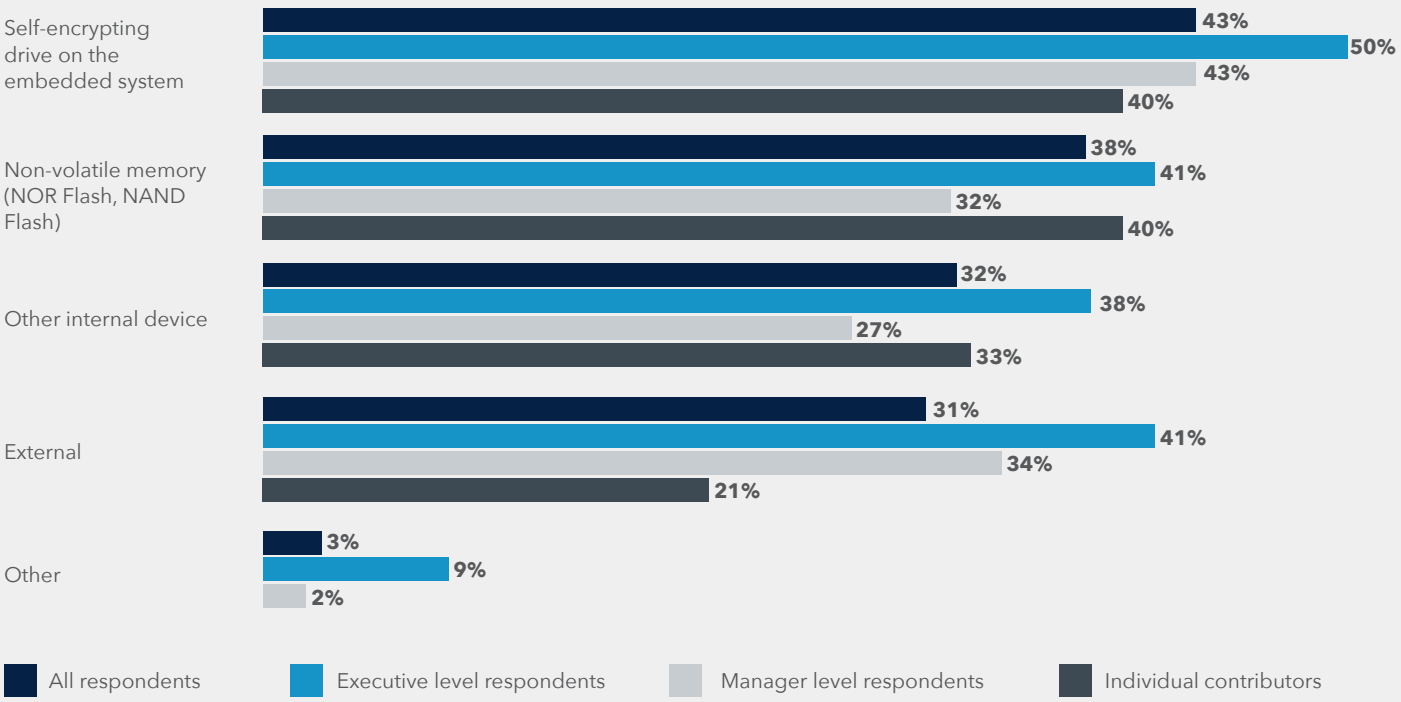


Figure 3: The handling of data storage.

Data storage is handled in a wide variety of ways and fairly equally across the board and include self-encrypting drives on the embedded system, non-volatile memory, other internal devices, and other external devices such as the cloud **(see Figure 3)**. As for what the best operating system respondents believe fulfills the most security requirements they face, executives believe that real time operating systems work best, while managers and individual contributors are split between real time, Microsoft Windows, and embedded Linux distribution. Less than 12 percent of respondents believed that enterprise Linux distribution was the right choice.

WHAT THE SURVEY DATA INDICATES

A number of things can be gleaned from the responses that came from our "Ensuring Security on Embedded Devices" research project. The first thing we believe it's important to note is how much variation there is between executive level respondents, manager level respondents, and individual contributors.

9% - 12%

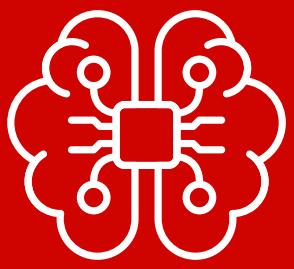
of companies

don't even do security maintenance updates

The average of

34%

who believe they've never had a breach indicates how removed companies are from the facts.

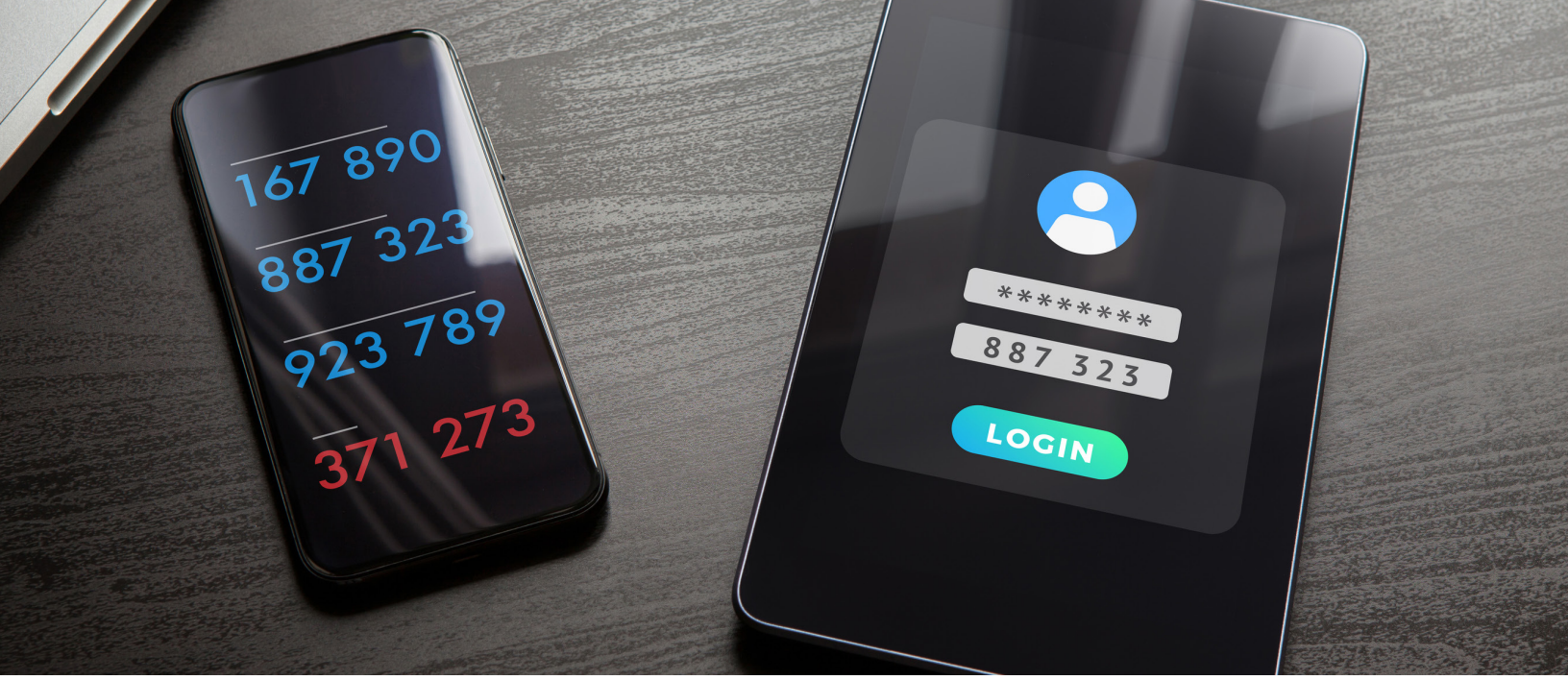


This variation is first seen when considering the results when asked what percentage of the organization's focus is on security in the first place. This disconnect is also relevant when considering the most importance design-in security considerations, which shows that authentication is a key factor to executive level respondents while access control is more important to individual contributors where executives rate that near the bottom of their concerns.

Even though all three groups believe in the need to determine how much security is enough, they can't seem to agree on how much focus should be placed on each phase of the device lifecycle. There is only a 9 percent average difference between design, implementation, requirements, and maintenance with the executive level respondents leaning toward design while the least concern from all three levels goes toward maintenance, which in any other aspect of their business would be a high priority. Along these lines, it is again, shocking, to see that 9 to 12 percent of companies don't even do security maintenance updates.

Another concern for any company should be how they perform security breach detection. Our survey shows that way too many companies rely on their customer to discover breaches and then alert them, leaving all the responsibility with someone else and taking very little of it for themselves. The average of 34 percent who believe they've never had a breach indicates how removed companies are from the facts.

So, how does the role of AI play in securing devices? According to the survey results there is a mismatch between executives who believe (at a 59 percent rate) that AI should be located on the deployed device, while 60 percent of the individual contributors responded that there are no plans of using AI at all. Once again, this disconnect is concerning.



WHAT A SECURITY PLAN SHOULD LOOK LIKE

This white paper has shown what research has uncovered concerning embedded security devices, as well as what this indicates might be a huge disconnect between the three different sets of in-house players. Using this information, we'd now like to draw a clear and implementable picture as to what a security plan for embedded devices should entail.

Transparency between the three levels of in-house teams is shown to be a key missing element in the research. Simply allowing executives, managers, and individual contributors to your embedded security plan will allow everyone to be on the same page. Having an agreed upon security policy before a project starts gets everyone on the entire team on the same page. Such a policy also provides an artifact that all stakeholders can refer to and refine throughout the product lifecycle.

Security issues must now be carefully considered at every phase of product development—from design and testing to delivery and maintenance—to combat complex and rapidly growing threats. This means that a combination of simulated in-house testing and third-party testing is important to exposure to a wide variety of growing threats as well as cover new vulnerabilities including device failures, takeovers, and stolen credentials.

In order to appropriately secure a system, the project team must consider what is most important to each level of operation. This includes what is needed to secure the individual devices, the communications between devices, the network, and the systems that the devices connect to. This means that updates and maintenance are part of the essential picture in providing a secure system for a long period of time. Devices must be designed and maintained to continually protect critical infrastructure sectors, such as manufacturing, energy, transportation, medical, and defense.

Wind River's position is that we understand no one has infinite time or infinite money to secure a system. With this in mind, we take a systematic approach in securing the device.
Because the cost of a cybersecurity breach is high. According to Cybercrime magazine, it is estimated that cybercrime damage will hit $6 trillion annually by 2021. In many sectors of IoT and embedded systems, including commercial markets like medical, industrial, infrastructure, and military, devices perform functions considered mission-critical where the cost of a breach goes well beyond the loss of data, IP theft, and damage to a company's brand. It can result in a catastrophic event or loss of life.

As discussed, when covering the survey mentioned in this white paper, establishing a device security policy is the first step. Regardless of the market, there is an industry standard model that guides the development of a security policy called the confidentiality, integrity, and availability (CIA) triad. This triad defines the principles needed to protect a device from unauthorized access, use, disclosure, disruption, modification, or destruction.

Confidentiality implementations protect the privacy of embedded systems data in motion, data at rest or stored on the device, data being processed by the device, and data passing to and from the device.

Integrity implementations assure that the embedded device data has not been modified or deleted by an attacker, including data being generated or consumed by the embedded device as well as its programming data (the operation system, applications, configurations data, etc). Availability implementations make sure an embedded device performs its intended function—an attacker cannot change a device's intended functional purpose—particularly devices that perform life- or mission-critical tasks.

Since Wind River recognized there is no single silver-bullet solution for protecting a device or system from all possible attacks, they recommend a layering approach that uses different mitigation controls to deliver a multifaceted protection shield and, ultimately, a much stronger cybersecurity implementation. This concept of defense in depth, which originates from the US Military, states that multiple security implementations are to be used in defending against an attack. These layered defenses must then be built on a trusted foundation that allows the flexibility to add new protection throughout the lifecycle of deployment and new security threats that are constantly emerging.

One approach gaining traction is Development, Security, and Operations (DevSecOps), which allows a software development team to introduce security features earlier in the development lifecycle and embeds security in all parts of the development process to minimize vulnerabilities. To handle the quantity of cyber-attacks, it is possible to simulate entire systems of devices, the infrastructure they run in, and the applications that run on top of them. System simulation is an efficient and effective means of researching, analyzing, and testing a wide variety of attack methods and security countermeasures, and allows developers to inject faults and vulnerabilities into their designs to see what would happen before the actual product deploys.

Cybersecurity is an ongoing effort for the life of the product. Once a product is deployed in the field threats must be constantly monitored and mitigated during deployment. How a company monitors and mitigates cybersecurity threats should be defined in the security policy before a project is even started.

I SECURITY EXPERTISE AND PRODUCTS FROM WIND RIVER

Wind River® provides secure, safe, and highly reliable embedded software solutions consisting of software, services, support, and experience. The company's runtime platforms are designed to serve as the trusted foundation for developers to innovate securely and protect their devices and systems against current and future threats. Additional software offerings provide hardening and automated threat simulation.

Wind River VxWorks®, Wind River Linux, and Wind River Helix™ Virtualization platforms provide a trusted foundation from which to build embedded devices of all kinds. These proven software platforms include a rich set of security capabilities for implementing components of the CIA Triad and secure processes based on industry standards.

- VxWorks, when compared to other operating systems, has the fewest known CVEs in its kernel. In addition, the VxWorks engineering team proactively monitors all CVEs from third-party open source components to minimize the attack surface.
- Wind River Linux includes more than 250 security packages in its distribution, each one tested and validated by the company's team of engineers. In addition, the Wind River Linux engineering team proactively monitors all CVEs and alerts customers to priority vulnerabilities.
- Wind River Helix Virtualization Platform provides strong partitioning to enable both a safe and secure system by leveraging the security capabilities of both VxWorks and Wind River Linux in a partitioned system.

Wind River offers operating system hardening and anti-tampering capabilities to fortify devices deployed in the field. These added security capabilities help maintain the integrity and confidentiality of critical data and configurations while assuring continued operations.

Wind River Simics enables device developers to automate fault testing and simulate threat scenarios. Developers can use Simics to inject faults into devices and systems to determine the impact before and during deployments.

Professional service and support matters. With a team that has over 35 years of providing security solutions, the company provides world-class professional services to the embedded industry that spans all vertical market segments. Company experts provide security assessments, offering a strong resource to support any embedded project—including top secret security conversations with U.S. Department of Defense customers. The company provides a number of online education and development training courses to keep customers up to speed on the latest technologies.

WIND™

[1] https://www.identityforce.com/blog/2020-data-breaches

[2] https://techcrunch.com/2019/08/01/hexane-oil-gas-telecoms-hackers/

[3] https://www.uscybersecurity.net/risks-2019/

[4] https://ciso.economictimes.indiatimes.com/news/375-new-cyber-threats-per-minute-seen-in-q1-globally-mcafee/77119240