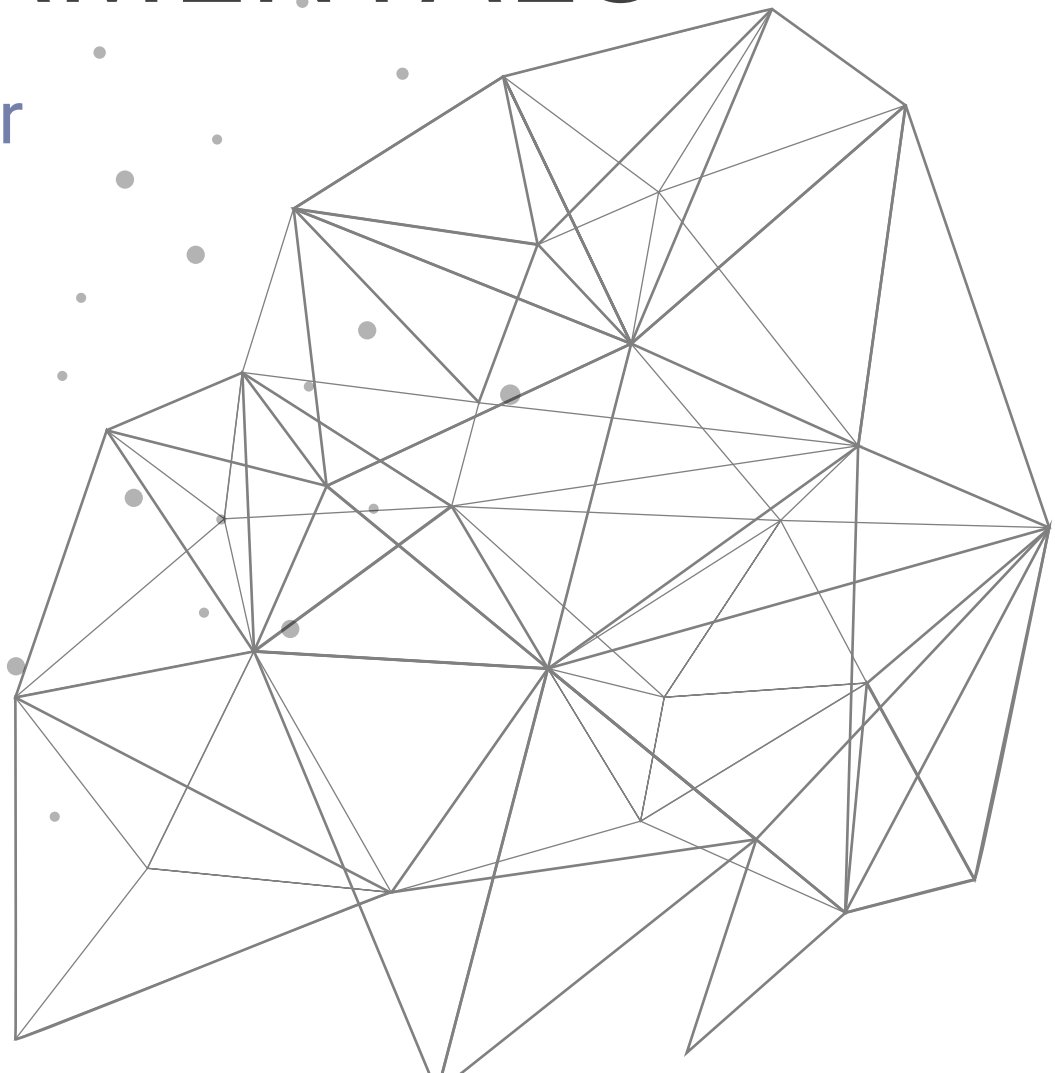
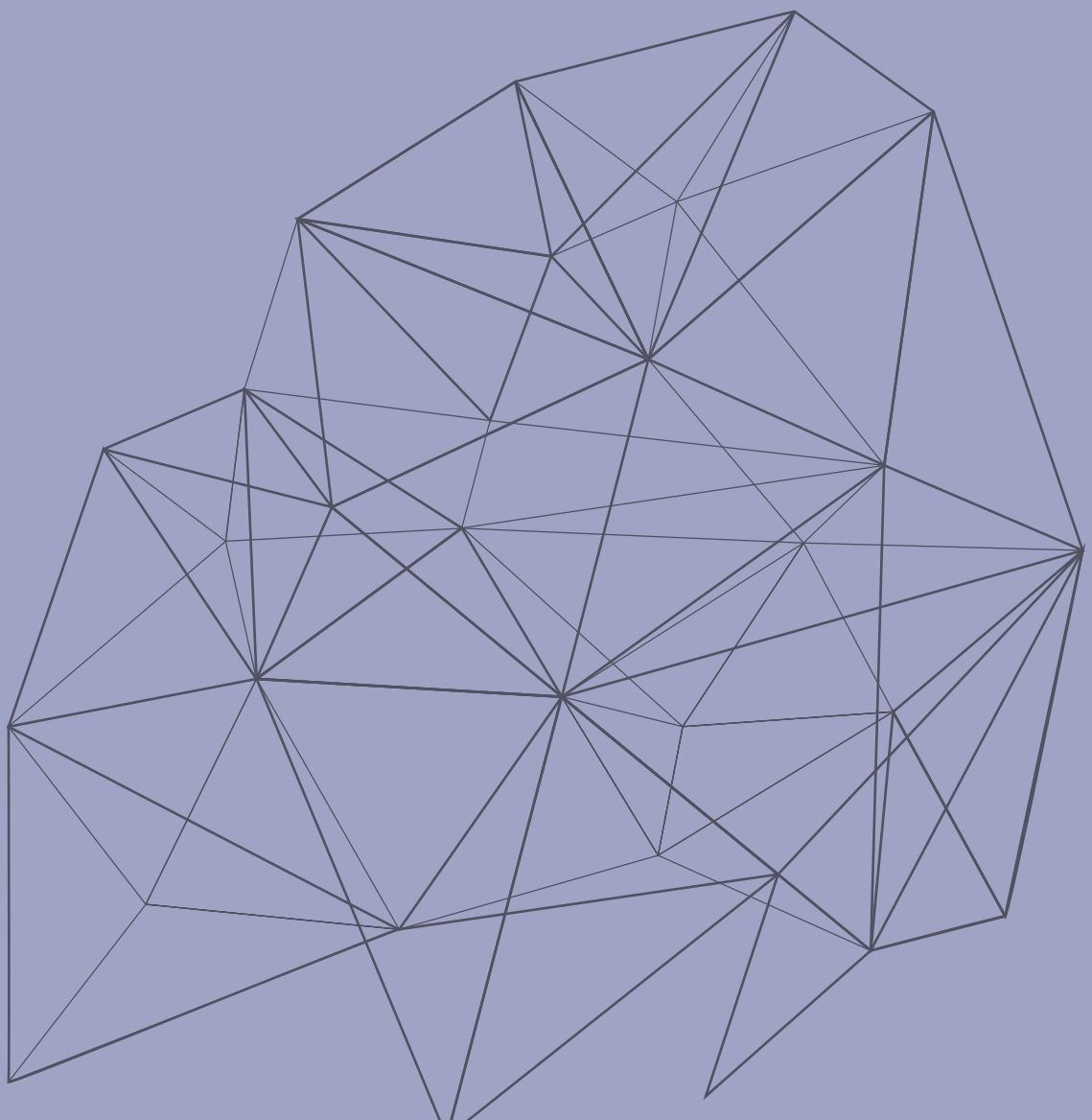
MAKPAR

In Response to The SolarWinds Breach:

THE NEED TO RETURN TO CYBERSECURITY FUNDAMENTALS

White Paper





INTRODUCTION

In mid-December 2020, SolarWinds acknowledged that it experienced a massive supply chain attack where its compromised software channel was used to push out malicious updates to 18,000 of its Orion platform customers. Several government agencies were impacted in this unprecedented breach, including the Department of Defense, Department of Commerce, Department of Homeland Security, and others.

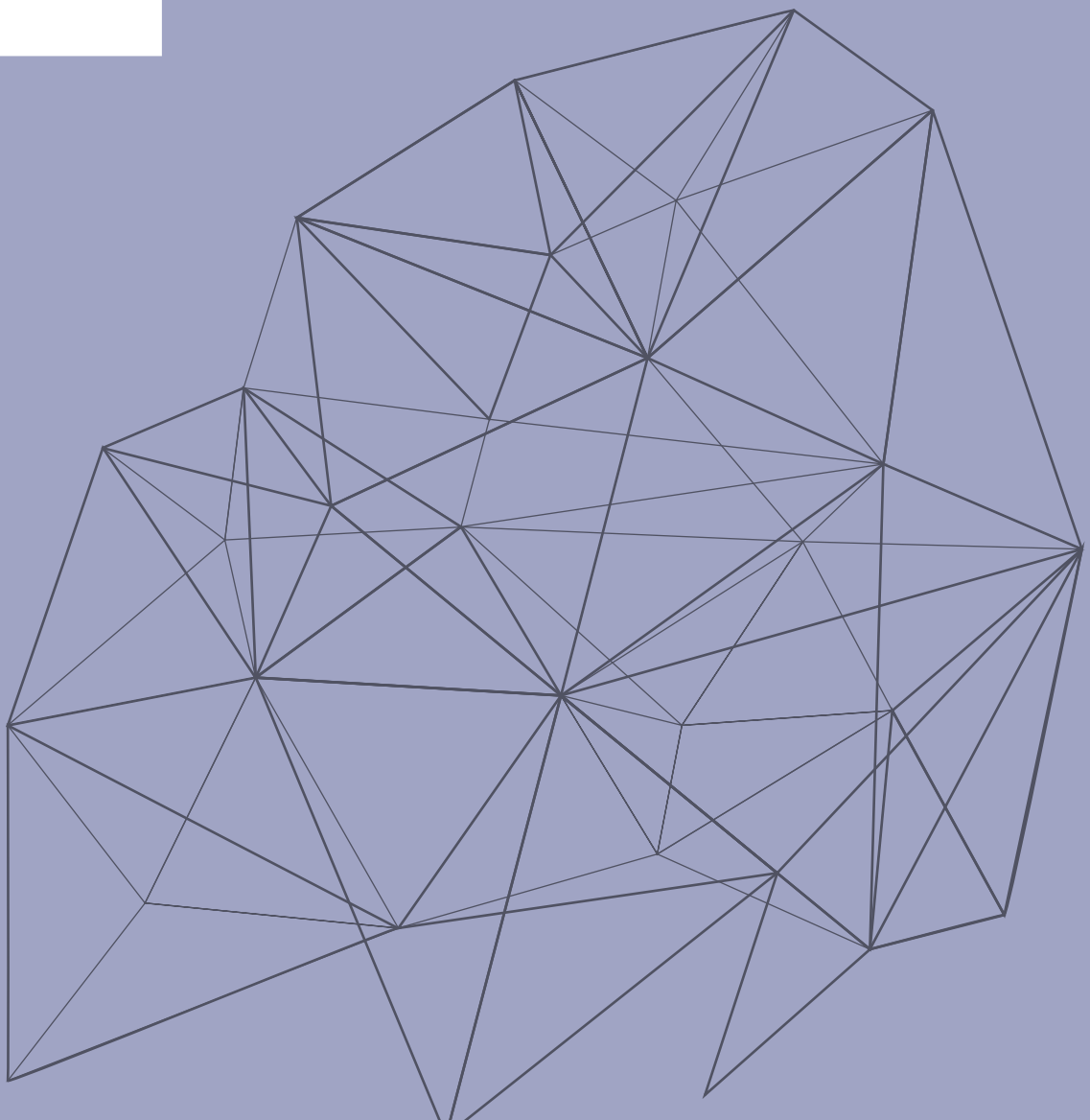
The fallout of this attack continues even now with the Department of Justice announcing that hackers accessed its Microsoft Office 365 email server, gaining the ability to see internal emails and correspondence.

While much of the commentary around the breach focuses on how it happened, little has been said about how to respond moving forward. This incident reminds us: we're never too far gone to ensure we're implementing the fundamentals. Utilizing cybersecurity basics can alleviate a number of the issues that allowed the hack to happen. Here are our top five cyber fundamentals to help mitigate such future attacks.

TOP 5 CYBERSECURITY FUNDAMENTALS

1

FOCUS ON HIRING THE RIGHT SECURITY PROFESSIONALS



The Value of the Right Hire

While cyber tools are valuable for creating a strong security posture, this widespread breach points to how agencies have become too tool dependent. In the SolarWinds breach, SAML (Security Assertion Markup Language) tokens were forged without corresponding issuing logs at the identity provider. While it is unlikely a service provider would detect the forgeries, a qualified security professional could have double-checked these tokens to ensure that there was a corresponding action for their issuance (e.g., was a work ticket created to issue this credential?).

Additionally, there is often not enough logging occurring in Windows environments. Out of 11 Windows logging categories, and 56 subcategories, a Windows 10 computer only has 12 subcategories enabled by default. It requires a knowledgeable security professional or system administrator to configure the additional logging necessary to capture the right amount of information to identify advanced persistent threats. This advanced logging could have made it possible to correlate events and identify lateral movement in the environment. It is much easier to determine false positives and actual breach events by having knowledgeable cyber professionals and subject-matter experts configure these tools and analyze the results and logs generated by these tools, rather than relying completely on automated security tools.

Of course, we are not advocating for agencies to stop their investments in a security toolset; conversely, tools do not replace human analysis. The reality is that experienced cybersecurity professionals have the expertise to spot and anticipate this kind of breach. During the hiring process, it is helpful to seek out professionals with hands-on skills in network monitoring, incident response, threat hunting, and vulnerability management, as opposed to candidates who only possess numerous certifications.

In addition, experienced professionals can maximize the use of available tools and solutions tailored to the environment. The software ecosystem and supply chain for security tools is massive – creating an even wider-range of vulnerabilities when new tools are introduced. All too often, agencies acquire and use the most popular security tools, such as SolarWinds, without completely understanding their configuration and deployment. When a breach of this magnitude occurs, most agencies become vulnerable. Trained cyber professionals can help to develop and understand the right threat mitigation solution. By leveraging automated monitoring solutions, agencies' security professionals can receive alerts to when data is being sent out from their networks to an unknown location. Cyber threat hunting, where security professionals proactively search through networks to detect and isolate threats with an "assume breach" mindset, is also helpful to identify weaknesses.

Security assessments should also be conducted on all third-party tools used in the environment. Vendors should be using security best practices themselves, which can include having Security Operations Center (SOC) and supply chain risk management regularly undergo penetration testing and more.

Considerations for Hiring the Right Workforce

Outside of the Box Thinkers

The best cybersecurity professionals are able to creativly solve problems. You may find that they don't have the exact degree you were looking for, but they have the right attitude for problem solving. Keep an open mind.

Always Learning

The cyber space is constantly changing. You want to work with people who are passionate about keeping up with everything. They're reading cyber blogs, listening to podcasts, taking courses. They're reliable resources.

Certifications

Keeping an open mind is key and certifications aren't everything, but they can be a key indicator to a dedication for training. Often, great candidates will keep up with the latest certifications in the changing landscape.

Relevant Work Experience

For higher level positions, those who have relevant experience working with cybersecurity already will be reliable resoruces who can continue to build upon their base knowledge. They'll be primed to catch threats before they happen.

Offer Training to Staff

As you're likely focused on hiring voracious learners, offer them opportunities to continue their training on the job. This will be attractive to top cybersecurity candidates.

Key Skills

Of course, never overlook the key skills: Strong analysis and threat detection, secure software development, skilled in attacking problems from different angles, understanding of network architecture, and strong communication and collaboration.

Industry Insight:

Currently we're facing a cybersecurity talent gap, similar to what happened with the internet boom of the 1990s.*

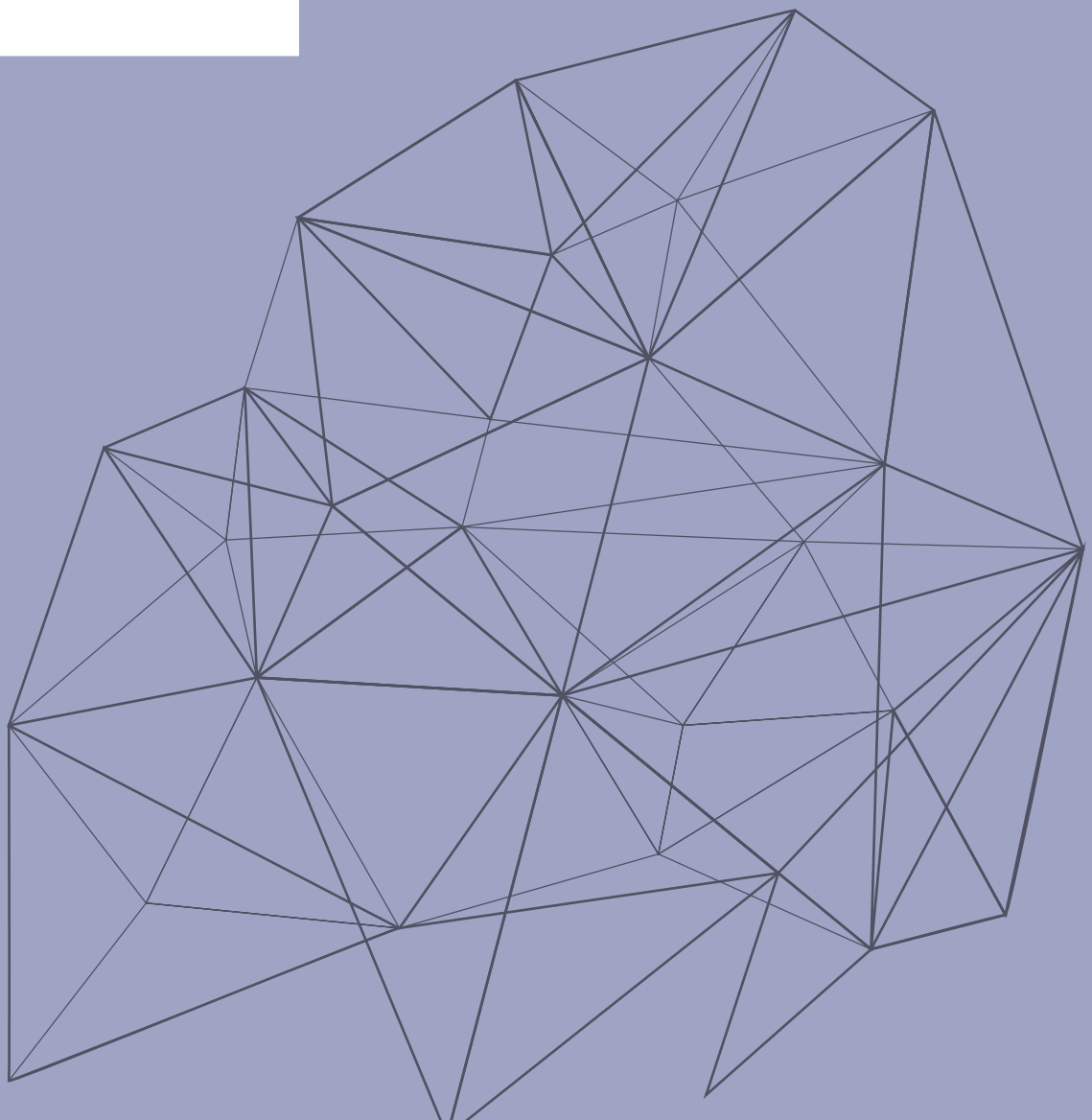
One way that industry and government can close this gap is by offering a culture rich in support and continuous training.

The best cybersecurity professionals are constantly learning and growing, and will continue to do so on the job.

* 350% growth in open cybersecurity positions from 2013 to 2021.
Source: *Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021* (October 2019); Cyber Crime Magazine

2

EMBRACE CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)



The Foundation for Zero-Trust

A strong and robust Continuous Diagnostics and Mitigation (CDM) Program will help to provide a proactive approach to improving an agency's cybersecurity posture. CDM is the Department of Homeland Security (DHS) program for civilian agencies to deploy sensors across its network and assets to provide real-time data in an automated and continuously-updated dashboard on an agency's cybersecurity flaws.

Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside their perimeters. Rather, access to all agency systems must be verified first before being granted. CDM Phase 2, and eventually CDM Phase 3, will serve as a foundation to achieve "zero trust" verification for all applications and processes connected to agency systems before granting users access. In order to get to Zero Trust, agencies need to first understand what is happening on their networks through their CDM efforts.

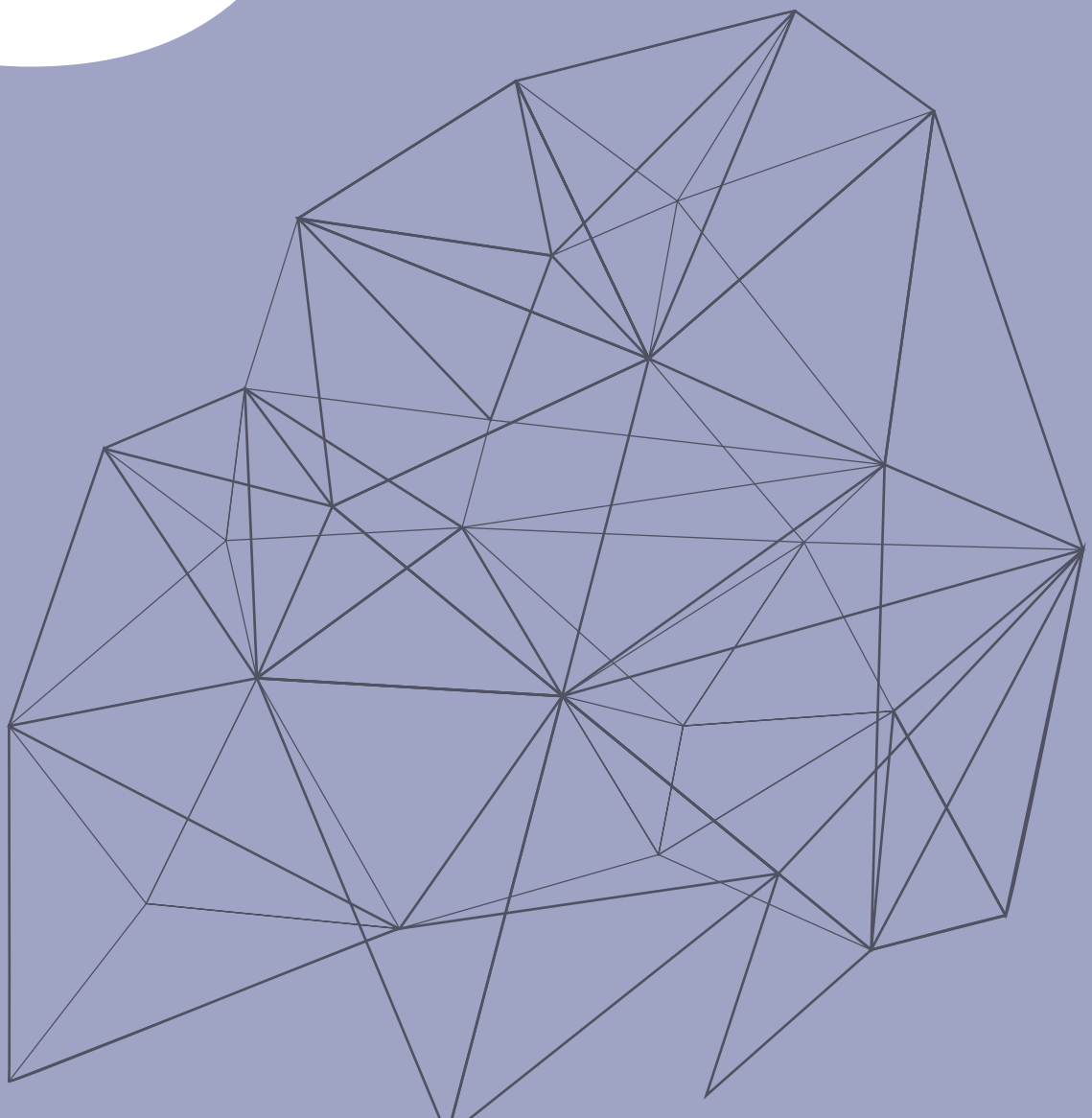
By adopting a Zero Trust mindset, federal agencies can protect all resources regardless of location; deploy a least privilege strategy with strict access control; and inspect all log relevant traffic on a network. Ultimately, this enables agencies to ensure that the action was generated by a trusted entity. For example, in the case of SolarWinds, attackers inserted malicious code next to trusted code within the SolarWinds Orion Platform DLL. They were then able to gain access to any organization that downloaded that code. Employing Zero Trust would have impeded lateral movement by the hackers across the network, such as what happened at the Department of Justice where the SolarWinds hackers were able to escalate their privileges to gain access into the email servers.

The Future of Federal IT:

Identity management and authentication are integral to zero trust. Zero trust is what prevents hackers from accessing the keys to the castle as quickly as they want, and eventually discourages them from continuing to try.

3

INCREASED SECURITY AWARENESS TRAINING



Invest in the Latest Trainings

Security awareness training would also play a major role in putting the spotlight on changing human behavior – countering social engineering efforts – in ways that reduce vulnerabilities.

Social engineering has emerged as a top threat vector for hackers to exploit human behavior to gain access to networks via malware. For example, the 2020 Verizon Data Breach Report found that 96 percent of social engineering attacks enter organizations through email inboxes. Even the biggest tech companies are not immune from social engineering. Last summer, Twitter experienced a coordinated attack that compromised some high-profile accounts of celebrities and politicians.

Best practices in Security Awareness Training include: having an organization wide participation in security awareness so the relevance of cybersecurity best practices is understood by end users at all levels of an organization, having baseline vulnerability measures to gauge your progress and success in delivering security services, scheduling regular assessments and trainings to raise awareness of cybersecurity education among end-users, and consistently tracking and reporting data that adds to actionable business intelligence among other courses of action.

Center for Development of Security Excellence, Defense Counterintellgience and Security Agency (CDSE)

Security Awareness Hub

This resource includes frequently-assigned courses, including mandatory annual training, to DoD and other U.S. Government and defense industry personnel who do not require transcripts to fulfill training requirements for their specialty. You do not need an account or any registration or sign-in information to take a Security Awareness Hub course: securityawareness.usalearning.gov

Courses Available on the Following Disciplines:

Counterintelligence

Cybersecurity Awareness & Risk Management

General Security (DoD Principles)

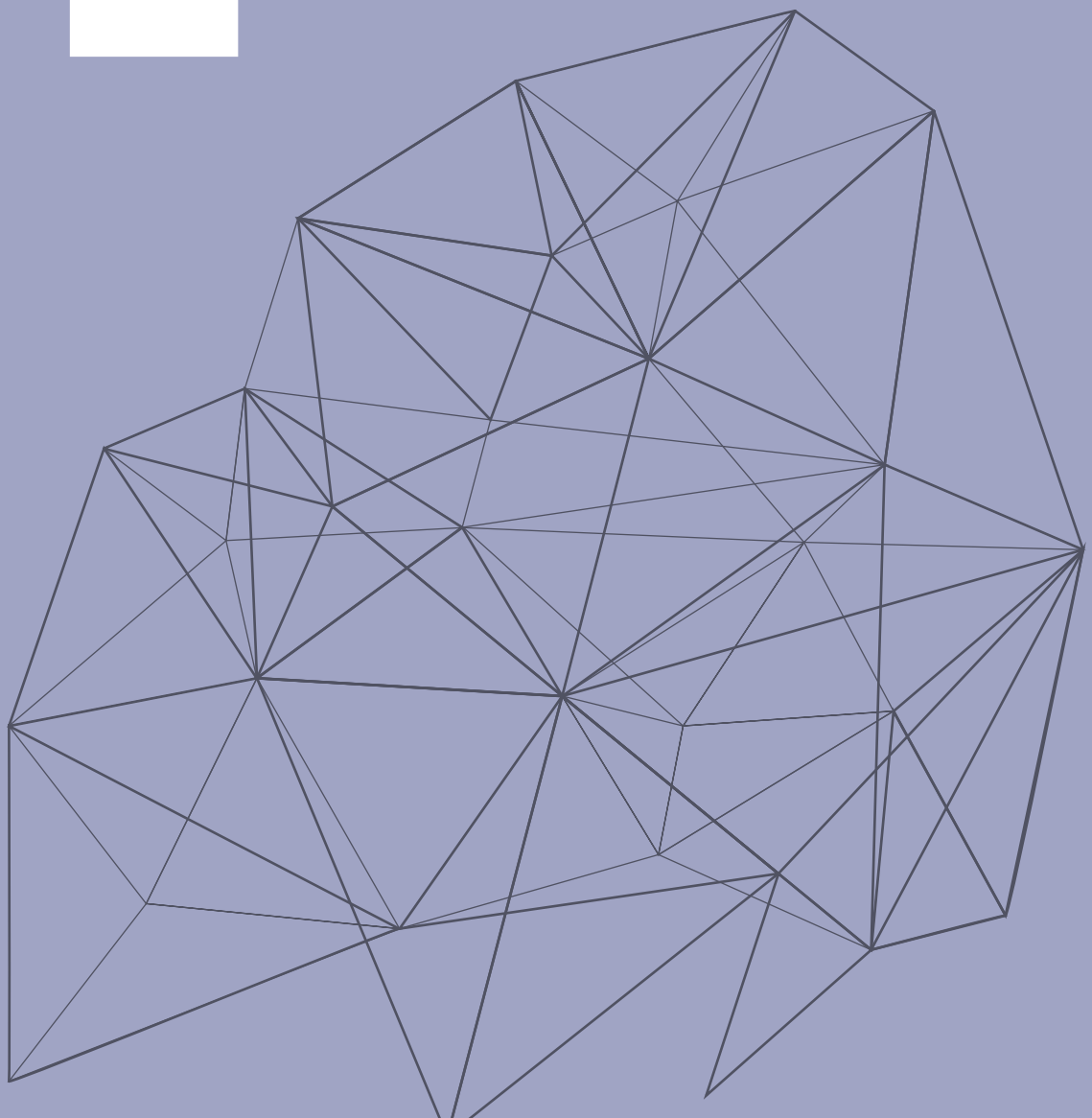
Information Security

Insider Threat

Operations Security

4

CHANGE PASSWORDS AND USE MULTI-FACTOR AUTHENTICATION (MFA)



Multi-Factor as a Baseline Always

One of the best defenses against being hacked is having strong passwords. We recommend changing default passwords immediately with every device, as well as using no less than eight characters that are a combination of letters, numbers, and symbols. It's always good to remember that the strongest passwords have the most characters. For example, the password "trombonetriangleredhorse," which is longer, will be more difficult to hack than "Tr0mb#nE" despite its mixture of letters, symbols, and varied capitalization.

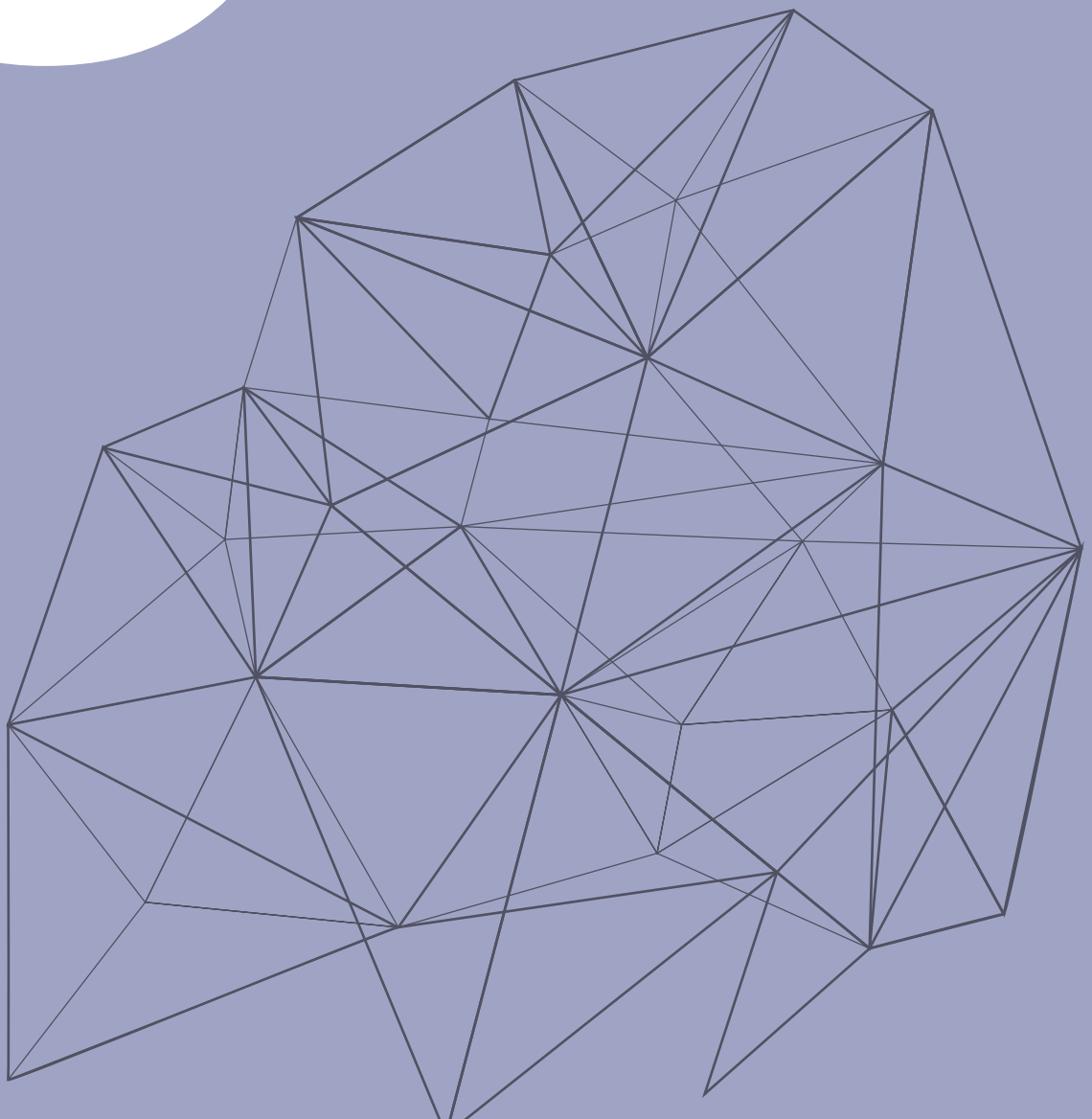
In addition to the most basic defense of changing passwords every 30 to 90 days, multi-factor authentication, and the use of Personal Identity Verification (PIV) credentials can help prevent future breaches. Everyone should move away from using text messages/SMS for authentication, which can be easily be spoofed or intercepted. Better security authentication methods include authenticator applications (e.g., Google, Microsoft), PIV cards, or security keys that are Fast Identity Online (FIDO) Alliance compliant (e.g., Yubikey, Titan), and all user accounts should have multi-factor authentication (MFA), which should be mandatory for administrator accounts.

99.9%

percent of compromised accounts did not use multi-factor authentication, according to a recent report. (Source: Microsoft)

5

THREAT MODELING AND RED TEAM SIMULATIONS



Staying Ahead of Threats Before They Become Threats

Threat modeling is a process to identify and prioritize potential threats and security mitigations. Also referred to as architectural analysis, threat modeling in the Software Development Lifecycle (SDLC) entails identifying the trust boundaries in your development and production environments, and data flows across those boundaries. This can help mitigate supply chain attacks by enumerating potential attack vectors, structural vulnerabilities, or the absence of appropriate safeguards. Threat modeling should be done regularly. For example, when following a DevSecOps approach, threat modeling can be done as part of the Planning phase.

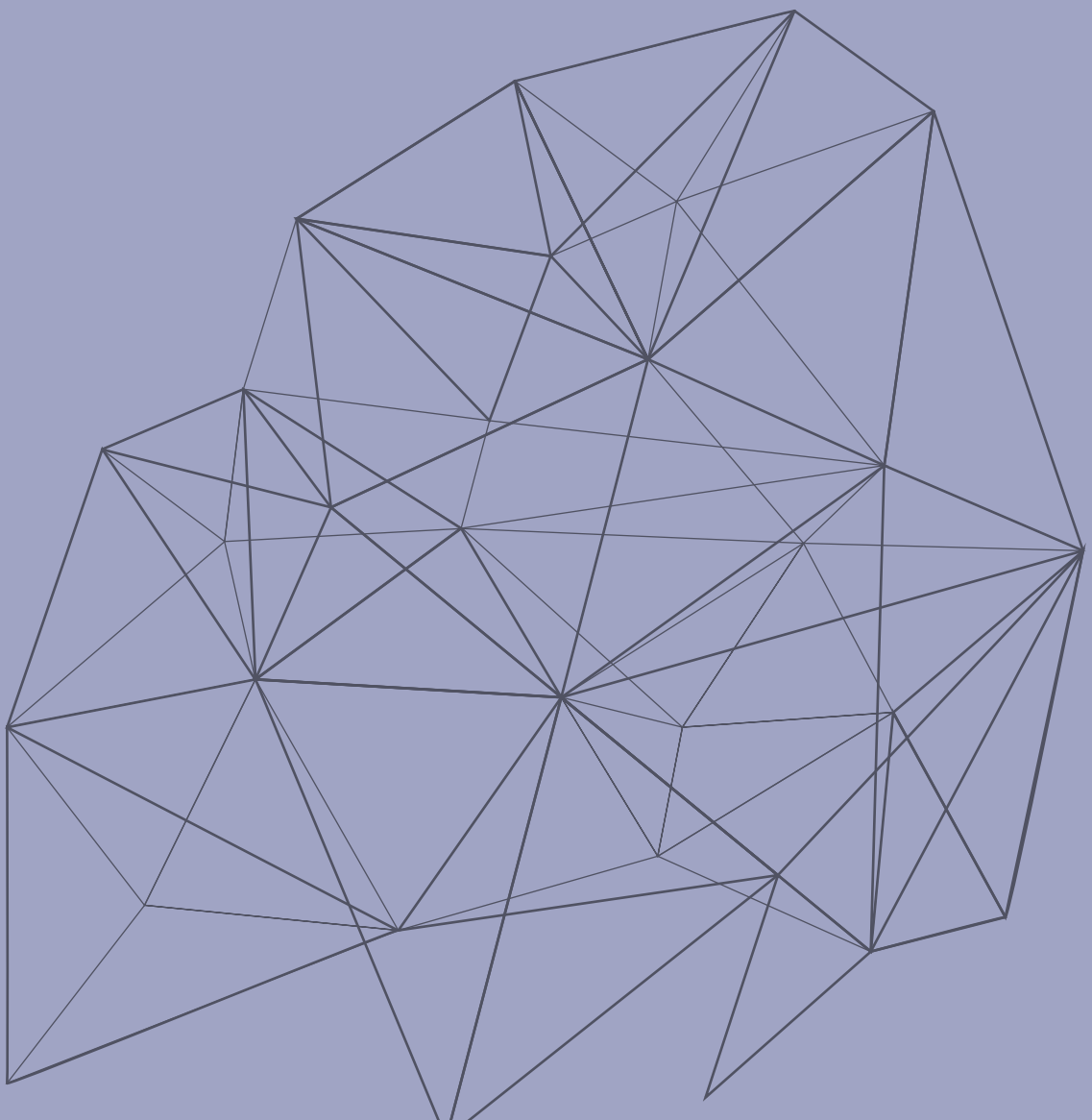
We also recommend using MITRE ATT&CK to mimic some of the most advanced attacks that your environment may encounter. The goal is to emulate your adversaries and potential attackers based on your organization type. This provides a systematic analysis of what controls or defenses need to be included, along with the attacker's probable profile and the most likely threat vectors.

7 top threat modeling methodologies:

1. **STRIDE** - stands for the six categories of threat: spoofing, tampering, repudiation, information discolsure, denial of service, elevation of privilege.
2. **DREAD** - stands for six questions you would ask about each potential threat: damage potential, reproducibility, exploitability, affected users, discoverability.
3. **PASTA** - stands for *Process for Attack Simulation and Threat Analysis*, is a seven-step process focused on aligning technical security requirements with business objectives.
4. **VAST** - stands for Visual, Agile Threat Modeling, and underlies ThreatModeler, an automated threat modeling platform that distinguishes between application and operational threat models. Designed to integrate into DevOps workflows.
5. **Trike** - a framework and accompanying open source tool for threat modeling and risk assessment, built to be defensive rather than emulate hackers' processes.
6. **OCTAVE** - stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation, and focuses on organizational rather than technological risks.
7. **NIST** - The U.S. National Institute of Standards and Technology has its own data-centric threat modeling methodology with various steps.

Source: *Threat modeling explained: A process for anticipating cyber attacks* (April 2020), CSO

CONCLUSION



There are always lessons learned in the wake of any major cyber-attack. These five cyber basics can ensure that your system is cyber resilient so you can mitigate the risk of a similar type of breach happening in the future.

In Review

#1: Hire the right people. Invest in training and support.

#2: Embrace CDM practices.

#3: Increase security awareness training.

#4: Change passwords frequently and employ multi-factor authentication.

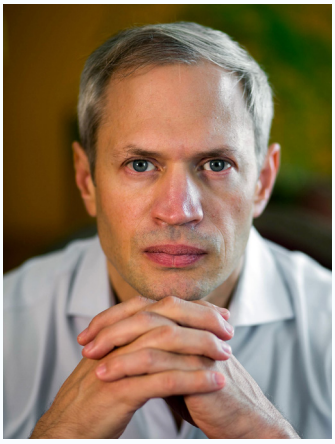
#5: Implement threat modeling.

CONTRIBUTORS

Mustafa Lutfi

Senior Security Engineer at Makpar | CISSP | CISA | CISM

Mr. Lutfi is a Senior Security Engineer at Makpar, who has used his expertise to lead to successful proejct delivery for Federal clients, including developing the operations and standards for quality control for the IRS. Mr. Lutfi holds a Bachelor of Science in Business Administration and Computer Science from the University of Alabama, as well as several recognized cybersecurity certifications. He is currently sitting for the Offensive Security Certified Professional (OSCP) certification.



Alexander Fry

Principal Security Consultant; President & CEO of Strong Crypto MSISE | GSE

Mr. Fry is the Principal Security Consultant, President, and CEO at Strong Crypto Innovations LLC (DBA SCI), providing innovative Cybersecurity solutions for its US government and commercial clients. Mr. Fry holds a Master of Science in Information Security Engineering (MSISE) degree from SANS Technology Institute and is GIAC Security Expert (GSE) #146.

Makpar

Makpar's highly skilled and certified cybersecurity experts understand the technology and methodologies required to preserve the confidentiality, integrity, and availability of information in all computing environments.

Our experts have experience in Information Assurance Certification and Accreditation, Vulnerability and Risk Management, Incident Management, Disaster Recovery, Compliance, Network Security, Cloud Security, Threat Modeling, and other security focus areas in Cybersecurity.

www.makpar.com

Strong Crypto Innovations (LLC)

Makpar thanks our good friends at Strong Crypto Innovations (LLC) for their support in preparing this. Strong Crypto Innovations (SCI) delivers security solutions that are resilient against known attacks and adapt to a changing threat environment.

Their expertise spans several security disciplines including software security, active defense, security assessment, security engineering, firewall design, penetration testing, mobile device and application security, automated static analysis, security testing throughout the SDLC.

www.strongcrypto.com

Makpar
50 CATOCTIN CIR NE, SUITE 205 LEESBURG, VA 20176
MAKPAR.COM