0-100 MPH Journey to Cybersecurity Peace of Mind

cipher
a PROSEGUR company

Contents

The Importance of Cybersecurity for Organizations

The journey of a million miles starts with a single step. Or in the case of this analogy, a press of the gas pedal. The journey to a thorough, efficient, and effective cybersecurity posture also must begin somewhere. We will cover the stages that a cybersecurity leader within an organization goes through in order to achieve world-class cyber strength and resilience.

Each of these steps can be accomplished with an internal team or using an outside partner like a Managed Security Services Provider (MSSP). An internal team requires money, employee skills, and time. That is why many organizations outsource some or all of these activities to an MSSP. Regardless of the team composition, an organization goes through a process to become secure. The cybersecurity leader of the organizations drives the team towards the goal of cybersecurity peace of mind.

0 MPH | The Starting Line

There are many situations where an IT or cybersecurity leader at an organization might begin the quest to improve their cybersecurity.

A newly formed companies needs to build a strong foundation for information security. A company is likely focused on the development of their good or service to start. Then marketing, sales, and customer service come into play. That being said, cybersecurity should not be overlooked. A lapse in cybersecurity could negatively impact all elements of a company. Starting a company with a security-conscious culture lessens this risk.

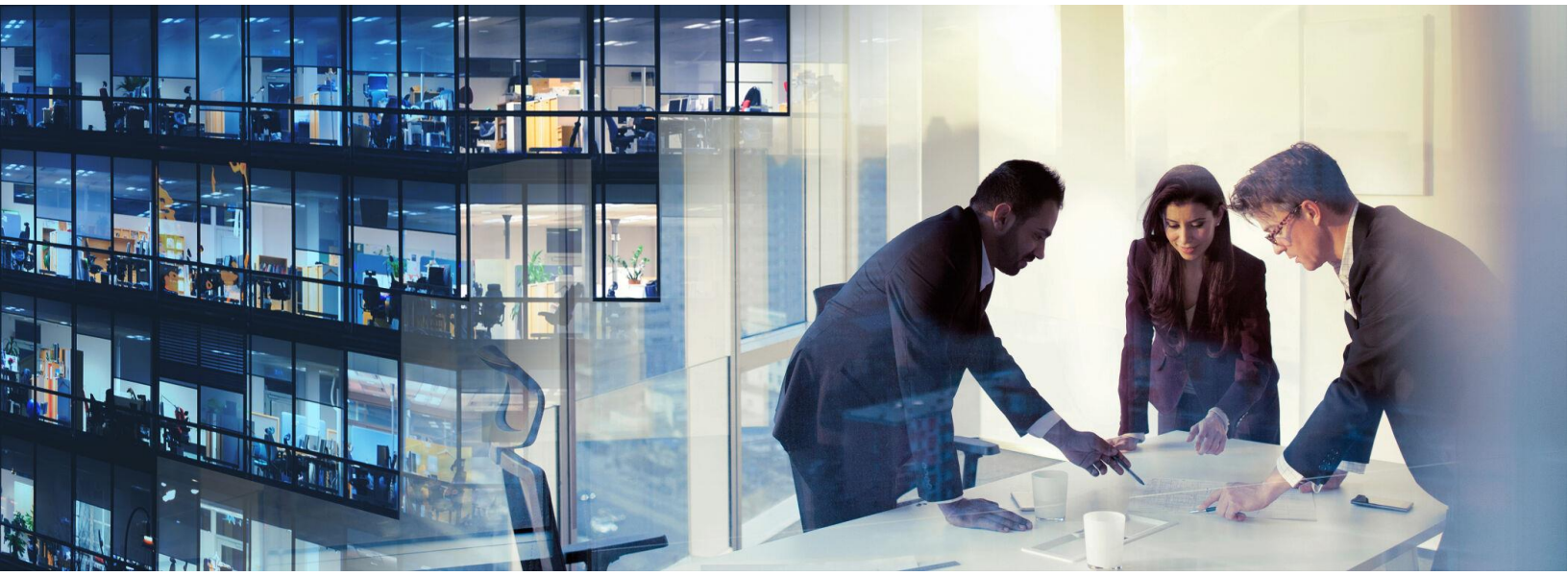
Companies that have been in existence for longer might also be at the starting line when it comes to cybersecurity. Then one day the need for improved security becomes apparent. One type of unfortunate event that is the motivator for many cybersecurity journeys is an cyberattack incident. This could be a data breach, ransomware, business email compromise, or another harmful event.

Other reasons that a cybersecurity or IT leader will choose to taking cybersecurity more seriously include:

- Person has a new awareness from a current event or news story that focuses on cybersecurity threat
- Company has requirements from 3rd party customers or partners they need to satisfy
- Person has realized the internal resources of company are not sufficient for task
- Regular compliance or certification cycle has come, and the person is looking for outside help
- Person is new in role and change up vendors
- Person is not satisfied with current vendor
- There is a new technology product and the person need to test before launching
- The internal dynamic changes of company have changed, and the person needs to find solution

Regardless of the scenario, admitting that there is a problem that needs to be addressed is the first step in getting off the finish line. Committing to a culture of security-by-design is vital.

30 MPH | Know Where You Stand



You cannot arrive at a destination unless you know where you are. Frameworks and regulatory guidelines will shape the process at this stage. Different industries have unique regulations. Many of the requirements or controls involved are the same between them.

The National Institute of Standards and Technology (NIST) Cybersecurity framework is a popular standard to use in order to measure your company against. According to NIST, the framework is "voluntary guidance, based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk."

Areas include guidance around five key areas: Identify, Protect, Detect, Respond, and Recover.

Companies that do business with the Department of Defense need to adhere to the Cybersecurity Maturity Model Certification (CMMC). This structure relates the type of information the contractor handles. Companies handling non-sensitive information are

at Level 1, and they require basic cyber hygiene. Companies handling secret information are at Level 5 and require organizations to have the ability to resist Advanced Persistent Threats (APTs).

You might be tempted to run the assessments and audits internally with Excel or other tools. This could work in the short-term or with a small environment. The best way to handle these assessments is to engage with an outside expert that document and track results and progress using modern methods.

After getting an assessment of your IT environment, metrics or key performance indicators are established to understand the situation. Important metrics to put in place include:

- Mean-Time-to-Detect and Mean-Time-to-Respond
- Number of systems with known vulnerabilities
- Unidentified devices on internal networks
- Security Incidents
- Number of patches required

Now that you understand where you stand, you can accelerate to improve by investing in core cybersecurity tools and establishing processes.

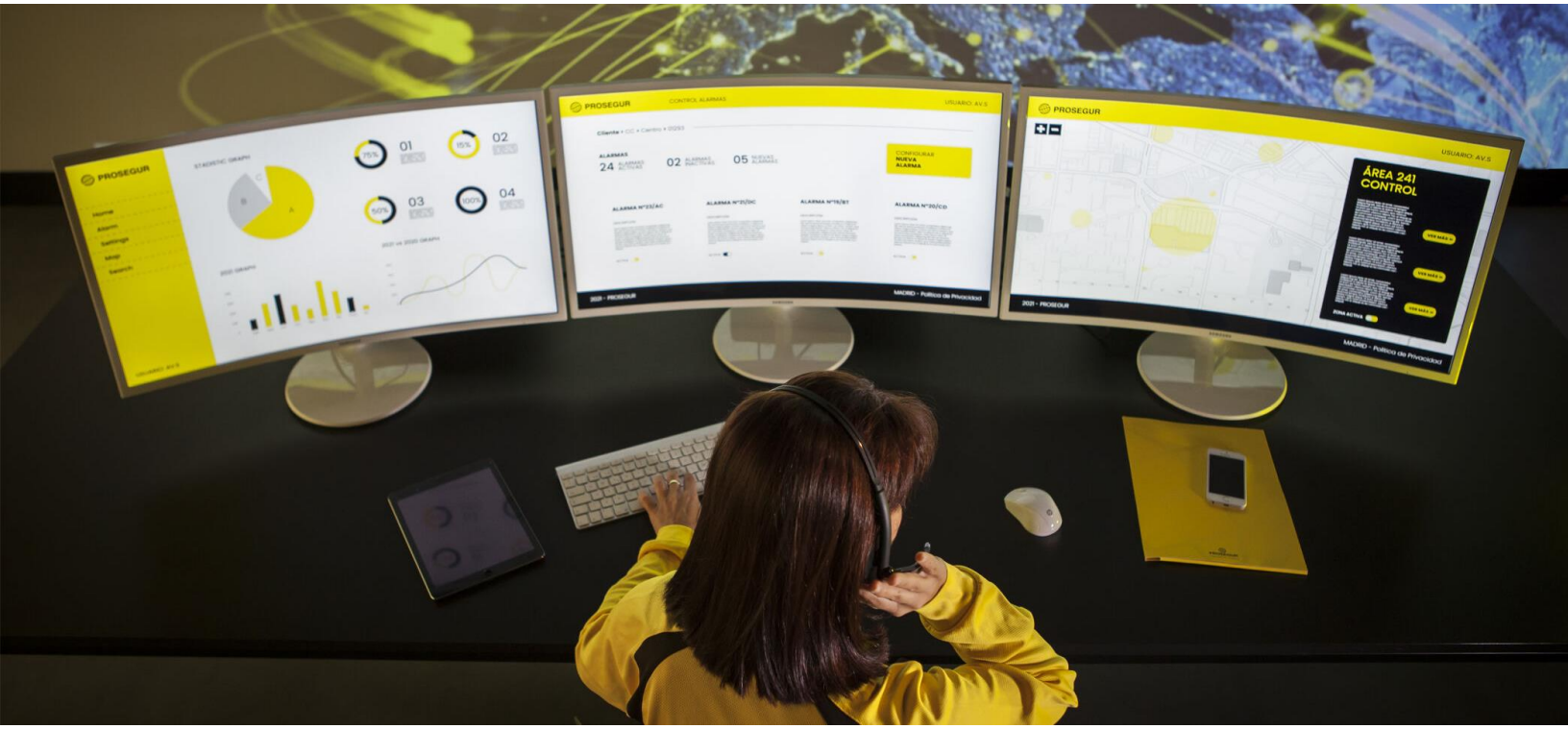
45 MPH | Raise the Defenses

After identifying gaps, you need to fill the gaps with tools and policies to address them. Firewalls, antivirus, and endpoint protection are foundational elements to achieve a layered cybersecurity posture. The solutions solve specific issues. An Endpoint Detection and Response (EDR) tool can protect devices from malware. A firewall stops people outside of your network from getting access.

Processes are just as important as the different tools that can be brought to bear. Train employees on signs of phishing emails and other best practices. Ensure user access rights are appropriate. Backup data regularly to lessen the impact of data compromise.

Software vulnerabilities are a huge vector for threat actors to attack. Ensure patches to vulnerabilities are installed and monitored. Doing this in a systematic and comprehensive way can be done using management software tools.

60 MPH | Gain Visibility

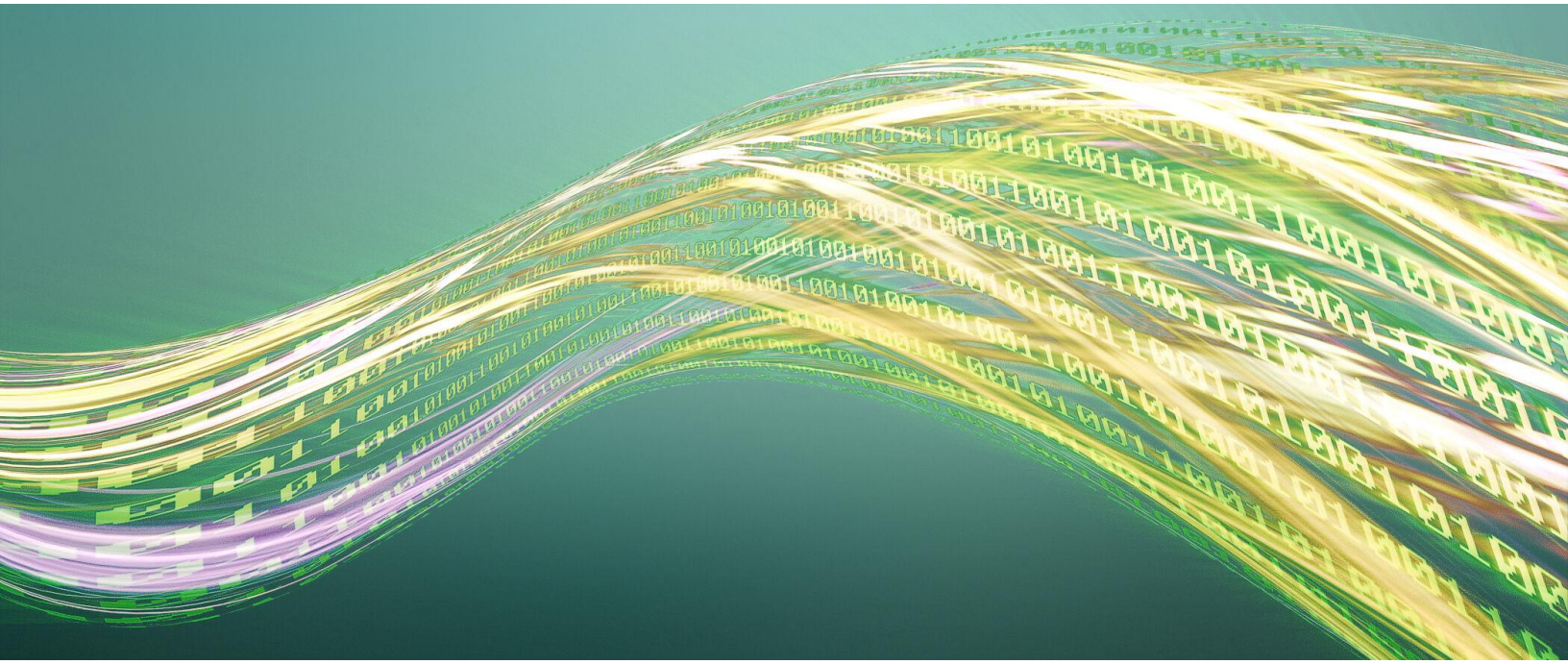


It takes different types of software and systems to secure an enterprise. Having all these tools running in silos and different areas creates complexity. Analysts scrambling from one program to another is not efficient. Using a Security Incident Event Management (SIEM) system can give the company visibility.

The cybersecurity leader can now link events across different software and systems to get a full picture of what is happening. Alerts from these disparate tools can be evaluated by cybersecurity experts. These alerts and insights increase the ability to detect and investigate incidents.

Alerts and triage related to the SIEM should be monitored on a 24x7 basis in a Security Operations Center (SOC) for full protection. Again, this can be done internally with staff employed by your company or outsourced to an MSSP.

100 MPH | Get Proactive and Forward Thinking



New innovations come every day in the world of cybersecurity. Advanced platforms and other innovative technology to stop attacks. If you start using a cutting-edge tool before the foundation is in place there could be disaster. That is why innovating and trying the new things comes after we are up-to-speed with the other areas.

Adversary Emulation platforms can simulate what would happen if your company is breached. User and Entity Behavior Analysis (UEBA) platforms take analytics from activity and analyzes them using unique algorithms to measure insider risk.

Machine learning and artificial intelligence can help improve alert prioritization in a SIEM platform. Machine learning algorithms look for patterns through the large volume of log data to help the analyst quickly identify indicators of compromise. AI improves the accuracy of SIEM correlation rules and events. Not to mention, a security analyst can use AI to investigate more sophisticated and complex attacks to fill in the gaps.

References

https://www.acq.osd.mil/cmmc/

https://www.nist.gov/cyberframework

https://www.fcc.gov/general/cybersecurity-small-business

https://cipher.com/blog/10-cybersecurity-metrics-you-should-be-monitoring/