SentinelIPS™

7 Security Mindsets to Adopt Today

Security should be about using specific mindsets as guiding principles when designing and building a network's architecture.

24/7 monitoring & one-of-a-kind Network Cloaking technology.
The Sentinel team relieves the burden of managing IPS and IDS once and for all.

Visit us today at www.SentinelIPS.com

✓ NETWORK KNOWLEDGE & PROTECTION ✓ TRUSTING YOUR NETWORK DATA ✓ THREAT INTELLIGENCE & PREPARATION

NETWORK SECURITY
isn’t about devices or hardware

It can be easy to get caught up in thinking if you just had that switch or this box or those tools then your security burden would be lighter. The reality is all of those devices simply become temporary roadblocks for someone who is determined to get into your network and steal data or disrupt performance.

Cybercriminals and hacktivists are constantly evolving their methods and finding new vulnerabilities to exploit. For that reason, the tool that works today will likely be much less effective tomorrow. And beyond that, every network is different. What may make sense for one, won’t for the other.

Security should be about **MINDSETS**

Security should be about using specific mindsets as guiding principles when designing and building a network's architecture .

7 Mindsets you should adopt TODAY

I WILL

1 I will make it harder to exploit my network through legitimate means.

2 I will layer security across my network.

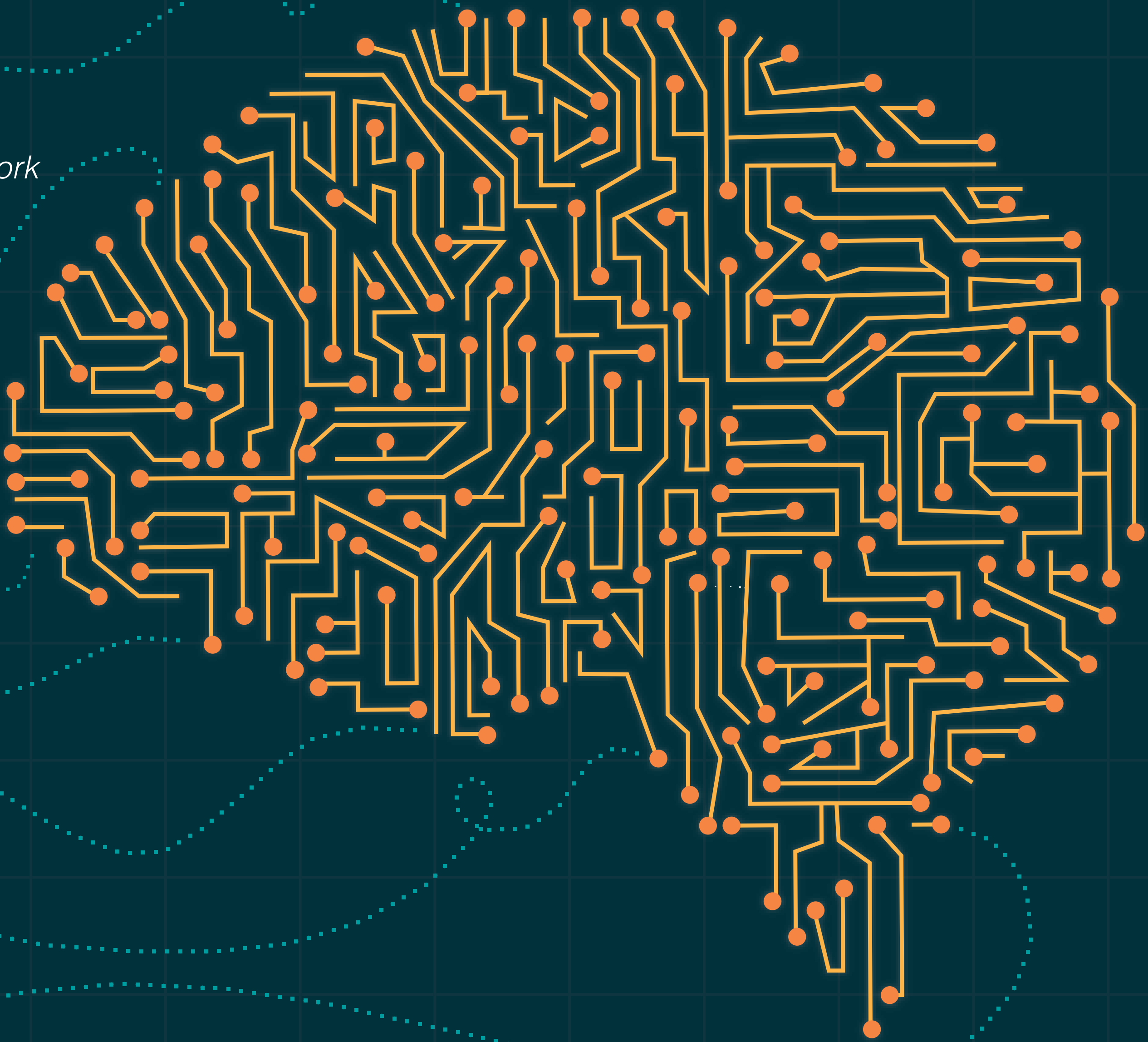
3 I will create a baseline for my network so I'll know what's normal.

4 I will be able to act on what my data tells me.

5 I will implement threat intelligence.

6 I will stay current on the latest threats and trends.

7 I will adopt the 'assume breach' mentality.



1 “I will make it harder to exploit my network.”

Most security breaches don’t occur because someone has discovered a way to take advantage of a network vulnerability. Instead, most unwelcome visitors enter the data center through legitimate methods, like just typing in an active username and password.

A PRIME EXAMPLE

“According to a former IT employee with Sally Beauty Supply, the retail chain’s network was breached in 2014 when someone was able to gain entry through a Citrix remote access portal using the login credentials of a district manager who often worked remotely.”

“This guy was not exactly security savvy,” Blake Curlovic told Krebs on Security. “When we got his laptop back in, we saw that it had his username and password taped to the front of it.”

That’s why it’s critical to consistently do these three things:

- *Preach rock solid login credentials with really good passwords.*
- *Lock down application logins as much as possible to prevent brute force logins.*
- *Reinforce the importance of not being casual with login information.*

Also, take time to educate your employees on social engineering. Just because they aren’t keeping their passwords written on a sticky note doesn’t mean they won’t make it almost as easy for a potential threat to get their login information. Phishing emails, phone calls, whatever social engineering looks like, being able to spot and avoid these scams means fewer unwanted visitors and more time the security teams can spend on bigger issues.

2 "I will layer security across my network."

It'd be nice, as the SANS Institute points out, if there was one device that could be counted on to keep a network safe. Plug it in. Security. But that's just wishful and potentially dangerous thinking.

"There is no such thing as a silver bullet, and it takes many technologies and processes to provide comprehensive risk and security management," the experts at SANS write in a white paper on layered security. "Trusting the latest thing will not end up well if your organization finds itself under a targeted attack. Even if you aren't specifically targeted, assuming you are safe is a dangerous way to operate. Instead, organizations should continually be checking their systems for vulnerabilities, learning about new threats, thinking like attackers and adjusting their defenses as needed."

THE KEY TO SECURITY IS VISIBILITY

You have to know what's coming into your network, where it's going and what it's doing once it's inside. This requires layers of security. It's an IPS and firewall at the perimeter. It's a web filter or proxy service to monitor users' web traffic. It's antivirus protection at the endpoints. And for all the area in-between, it's switches and tools that can watch the data move around. Maybe that's a Security Incident and Event Management appliance, or SIEM, that gathers log information from across your network and makes that data available for analysis all in one spot.

This type of layered security is only going to become more important as the traditional idea of a network, and what constitutes its edges, begins to change. The traditional definition of an end point is getting fuzzy; it's no longer the desktop computer in an office somewhere. It could just as easily be a smartphone sitting in someone's pocket or a tablet tossed quickly into a briefcase.

3 “I will create a baseline for my network so I’ll know what’s normal.”

If you are going to spend the time to build layered security into your network, then you also need to establish what normal looks like, a baseline to measure against. That’s the only way you will know when something is potentially wrong.

There are several tools that can help monitor the amounts of traffic traveling over certain ports. A SIEM device is one, but if that’s outside of your budget some basic network monitoring tools should be able to give you an idea of what's relatively normal on your network’s most important assets.

Who’s talking to those assets? When, why, and how much? That will give you a yardstick to measure future traffic against.

4 “I will be able to act on what my data tells me.”

Putting layered security in place creates a lot of data. You need to be able to act on that data in some way, otherwise, it’s useless.

The well-known 2013 Target breach is a great example. Just before the hackers launched their attack, something raised red flags for security contractors in India. Those contractors contacted Target officials in Minneapolis, and those Target officials did … nothing.

Target’s not alone, and it's amazing to think about. These large companies allow people into their networks with legitimate credentials. Then, when they actually see alerts tripping on different devices, they aren't able to act on it, or they choose not to. That’s where threat intelligence comes into play.

It’s not enough, though, to just act when you see something is wrong. The data you are collecting becomes even more valuable when you are able to use it to be proactive about threat protection. Use this data to stop people before they do anything by placing reputation information into your firewall or your IPS, or having that information in your SIEM.

5 “I will implement threat intelligence.”

You don’t have to try and tackle network security in a vacuum. The security world is actually a very helpful place. It’s common for businesses to share their latest threat information with others, often for free. Use that threat intelligence whenever possible to make your network defenses stronger. And, if your budget allows, there are many threat intelligence vendors.

But you should be able to implement at least some threat intelligence on your external IPS, firewall, in your SIEM, and on your IDS device to help with correlation of data you see going across the network.

! CLICK HERE TO SIGN UP FOR THE CINS NOTIFICATIONS

Free Threat Intelligence Resources

For a range of technical and informational resources regarding data security, check out these free sites:

- ✓ *Emerging Threats (proofpoint)*
- ✓ *shadowserver.org/*
- ✓ *Center for Internet Security*
- ✓ *AlienVault’s Open Threat Exchange*
- ✓ *Sentinel’s CINSscore.com*

6 “I will stay current on the latest threats and trends.”

Security is too important to wait on some professional group or government organization to make an announcement about an emerging threat. It’s important that network professionals be current on the latest threats and trends. And, with social media, there’s no real reason not to be up to date.

There's a great community of network security people out there on Twitter, for example. Get a Twitter handle; get out on Twitter; start following network security professionals and journalists. Do that and you'll be much closer to the zero day than you would be otherwise.

SUGGESTED PEOPLE AND RESOURCES TO FOLLOW

@briankrebs
@CIOonline
@cyberdefensemag
@DarkReading
@CISecurity
@SearchSecurity
@SecIntelligence
@sentinelips
@Securelist

7 "I will adopt the 'assume breach' mentality."

Planning for network security should start from the assumption you're going to be breached, or that you already have. You start there, then prepare for the worst.

Have reliable backups and a solid disaster recovery plan in place. That way, if somebody does get in and they wipe a laptop, or you get Cryptolocked, you're not spending three days getting somebody back up and running.

And don't fall into the trap of thinking your business isn't important enough to hack. Even if you're a small organization, you have assets that may be important to somebody. Recognize that. A small payment processing company that might be a small player in the business. Local banks. They hold lots of important information.

Plus, while risk goes up if the data's important to somebody else, it's certainly important to you. That's the attitude you have to come from. A poorly secured network with untrained users is an easy target for all kinds of threats, some more sophisticated than others. And for a small company with an IT staff of one, something like a Cryptolocker can be crippling.