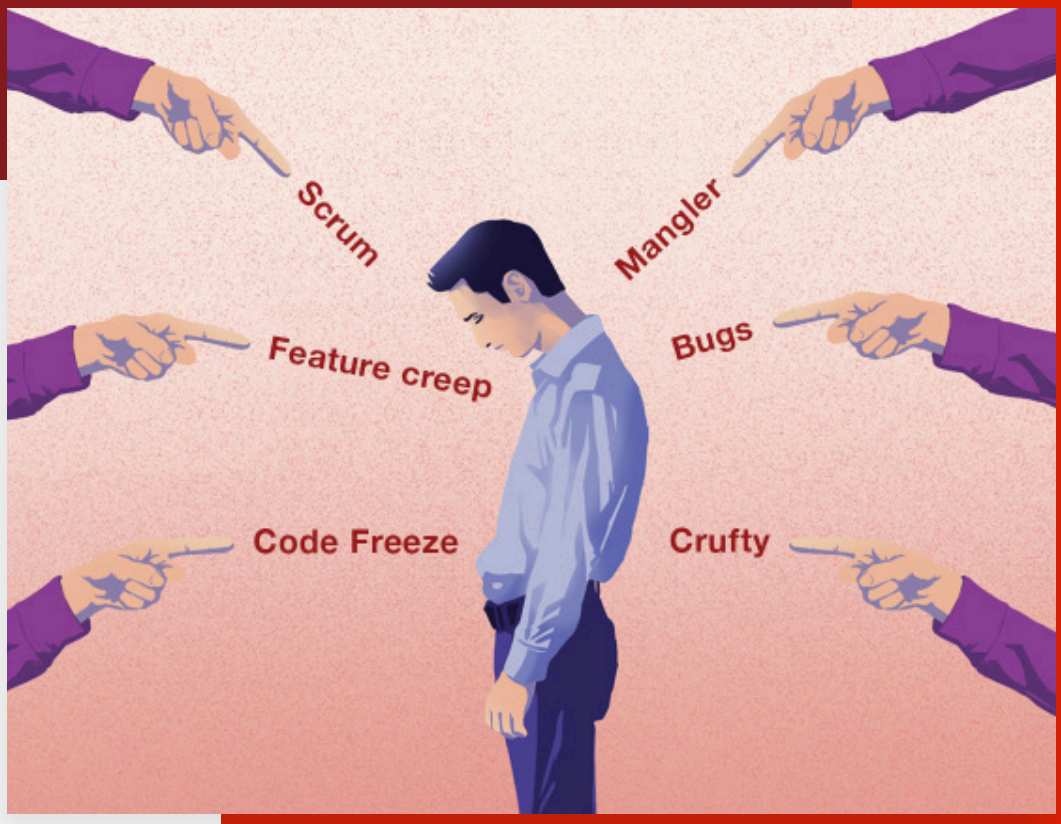
GRAMMATECH

# From Coding Scapegoat to Coding GOAT




SOFTWARE CYBER SECURITY BEST PRACTICES FOR CODERS

Coding has been around since the dawn of human communication. With the ability to communicate important information, came the need to protect it from getting into the wrong hands. The history of transmitting information through language – and the lengths people have gone to protect it from being exploited – goes back further than you may think.

Case in point: Julius Caesar. Roman General, Cleopatra's lover, and the OG of coding. Caesar developed cipher code as a way to protect classified messages sent to military personnel. By replacing each letter with a shift of three, this secret code prevented enemies (and frenemies) from reading classified information. The Caesar Cipher is an iconic example of early-day encryption, which is now practically useless in terms of security.

Vulnerabilities and threats continue to grow both internally and externally. They're bigger and badder than ever before – and the stakes are higher, too.

COVID-19 has accelerated the constant struggle between cybersecurity and threats. The pandemic turned the world upside in ways that many of us didn't think possible before March of 2020. It has caused hundreds of millions of office workers to suddenly become teleworkers, bringing their technology and security vulnerabilities to their homes. COVID-19 has led to what some are calling a cyber pandemic, in which cyber threats have gone through the proverbial roof.[1]

Something as simple as an unintentional error in code – perhaps caused by pressure to get to market or just COVID fatigue, can have devastating consequences for you and your company.

Vulnerabilities and threats create massive financial and legal liabilities – they also have

[1] Lohrmann, Dan. "2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic." Government Technology State & Local Articles - e.Republic. Government Technology, December 12, 2020. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

the potential to severely impact human lives. Just think about how many TV shows or movies you have seen that depict a story about a compromised system that leads to catastrophic effects.

Then there are the real-life scenarios. Security flaws found in anesthesia machines that could be used to make remote and unauthorized adjustments to people's oxygen levels, the notorious Equifax breach that affected over 145 million customers, the Heartbleed bug that was deemed one of the worst security vulnerabilities to exist. Also, who can forget Wikileaks – the biggest classified data breach in history.

Hackers find opportunities everywhere. Having already gone after the low-hanging fruit with phishing, web exploits, network intrusion, and other means, they have now turned their sites on you – the developer. They want to hack into your code to damage you, your company, and your customers! Hackers are constantly looking to exploit even the most guarded systems.

**As a result, cybercrimes are rising and are estimated to cost unsuspecting organizations as much as $6 trillion globally in 2021 and up to $10.5 trillion globally by 2025.**[2]

We want to equip you with the tools to fight back against them.

From CEOs to legal teams to entire organizations, it's no surprise that security is on everyone's mind. According to IBM's C-suite Series: The 2021 CEO Study,

**72% of customer-focused outperforming organizations identify protecting against cybersecurity risks as a top-three priority.**[3]

The pressure is on for developers to consistently create error-free code. For developers, the increase in cyberattacks, and the need for smarter and faster defense, means bigger and broader job responsibilities, new challenges, and more risk. It means that developers are on the hook as potential scapegoats for any errors in their code.

**When it comes to cybersecurity, you and your team are the first and best line of defense against threats and internal issues – and the best defense is a solid offense.**

Your offense needs to be focused on writing safe and secure high-quality code that puts your company, and you, on top.

[2] Morgan, Lisa. "5 Ways Static Code Analysis Can Save You." SD Times, September 4, 2018. https://sdtimes.com/test/5-ways-static-code-analysis-can-save-you/.

[3] Foster, Mark, Jesus Mantas, and Peter Korsten. "2021 CEO Study -- Find Your ESSENTIAL: How to Thrive in A Post-Pandemic REALITY," February 2021. https://www.ibm.com/thought-leadership/institute-business-value/report/ceo#.

The pressure to deliver is high, and there are always going to be internal barriers – this doesn't have to be a bad thing. This is the time for developers to shine and confront the fear of scapegoatism. Developers have the opportunity to educate themselves and their teams on the problems they face (both internally and externally), impending security threats, and the cost of errors. They also have the opportunity to use powerful tools to mitigate their risks, escaping the coding scapegoat, so that they can find potential errors before they become exploited vulnerabilities.

**Early testing is your friend and ally in this fight against cybercrime. This will also help protect your code.**

Better security means a smoother workflow, more time for projects, and less agony over delivering flawed code that could cost millions to fix.

According to the U.S. Bureau of Labor Statistics, there are over 1.4 million coding jobs in the U.S. alone[4] – making it one of the fastest-growing occupations in the country. Not to mention, there seems to be a coding boot camp being promoted every other second. Developers have a chance to stand-out among the pack and become lead defenders in the rapidly growing cybersecurity space.

This eBook will arm you with the right tools and education to take control, become a cyber Macgyver, and "Go From Coding Scapegoat To Coding GOAT."

## Coding GOAT Tip

Learning is Forever: Keeping up to date is a life-long process for coders. New knowledge helps you stay relevant in a dynamic landscape, no matter where your career takes you.

[4] "Software Developers: Occupational Outlook Handbook." U.S. Bureau of Labor Statistics, September 1, 2020. https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm.

## NEVER FEAR, STATIC ANALYSIS IS HERE

Code errors and defects happen – it's simply part of the process. Left unresolved, these defects lead to vulnerabilities that could have drastic consequences, costing millions – like the lofty average cost of **$3.86 million per breach in 2020**[5] – and ruining reputations.

According to *Forrester's State of Application Security, 2020* report, software vulnerabilities are and continue to be the leading method for an external attack.[6] It's more important than ever to have the proper testing and defenses put in place so that your code doesn't become an exploited vulnerability – and so that you don't become the scapegoat. Don't let fear, uncertainty, or doubt keep you from achieving coding greatness.

Like any sport, it's important to focus on the fundamentals. When it comes to testing, there are two basic ways to go about testing – **static and dynamic analysis testing**.

The best way to defend against the costs of code defects is to catch these as early as possible. That's where static analysis comes in – examining code before program execution and catching these errors before they become costly problems. This form of testing minimizes or gets rid of the possibility of exploitation and can find errors that dynamic testing may not down the road.

Static testing finds errors in the early stages of development, whereas dynamic testing is performed in the later stages to catch errors. Used in tandem and correctly, these two forms of testing can make a powerful defense.

For this eBook, we'll be focusing on the power of static analysis testing.

[5] "2020 Cost of a Data Breach Study." IBM Security, June 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

[6] Carielli, Sandy, and DeMartine Amy. The State Of Application Security, 2020. Forrester, May 4, 2020. https://www.forrester.com/report/The+State+Of+Application+Security+2020/-/E-RES159057#.

**This form of testing minimizes or gets rid of the possibility of exploitation and can find errors that dynamic testing may not down the road.**

Static analysis can be done manually – or it can be automated, which drastically cuts down on time and human error. An automated analysis brings some important benefits to your development process. It efficiently works through millions of lines of code, detecting hard-to-see errors and security vulnerabilities, all while reducing efforts for your team.[7]

There is one thing that hasn't changed over the centuries – and that is change itself.

**As the ancient Greek philosopher, Heraclitus said, "change is the only constant in life." Heraclitus was right, and being in the digital and information age means that things are changing faster than ever before.**

This is especially true in the cybersecurity space, where new threats are occurring every second, from around the world.

[7] Graham, Bill. Enhancing Code Reviews with Static Analysis. GrammaTech. https://blogs.grammatech.com/enhancing-code-reviews-with-static-analysis.

Static analysis helps you prepare for the inevitable change. It puts in place standard operating procedures (SOPs) that advance best practices for your company and help protect your code. Static analysis tools are constantly updating, meaning that you are evolving along with any threats. These static analysis SOPs also allow developers, across career stages, to work on the same assumptions and guidelines and advance their careers.[8]

## Coding GOAT Tip

Break Your Own Code: Finding defects or bugs before others do will bring you one step closer to delivering error-free work.

## THE SHIFT LEFT MOVEMENT – GETTING IT RIGHT

The term “Shift Left” was originally coined by Larry Smith in 2001 and goes hand-in-hand with the mantra, “test early and often”.

**By Shifting Left, there is an added emphasis on code quality at the earliest stages, putting a spotlight on developers and their work.**

This Shift Left Movement illustrated the need for static testing and why it became more important than ever before. This Shift led to baking-in information security from the start and carrying that focus throughout the entire development lifecycle.

Some companies, like GrammaTech, were early enablers of the Shift Left Movement and have a dedicated focus on safety and security. This dedicated focus allows you and your team to find flaws and issues in code more easily and to lower your risk (moving further away from scapegoat status).

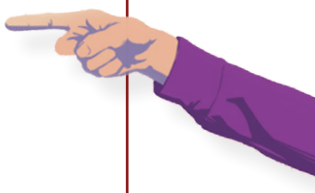
Shifting Left has many benefits. It empowers you and your team to focus more on your current and future projects and less on worrying about errors in code. It also carries beefits for the coder – allowing developers to perfect their craft, advance their career, have more control over their code, and even become better team players.

So naturally, the next question is, “how do we implement and execute a Shift Left?”. The answer is to transform DevOps into DevSecOps.

[8] Kunchala, Vikram, Michelle Shuttleworth, Kieran Norton, and Dylan Hack. “DevSecOps and the Cyber Imperative.” Deloitte Insights. Deloitte, January 16, 2019. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/embedding-security-devops-pipelines-devsecops.html.

## Coding GOAT Tip

Find Your flow: Go too slow or too fast never works. Stay organized, create proper code documentation, and focus on reducing friction in your environment and process.





So, what is a DevSecOps culture? Plainly stated, this is an integrated culture between Development, Security, and Operations – this is a security-focused culture of Shifting Left and is an evolution of DevOps.[9]

In DevSecOps, security is baked-in from the beginning and continued throughout the entire lifecycle, with many security processes being automated and handled by the development team. For example, in DevSecOps, security testing and fixing issues that arise are all handled by the development team.[10]

The benefits gained from bridging the gap between DevOps and security are tangible.

**This inclusive culture allows companies and teams to respond faster, improve workflows, increase transparency and trust, better accomplish shared goals, knock down the overstated silos, and ultimately be more successful. Who doesn't want that?**

The ability to respond to threats quickly, or to prevent them before they happen, has become even more important in today's pandemic reality. Cybercrime is on the rise and many companies and organizations are working remotely. Evolving your culture from DevOps to DevSecOps can help give you the tools and ability to successfully navigate the sea of threats.

[9] Kunchala, Vikram, Michelle Shuttleworth, Kieran Norton, and Dylan Hack. "DevSecOps and the Cyber Imperative." Deloitte Insights. Deloitte, January 16, 2019. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/embedding-security-devops-pipelines-devsecops.html.

[10] Constantin, Lucian. "What Is DevSecOps? Why It's Hard to Do Well." CSO, July 23, 2020. https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html.

Before going through the culture change journey, it's important to remember and reinforce that change takes time and is not easy – especially when it comes to company culture. It will take everyone on the boat rowing in the same direction to effectively change your culture.

Along the way, there will be resistance, frustration, bad decision-making, and fear. Some in your company may leave or decide that they are looking for something else. DevSecOps requires breaking down the silos between two parts of your company that may have a bit of friction with one another.

**Developers are not suddenly security experts once a DevSecOps culture is decided upon – everyone is now responsible for security[11] and it'll take time to build that skill set.[9]**

This all is to be expected when culture change occurs and it doesn't mean that it's any less worthwhile.

So how do you establish a DevSecOps culture? This depends upon your business – as every company is different. Start with the end in mind. What do you want your culture to look and feel like? How do you want your teams to work together?

**In a DevSecOps organization, security permeates through every part of it. Think of duties, responsibilities, and processes that need to be implemented or updated to achieve this. Create a clearly defined "DevSecOps Roadmap" for your company, so that everyone knows what you are looking to build and how you are all going to work together to create it – from your trusty company lifers to your entry-level new hires.**

Focus on the fundamentals of change management – the DICE factors – Duration, Integrity, Commitment, and Effort. These four key factors were derived from a study by Harvard Business Review and have been used by organizations for over a decade and a half.[12]

[11] Anderson, Erica. "How to Build an Effective DevSecOps Culture." The GitHub Blog. GitHub. https://github.blog/2020-04-28-how-to-build-an-effective-devsecops-culture/.

**1. Duration**[12]

Duration matters, but in a different way to what you may initially think. According to Harvard Business Review, "Companies make the mistake of worrying mostly about the time it will take to implement change programs. They assume that the longer an initiative carries on, the more likely it is to fail…However, contrary to popular perception, our studies show that a long project that is reviewed frequently is more likely to succeed than a short project that isn't reviewed frequently. Thus, the time between reviews is more critical for success than a project's life span."[12]

**2. Integrity**[12]

It sounds cliché, but integrity is everything. This is especially true when companies think about their top performers and how they can help with changing culture. According to Harvard Business Review, "… since the success of change programs depends on the quality of teams, companies must free up the best staff while making sure that day-to-day operations don't falter. In companies that have succeeded in implementing change programs, we find that employees go the extra mile to ensure their day-to-day work gets done."[12]

**3. Commitment**[12]

A successful culture change will need a certain degree of commitment from all of those involved – especially from those at the top of the organization. According to Harvard Business Review, "Top-level commitment is vital to engendering commitment from those at the coal face. If employees don't see that the company's leadership is backing a project, they're unlikely to change. No amount of top-level support is too much… A rule of thumb: When you feel that you are talking up a change initiative at least three times more than you need to, your managers will feel that you are backing the transformation."[12]

**4. Effort**[12]

It will take additional effort on top of what employees and leaders already need to accomplish with day-to-day responsibilities to effectively change the culture. It's important to not add or change too much at once – there is a sweet spot to be found. According to Harvard Business Review, "When companies launch transformation efforts, they frequently don't realize, or know how to deal with the fact, that employees are already busy with their day-to-day responsibilities… Project teams must calculate how much work employees will have to do beyond their existing responsibilities to change over to new processes. Ideally, no one's workload should increase more than 10%. Go beyond that, and the initiative will probably run into trouble."[12]

## Coding GOAT Tip

A Stronger Team Means Stronger Code: Successful projects rely on teamwork, even if goals differ. Define team structures, delegate tasks and make sure you're communicating as soon as a challenge arises.

[12] Sirkin, Harold L., Perry Keenan, and Alan Jackson. "The Hard Side of Change Management." Harvard Business Review, October 2005. https://hbr.org/2005/10/the-hard-side-of-change-management.

## KNOW THY ENEMY TO PROTECT THYSELF

To stand out and become a Coding GOAT, you must first understand the questions and challenges in front of you.

2020 has shown a huge uptick in cyber threats, especially ransomware. There are hundreds of security vulnerabilities, and they each have a way of causing serious damage to your code and workflow. If you know what's lurking out there, and what is about to emerge, you have a better chance of spotting it and fixing it before it turns into a serious liability.

**In the wise words of the Chinese general and philosopher Sun Tzu, "if you know the enemy and know yourself, you need not fear the result of a hundred battles."**

Before we get into emerging security threats, let's do a quick review of some of the top security risks plaguing companies (and their teams) and how to mitigate them. Here's a refresher of the top OWASP security risks (with a focus on the first five).[13]

**1. Injection: Stop Cyber Attacks Slipping Through Form Submissions**[13]
Injection flaws allow attackers to inject untrustworthy code into an application, using things like insecure form submissions, which can cause the application to go rogue and execute unintended commands. For example, SQL injection attacks were employed during the Heartland Payment Systems Data Breach, resulting in over 134 million credit cards being exposed.[14]

To prevent this, OWASP recommends using a safe API (avoids the interpreter or provides a parameterized interface), positive or "whitelist" server-side input validation, and escaping special characters using specific escape syntax for that interpreter.[13]

**2. Broken Authentication: Bulk-Up Authentication and Protect Your Passwords**[13]
Broken Authentication occurs when web application authentication systems are exploited (like passwords) – meaning access to user and admin accounts. Attackers used this method to hack the South Carolina Department of Revenue in 2012, exposing 3.6 million social security numbers – it was also used in 2015 to attack the IRS and expose the personal information of over 700,000 people.[15]

To prevent this, OWASP recommends tactics like implement-

[13] OWASP Top Ten. OWASP, 2017. https://owasp.org/www-project-top-ten/2017/.

[14] Ritchey, Diane. "Data Breach Directions: What to Do After an Attack." Cyber Security News. Security Magazine, February 1, 2015. https://www.securitymagazine.com/articles/86071-data-breach-directions-what-to-do-after-an-attack.

ing multi-factor authentication, avoiding shipping or deploying with any default credentials, and implementing password best practices.[13]

**3. Sensitive Data Exposure: Guard Your Sensitive Data**[13]
If you don't have buffed-up security for sensitive data, hackers can modify it and use it for their own purposes. One real-life example of this is the 2013 Target store data breach that exposed payment and contact information for about 40 million and 70 million customers respectively.[16]

To prevent this, OWASP recommends tactics like classifying application data, applying controls for the classification, and proper data controls.[13]

**4. XML External Entities: Arm Yourself Against Web Security Vulnerabilities**[13]
Attackers can attack XML processors by uploading XML and exploiting vulnerable code. Examples of this include internal file share exploits, remote code execution, and Denial of Service (DoS) attacks (i.e., Billion Laughs Attack[17]). A proof-of-concept attack even illustrated how a user could inject malicious code into shared online repositories and obtain files available on the device reading the code.[18]
To prevent this, OWASP recommends tactics like using simpler data formats, patching or upgrading all XML processors, and implementing positive "whitelisting" server-side input validation.[13]

**5. Broken Access Control: Put Broken Access Control Back Together Again**[13]
Broken Access Control allows attackers to bypass authorization and execute tasks as if they had admin rights and privileges – gaining access to all sensitive data and info. One real-life example of this is January 2014's Snapchat brute force enumeration, which revealed 4.6 million usernames and phone numbers.[18]

To prevent this, OWASP recommends tactics like denying by default, implementing access control mechanisms, and enforcing record ownership.

The last five remaining OWASP vulnerabilities include Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, and Insufficient Logging and Monitoring.[13]

## Coding GOAT Tip

Kill Your Darlings: Don't get too emotionally attached to your code. A technical approach will make you hyper aware of blind spots, and benefit you in the long run.

[15] Sukianto, Axel. "Real Life Examples of Web Vulnerabilities (OWASP Top 10)." Cyber Threats. Horangi Cyber Security, June 19, 2020. https://www.horangi.com/blog/real-life-examples-of-web-vulnerabilities.

[16] Abrams, Rachel. "Target to Pay $18.5 Million to 47 States in Security Breach Settlement." The New York Times. The New York Times, May 23, 2017. https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

# THREATS DU JOUR

After having a refresher on some of the top threats, let's now dive into what is emerging. This is 2021, new threats emerge at breakneck speed. Cyber threats have increased and evolved (mutating like a virus) due to the COVID-19 pandemic. The need has never been greater to correctly respond to these threats and to do it quickly.

Booze Allen Hamilton compiled a report of Eight Cyber Threat Trends to Watch Out for in 2021[19], which is outlined below. Armed with this knowledge, you and your teams will be in a better position to defend against cyberattacks.

**1. Next-Generation Extortion and Evolution in Malware Business Models**[19]
2020 was a tumultuous and difficult year. Not only was the world dealing with a health crisis, it was also dealing with a cybercrime crisis – neither crisis ended on December 31st. Ransomware tactics became more prevalent and popular in 2020, especially from Maze and Sodinokibi operators.

Ransomware tactics are evolving to more than just holding data and systems hostage, operators are threatening to notify regulatory agencies and stock exchanges to force submission and higher payouts. There is the evolution of the Ransomware as a Service (RaaS) model, giving hackers and attackers the tools, platforms, and potentially even financing (from cybercriminal venture capital groups), for future ransomware attacks.[19]

So how do you protect yourself, your team, and your company from this new Bond criminal-like form of extortion? Take a page from the Greek stoics – confront and get ahead of the worst-case scenario. According to Booze Allen, focus on a patching policy for critical vulnerabilities and finding these before they can be exploited, implement security tactics like two-factor authentication, create an aggressive backup strategy with pre-defined playbooks that you can wargame out, and establish a hunting program for suspicious activity.[19]

[17] Morgenroth, Sven. "Application Level Denial of Service – A Comprehensive Guide." Netsparker. Netsparker, January 19, 2018. https://www.netsparker.com/blog/web-security/application-level-denial-service-guide/#BillionLaughsAttack.

[18] Sukianto, Axel. "Real Life Examples of Web Vulnerabilities (OWASP Top 10)." Cyber Threats. Horangi Cyber Security, June 19, 2020. https://www.horangi.com/blog/real-life-examples-of-web-vulnerabilities.

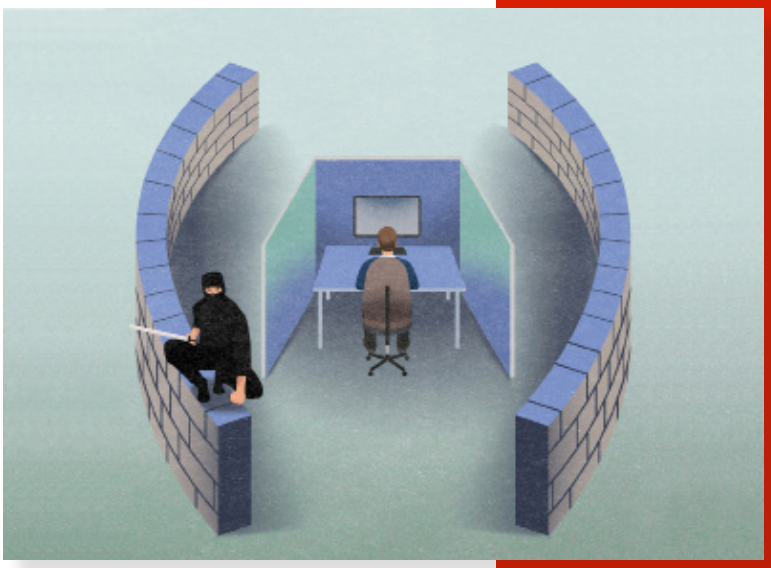
**2. Supply Chain Attacks via Cloud-Hosted Development Environments**[19]

There is the potential for cybercriminals to shift to attacking supply chains via PaaS cloud-based development environments. Cybercriminals will continue to evolve and hone their craft, using the cloud to insert malware into PaaS solutions. To add to this, many companies are undergoing digital transformations from in-house servers to IaaS hosting in a way that leaves them more vulnerable to these attacks.[19]

According to Booze Allen, protect your team and organization by deploying endpoint detection and response (EDR) tools that could help detect suspicious behavior, implement controls that limit applications to only trusted vendors, make use of code signing, and secure your development environments with strict access controls and patches.[19]

**3. AI, Evasion, and Theft**[19]

Highly-skilled cybercriminals are searching for ways to defeat AI-based security and use your machine learning against you. Malware developers have been busy using exponential polymorphic, or self-modifying, malware to try to get ahead of AI-based security solutions.



It's possible, and shown in a proof of concept, that hackers could use AI and machine learning to pass a disguised malicious file to an antivirus engine – essentially sneaking the malware past your system guards. This could result in economic espionage and property theft.

So how do you mitigate this type of threat? According to Booze Allen, organizations should implement a defense-in-depth (DiD) strategy that incorporates a variety of security methods that are layered upon one another, expect AI to be a target and build and train it to react to attacks, and assign certain mitigations to attack techniques for your AI.[19]

**4. Parcel and Shipping as Critical Infrastructure**[19]

If 2020 has shown us much of anything, it's the importance of reliable shipping services. We all want our online purchases to be delivered quickly and to the right place. We also need freezing cold COVID-19 vaccines, mass amounts of PPE, and other critical materials to reach every corner of the country and world – meaning that we need effective and efficient shipping infrastructure.

Cybercriminals, and even state-aligned threat actors, see this reliance on shipping companies – a vulnerability that can be exploited and used as leverage.

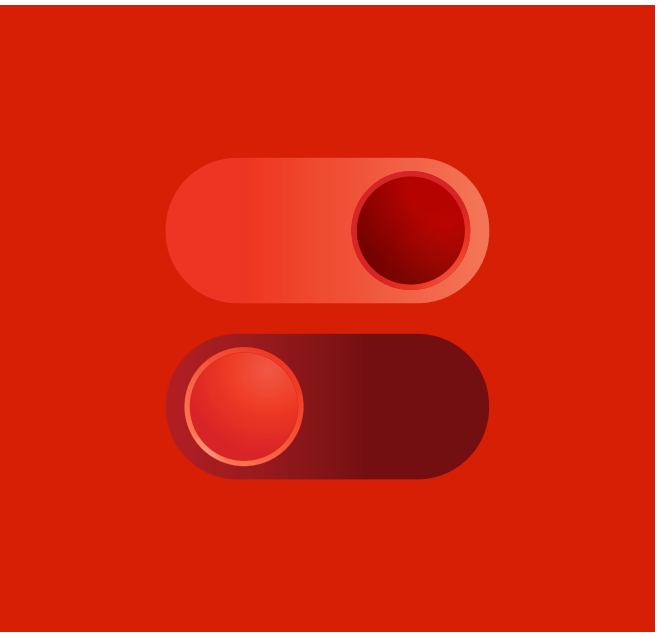
This could play out in many different ways – both on the consumer and business levels. Cybercriminals, and even state-aligned bad actors, could target the shipping sector with

[19] "8 Cyber Threat Trends to Watch Out for in 2021." Publication. Booz Allen Hamilton, 2020. https://www.boozallen.com/c/insight/publication/8-cyber-threat-trends-for-2021.html.

ransomware – which could cripple operations, delay or destroy potentially life-saving supplies, and cost billions in damages.

Non-shipping organizations have similar situations and risks. The pandemic has made many of us and or organizations wholly depend on digital infrastructures – much like how it has tethered us to reliable shipping. Think of how remote work would function without video conferencing, online collaboration, or even developer-specific tools like GitHub. Vulnerabilities or attacks on these tools, or even on your own systems and platforms, could cripple your company and others like it across the world.

How do we protect against this? According to Booze Allen, there are a few tactics that shipping organizations can take. Increase network monitoring around important periods of reliance on shipping companies (holidays, natural disasters, etc.), figure in the geopolitical environment, and educate the public and employees on what kinds of communications to expect.[19] These same types of common-sense mitigations can be taken for digital infrastructure and non-shipping companies.



**5. Mandated Contact Tracing Apps May Open Doors for Large-Scale Cyber Attacks**[19]

Contact tracing has become a household term during the COVID-19 pandemic. Governments and organizations around the country and world rely on tracing apps to track and isolate the spread of the virus.

These same apps that allow us to fight back against the COVID-19 pandemic could be used for large-scale cyberattacks. The apps were built quickly as a response to a deadly crisis without a large concern for security or privacy. This makes these apps vulnerable and open to espionage and criminal behavior. Criminals could create fake look-alike apps and blackmail users for a fee. Bad state-actors could target adversarial country apps, taking these programs down or even spreading disinformation.[19]

The burden falls on developers and the companies that created these tracing apps to ensure that they are safe and secure. According to Booze Allen, developers should test all facets of the app while looking into mobile device management (MDM) platforms and application containerization to centralize control and isolate applications or data.[19]

**6. Cybercriminals Will Likely Capitalize on Rapid U.S. Telehealth Adoption**[19]

COVID-19 largely expanded the use of telehealth, allowing people from around the country and world to see a doctor or nurse via a virtual appointment. Telehealth has increased healthcare access for many and has resulted in a lot more health data and vulnerabilities.

This could become of interest to cybercriminals looking to steal some of our most sensitive data, extort with ransomware attacks, and attack enterprise-grade systems to gain credentials.

According to Booze Allen, to defend against these outcomes, companies will have to implement refined telehealth services with cybersecurity at the forefront, evaluate their vendors' security controls and policies, implement stronger patient authentication measures and remote management for provider-used devices.[19]

**7. 5G to Expand the Attack Surface for Industrial IOT**[19]

5G is a powerful enabler of technology and progress. When it comes to industrial IoT, it's a double-edged sword. Many current industrial control systems use vulnerable legacy operating systems and depend on network segmentation to mitigate cyber risks.

The expansion of 5G allows for the industrial internet of things (IIOT) network to grow and expand, adding pressure to legacy systems and creating more vulnerabilities for cybercriminals to exploit. What was a closed system could become appealing for attackers to exploit and hold hostage.

The best defense is a good offense. According to Booze Allen, organizations need to upgrade their infrastructure and devices, plan their 5G network architecture, bake security into the entire process with vendors, and plan a security strategy.[19]

**8. 5G to Increase Security Pressure on Mobile Hotspots**[19]

5G is also a game-changer on a non-industrial level. Everyday lives will be changed by 5G, with more access to much faster internet. With more availability and access, comes more vulnerabilities and unwanted attention from hackers.

By having such fast mobile internet at our fingertips, consumers and businesses may opt for 5G modems and hotspots instead of the traditional internet connections – making for larger use of less secure technology. An attacker could seize control of mobile devices or even modems.[19]

Developers can have a direct effect on mitigating the worst outcomes. According to Booze Allen, organizations can prepare for attacks by monitoring trends to find vulnerabilities, bake-in security into 5G adoption, and follow security best practices. Using Shift Left methods and early testing with an increased focus on security will help make for more secure technology.[19]

## Coding GOAT Tip

You're only human: You might work with machines, but you aren't one. To avoid burnout (and bad code), make sure you're getting enough sleep, take breaks, and find a good chair, too.

## BECOMING A CODING GOAT WITH GRAMMATECH'S CODESONAR

You need the right tools to understand potential threats in your code and change your security culture – the stakes are simply too high not to.

Coding and dealing with cyber threats are like playing a very twisted game of dodgeball. Your objective is to eliminate players from the other team by using your best defense and offense – throwing balls before they are thrown at you, and blocking them to stay in the game. But in this version of dodgeball, instead of winning, the opposing team's members keep increasing. Not only that, their methods to bring you down continue to advance and evolve.

You need to figure out how to dodge the barrage of balls being thrown and beat your opponents at their own game – the same way you need to stop the growing swarm of hackers from exploiting vulnerabilities in your code before they even think of launching an attack.

That's where GrammaTech's CodeSonar comes in.

**CodeSonar is like the MVP on your team that knows the best defense is a great offense. It's a deep, detailed Static Application Security Testing tool that will help root-out fast-moving threats before they've even had a chance to ruin the game plan.**

GrammaTech has been an industry leader for over 15 years and our solutions are used by some of the largest and highest-risk industries like defense, aerospace, medical, industrial control, electronic, telecom/datacom, and transportation. Companies use tools like CodeSonar for products and services that we see in everyday life, including cruise control and home security systems.

With CodeSonar, your team actively Shifts Left with an enhanced focus on safety and security via automated static analysis testing – a real game-changer for many companies. Automated testing is on the rise, yet it is still a challenge for most – with only 14-18% of test activities being automated.[20]

The simple fact is that for many companies, their teams lack the necessary skills or bandwidth to implement testing. You need to be able to deploy test environments reliably and predictably while ensuring your data complies with regulations.

[20] Buenen, Mark, Ajay Walgude, Rahul Mitra, and Jayant Kumar. "Capgemini: World Quality Report 2018-19." Capgemini Worldwide, 2018. https://www.capgemini.com/service/world-quality-report-2018-19/.

**CodeSonar was made for developers and utilizes a mathematical foundation as well as a developer-friendly interface.**

CodeSonar helps protect your code. With our SAST tool, you can create complete security for your teams with the deepest and most detailed static analysis. CodeSonar employs a unified dataflow and symbolic execution analysis that examines the entire application – finding 3-5 times more defects, on average, than other static analysis tools.

CodeSonar is scalable, allowing for quick scans on subsets of code, and can be used for four of the top five programming languages (C/C++, Java, C#, Binary). The tool is designed to support large teams and can easily integrate into your team's development process – unlike many other tools. SAST technologies like CodeSonar simply attach to your existing build environments and add information to your verification process.

CodeSonar uses your existing build environment to create an abstract model of your entire platform, which then allows for exploration of program paths and reasoning about program variables. Advanced theorem-proving technology then prunes infeasible paths and checkers find common defects and violations of policies. Warnings are generated once anomalies are found and defects can be tracked across builds (even in your code changes).

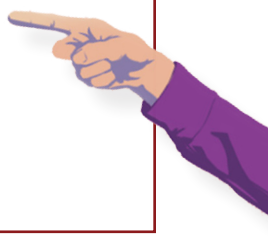
The tool is highly customizable and becomes more robust as you use it. Defects can be annotated, ranked, assigned, searched for, and compared to – all adding up to a treasure trove of historical information through data analysis.

CodeSonar is the perfect tool to evolve with your company. It reduces the risk of costly and brand-damaging vulnerabilities – allowing you to find errors before they become exploitable vulnerabilities – so that you don't fall into being a coding scapegoat. Instead, you ascend to Coding GOAT.

Don't waste time doing static testing the hard way. Automation is on the rise and GrammaTech's CodeSonar is there to protect you and your team by staying ahead of the game.

## Coding GOAT Tip

Understand the Bigger Picture: If you're aware of client needs, business strategies, and revenue pipelines, you'll deliver better results, use your expertise to contribute to company objectives, and prove your worth.



BOOK AN EVALUATION AND RECEIVE A FREE CODING GOAT T-SHIRT

## WORKS CITED


[1] Lohrmann, Dan. “2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic.” Government Technology State & Local Articles - e.Republic. Government Technology, December 12, 2020. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

[2] Morgan, Lisa. “5 Ways Static Code Analysis Can Save You.” SD Times, September 4, 2018. https://sdtimes.com/test/5-ways-static-code-analysis-can-save-you/.

[3] Foster, Mark, Jesus Mantas, and Peter Korsten. “2021 CEO Study -- Find Your ESSENTIAL: How to Thrive in A Post-Pandemic REALITY,” February 2021. https://www.ibm.com/thought-leadership/institute-business-value/report/ceo#.

[4] “Software Developers: Occupational Outlook Handbook.” U.S. Bureau of Labor Statistics, September 1, 2020. https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm.

[5] “2020 Cost of a Data Breach Study.” IBM Security, June 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

[6] Carielli, Sandy, and DeMartine Amy. The State Of Application Security, 2020. Forrester, May 4, 2020. https://www.forrester.com/report/The+State+Of+Application+Security+2020/-/E-RES159057#.

[7] Graham, Bill. Enhancing Code Reviews with Static Analysis. GrammaTech. https://blogs.grammatech.com/enhancing-code-reviews-with-static-analysis.

[8] Morgan, Lisa. “5 Ways Static Code Analysis Can Save You.” SD Times, September 4, 2018. https://sdtimes.com/test/5-ways-static-code-analysis-can-save-you/.

[9] Kunchala, Vikram, Michelle Shuttleworth, Kieran Norton, and Dylan Hack. “DevSecOps and the Cyber Imperative.” Deloitte Insights. Deloitte, January 16, 2019. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/embedding-security-devops-pipelines-devsecops.html.

[10] Constantin, Lucian. “What Is DevSecOps? Why It’s Hard to Do Well.” CSO, July 23, 2020. https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html.

[11] Anderson, Erica. “How to Build an Effective DevSecOps Culture.” The GitHub Blog. GitHub. https://github.blog/2020-04-28-how-to-build-an-effective-devsecops-culture/.

[12] Sirkin, Harold L., Perry Keenan, and Alan Jackson. “The Hard Side of Change Management.” Harvard Business Review, October 2005. https://hbr.org/2005/10/the-hard-side-of-change-management.

[13] OWASP Top Ten. OWASP, 2017. https://owasp.org/www-project-top-ten/2017/.

[14] Ritchey, Diane. “Data Breach Directions: What to Do After an Attack.” Cyber Security News. Security Magazine, February 1, 2015. https://www.securitymagazine.com/articles/86071-data-breach-directions-what-to-do-after-an-attack.

[15] Sukianto, Axel. “Real Life Examples of Web Vulnerabilities (OWASP Top 10).” Cyber Threats. Horangi Cyber Security, June 19, 2020. https://www.horangi.com/blog/real-life-examples-of-web-vulnerabilities.

[16] Abrams, Rachel. “Target to Pay $18.5 Million to 47 States in Security Breach Settlement.” The New York Times. The New York Times, May 23, 2017. https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

[17] Morgenroth, Sven. “Application Level Denial of Service – A Comprehensive Guide.” Netsparker. Netsparker, January 19, 2018. https://www.netsparker.com/blog/web-security/application-level-denial-service-guide/#BillionLaughsAttack.

[18] Sukianto, Axel. “Real Life Examples of Web Vulnerabilities (OWASP Top 10).” Cyber Threats. Horangi Cyber Security, June 19, 2020. https://www.horangi.com/blog/real-life-examples-of-web-vulnerabilities.
19 “8 Cyber Threat Trends to Watch Out for in 2021.” Publication. Booz Allen Hamilton, 2020. https://www.boozallen.com/c/insight/publication/8-cyber-threat-trends-for-2021.html.

20 Buenen, Mark, Ajay Walgude, Rahul Mitra, and Jayant Kumar. “Capgemini: World Quality Report 2018-19.” Capgemini Worldwide, 2018. https://www.capgemini.com/service/world-quality-report-2018-19/.