

The Diary of a Cyber GOAT

A GOAT Guide To Exposure Management

Head of Cybersecurity
at Grazing, Inc.

Gary Grit 

Preface

A New GOAT on the Block



Let me introduce myself: I'm Gary Grit, and yes, I'm a goat. But not just any goat - I'm the new Head of Cybersecurity at Grazing, Inc. It has always been my dream job. Sure, the last goat in this role ended up being a scapegoat after a massive breach, but not me. Nope. I'm no scapegoat.

I'm here to prove that this old goat's got new tricks. This is the story of my first 90 days on the job. I'm writing this diary to leave a path for future bucks and does to follow and to lead their security teams to greener pastures and stronger postures.

We all know Tom Brady, Michael Jordan, Serena Williams, Lionel Messi, Simone Biles, Floyd Mayweather, and Babe Ruth are the greatest of all time. This is my journey to become the Cybersecurity G.O.A.T.

And there we were - at an all-time low. When I joined, the company had just come off a breach. We thought we knew how it had played out: it started with a phishing email, spread through the network, erased a few backups, created rogue user accounts, locked out others, and eventually applied ransomware to part of the network.

I don't want to dwell on the details of how the company dealt with and recovered from it. The point is that employee trust was low, customer trust was low, and we weren't 100% sure it couldn't happen again and hit us from another angle. On the flip side, I had been given the unwritten mandate to lead a change.

I was determined to whip this company into cyber-shape. No more "hoofing it" like my predecessor - I was all about being proactive. I outlined a 12-week plan to achieve true cyber resilience.

Here's how I broke it down:

Week 1: Setting CTEM fundamentals

Week 2: Account for attack surfaces and assets

Week 3: Assess vulnerabilities

Week 4: Test and validate (the GOAT way, of course)

Week 5: Prioritize critical fixes

Week 6: Remediate the critical exposures

Week 7: Set up reporting and KPIs

Week 8: Integrate threat intelligence

Week 9: Grow ransomware resiliency

Week 10: Educate users (even the stubborn ones)

Week 11: Present a grassroots plan and budget to the board

Week 12: Receive sign off on our security validation program



A disclaimer - one goat year is equivalent to 4 human years. That should explain why I was able to accomplish this plan in 12 weeks. It may take humans a bit longer, but the operational principles and lessons I described here still apply.

Week One

Setting CTEM Fundamentals



I knew I needed a clear vision to lead the herd. Morale was at rock bottom. The team was feeling guilty about the breach, and other departments kept piling on the blame. On top of that, a new boss with horns and a beard had just been dropped on them. I needed to turn the tides, get their cooperation, and bring some color back to their cheeks. For that, I needed an operational vision.

I chose CTEM to guide everything related to posture management.

Gartner™ defines Continuous Threat Exposure Management (CTEM) as a proactive cybersecurity approach that continuously identifies, prioritizes, validates, and mitigates vulnerabilities across an organization’s attack surface.

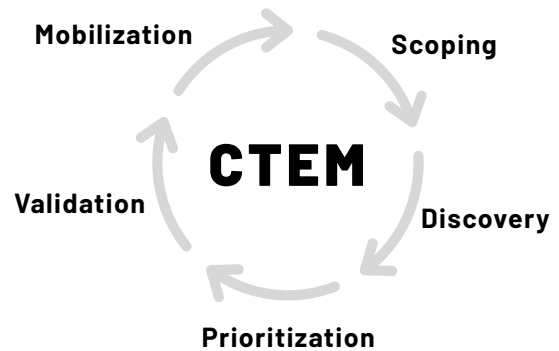
CTEM helps businesses strengthen their security posture by emulating real-world attacks and addressing weaknesses before attackers exploit them.

My scapegoat predecessor was set in his ways on traditional vulnerability management as the be-all and end-all of posture management. That was the critical factor in his demise. This misconception claims that only patchable vulnerabilities matter, while in fact 80% of cyber attacks today occur in the non-patchable vulnerability realm – misconfiguration, identity threats, excess privileges and supply chain attacks. I intend to avoid that trap.

Back to CTEM.

The fundamental principles of CTEM, as outlined by Gartner, focus on proactively identifying and mitigating vulnerabilities to improve cybersecurity posture. Here are the 5 key principles of CTEM in short GOAT form:

- 01 **Scoping:** Define the attack surface by identifying critical assets and understanding their importance to the business.
- 02 **Discovery:** Identify and assess vulnerabilities, misconfigurations, and other security risks across the organization's assets.
- 03 **Prioritization:** Evaluate identified risks to determine which pose the most significant threat, considering factors like exploitability and potential business impact.
- 04 **Validation:** Test and confirm the exploitability of prioritized vulnerabilities through simulated attacks to assess the effectiveness of existing security controls.
- 05 **Mobilization:** Implement remediation strategies to address validated vulnerabilities, ensuring alignment with business objectives, and efficient resource allocation.



So in this first week, I met with all of my team members, gave my CTEM pitch about headbutting the biggest exposures first and called up a few vendors I've used in the past to do a show-and-tell the following week. The first week was all about giving people assurance that we'll get it right.

When it comes to posture management and readiness, follow the CTEM principles. It starts with assessing your exploitable attack surface.



Tip of The Week

Week Two

Account for Attack Surfaces and Assets



A CTEM strategy starts with mapping the attack surface.

Like my father used to say, "You can't mind the herd if you don't know where the goats are!"

A little background on Grazing, Inc based in Minnesota.

We are a multinational provider of high-quality animal feed and nutrition solutions that ships approximately 6.5 million metric tons of animal feed annually through our distribution channels. We have vertically integrated infrastructure, meaning we control everything from breeding and feeding livestock to processing, packaging, and distribution.

Our operations include processing plants and factories, feed mills and grain storage, farms and livestock facilities, logistics and distribution centers, research and development centers, environmental and waste management systems, corporate offices and support centers.

We have about 50,000 endpoints to protect, including data centers for managing operational data, logistics, and inventory tracking. Many of our applications for customers and partners needed better scalability so we've also expanded our infrastructure to Azure and AWS. On top of that, we have a hoofful of IoT devices in our factories.

The breach we incurred last year cannot be considered a surprise given the state of security we had at the time or in place. Don't get me wrong - we use a very well-known EDR solution, a great SIEM technology, and a functioning SOC and ticketing system. In hindsight, our Achilles' heel is our underwhelming exposure management program and related posture management tech stack. Luckily for me, post-breach, I was given a mandate to prepare a modernized roadmap for our security infrastructure in the upcoming decade.

We have a creaky old Nessus scanner and a home grown CMDB that requires manual updates. Generally speaking, all our processes are manual for different compliance reviews. While we do have some understanding of critical assets, I have decided to double-check the list and make sure no dependencies are missed. Some of our peers in the industry have run into serious production issues after their own suppliers and partners were compromised. So we must ensure assets and processes in our supply chain are also meeting a new bar.

Here's what I did. I set up four task forces to break down the work and commission a third-party penetration testing exercise. Delegation is key - no goat can eat an entire haystack alone:

Task force 1 - Evaluated a modern asset management system, since our CMDB only accounted for IT assets and ignored IoT devices. Our shortlist: Armis™.

Task force 2 - Focused on mapping our external attack surface. Not being able to account for all our external-facing assets is a big problem. We decided to go with Pentera™ Surface.

Task force 3 - Realized we didn't have a clear map of our cloud tenants. Since about 40% of our network is distributed across AWS and Azure, this quickly became a red flag for us. The team looked into Wiz™ to address this.

Task force 4 - Kicked off a plan to evaluate supply chain risks with tools like Security Scorecard™.

All of these tools are agentless, and can be tested pretty quickly with relatively short POVs to give me the initial sense of what we're dealing with. I don't know yet if I'll get approval for every tool, but without a solid foundation, defending Grazing, Inc. will be tougher than climbing a steep cliff on greasy hooves.

At least things are in motion, and I'm feeling optimistic. To silence my own thoughts for a couple of hours, I'll be heading to the cinema to catch a special screening of the classic film, *The Silence of the Lambs*. Let's hope it's not as terrifying as landing this new job of mine.

It's not all process and people. Get the best-of-breed technology stack.



Tip of The Week

Week Three

Assess Vulnerabilities



I started this week with confidence. The plan was simple: scan the entire network, map vulnerabilities, and develop a prioritized roadmap for risk mitigation. What I wasn't prepared for was the avalanche of vulnerability data that poured in. Goats are always fearsome of avalanches.

The Nessus scanner ran for what felt like an eternity. When it finally spat out its report, I nearly fainted. Thousands of critical vulnerabilities (CVSS 9.0+). Tens of thousands of high-severity vulnerabilities (CVSS 7.0 - 8.9). Hundreds of thousands of medium-severity issues. It was too much to handle, even for the toughest goats on the mountain.

I also had this gnawing feeling that Nessus was showing me only half the picture. It showed what was inside the barn but ignored the fields outside. So, I pulled data from the previous run of Pentera on my external attack surface. That's when I saw the exposed web assets and misconfigured cloud services practically waving flags that said: "Hack me!"

My frustration hit its peak when I realized that most of the vulnerabilities that Nessus flagged weren't actionable. Many were false positives or theoretical risks with no real-world exploitability. Worse, I couldn't tell which vulnerabilities actually led to critical systems or sensitive data. I needed a better way to sort the wheat from the chaff.

Instead of drowning in CVEs and CVSS scores, I wanted to focus on proven exploitability. Could an attacker realistically exploit this vulnerability? If yes, we needed to prioritize and fix it ASAP. If not, my team had better things to do than mitigating it. It's just a matter of smart prioritization that would allow us to address all our needs with limited team resources.

This required CORRELATING three elements into a single criteria that I dubbed **ALL**, as in *ALL I want to know*:

A vulnerability, or security gap, that is -

Lacking a compensating control (when there are no defenses in place to block or mitigate an attack)

Leading to a critical asset (with attack vector potentially reaching our crown jewels, like customer data or operational systems)

This trifecta has become my new North Star for exploitability.

But let me tell you, separating signals from noise was no easy feat. I called 'goat pellets' on the vulnerability vendors' pitches about AI-based prioritization heuristics. None of it felt real. The vulnerability data overload wasn't just unhelpful - it was paralyzing.

I wrapped up this week feeling more frustrated than accomplished. I know what has to come next. Gartner calls it **Adversarial Exposure Validation**, vendors call it **Automated Security Validation**. In both cases, it's about emulating real-world attacks to see what's actually exploitable.

For now, I'm heading home. The team needs a breather and I need to see the kids and explore a few free grazing ranges!

**CVSS scores alone may lead you astray.
Focus on ALL, the exploitability trifecta:
A vulnerability with an exploit in the wild,
Lacking compensating controls, and
Leading to a critical asset.**

Tip of The Week



Week Four

Test and Validate (the GOAT way, of course)



Following last week's vulnerability overload, on Monday morning we immediately shifted gears into full-scale security validation mode (or as my team likes to call it: **SecVal**). Testing ourselves as an adversary would, considering both outside-in and inside-out.

When it comes to attacks, there's one framework we trust - the MITRE ATT&CK matrix. Our job this week was to put it into action and emulate those TTPs (Tactics, Techniques, and Procedures) against our security infrastructure.

No assumptions - just real-world attack emulation.

The objectives were clear:

- 01 Validate which vulnerabilities were actually exploitable, narrowing the list to the 3%-5% that truly mattered.
- 02 Evaluate whether our outsourced SOC team could detect and respond to threats in-line with the Critical Clarity Methodology, prioritizing high value assets:
 - A. Detecting high-priority alerts within 5 minutes to identify potential breaches or cyber incidents and ensure timely escalation for investigation.
 - B. Triaging high-priority incidents within 15 minutes to analyze and categorize alerts, confirm their validity, and determine the necessary response.
 - C. Responding to high-priority incidents within 60 minutes, including notifying relevant stakeholders, to mitigate impacts, restore operations, and maintain organizational continuity.

I briefed the team on the plan, and emphasized the need to keep operations running smoothly during testing. We'd already rolled out Pentera's security validation full suite (Core, Surface, and Cloud) and organized the week as follows:

- Monday-Tuesday: Running 48-hour tests of on-prem networks and data centers.
- Wednesday-Thursday: Running 48-hour tests of our AWS and Azure cloud environments.
- In parallel, we decided to run Pentera Surface all week long to test our network from the outside-in.
- Friday: Running ransomware emulation and Active Directory assessments with the SOC actively monitoring.

Watching Pentera work was like a Sunday NFL football game. You could see our defense coping while Pentera's relentlessly probed for weaknesses. The best part? No interruptions to operations thanks to its inert-engineered payloads. Pentera's attack orchestrator acted as the quarterback, calling plays and adjusting strategies based on progress.

In contrast to football, Pentera's test attack quarterback doesn't have a blind side. With tens of millions of combinations of IPs, ports, protocols, and payloads, this isn't something humans could do alone. With Pentera, we were able to map out our entire attack surface and approach it with machine-like efficiency.

What really stood out to me was its ability to move laterally and "live off the land" (LOL). Pentera's platform gathered intelligence from every host, database, and file it reached, pieced together data, and used it to escalate attacks, replicating real-world adversary behavior.

Unlike single-step adversary testing tools, Pentera continued digging even deeper, recalculating routes until it reached the target. It reminded me of a GPS navigation app, adapting routes until it got to the destination.

By Friday, we had aggregated findings and scheduled next week's session to prioritize their fixes. This was an eye-opening experience. We finally saw ourselves from an attacker's perspective, and some areas clearly needed immediate reinforcement.

We had user hashes cracked, end-points that could be ransomed, legacy protocols still enabled, missing segmentation firewalls, and accounts that could be taken over.

We also had confirmation that our tools were working, just not at the extent we wanted them to. Our EDR noticed Pentera's remote code execution, however we had left many assets under a "monitor only" policy. We had started to implement some privileged account management policies, but we weren't able to roll it out across the board, as some users were hesitant to make such workflow changes.

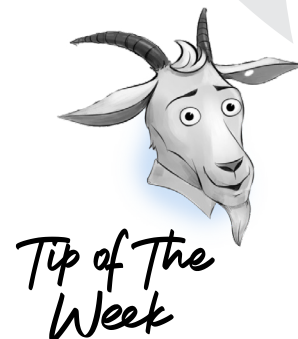
Early on, we realized that Pentera's movement across those accounts we had implemented new policies on was indeed limited and unsuccessful, whereas it was able to move laterally across the accounts we had left unchanged. At least now we have the evidence we need to justify moving this project along!

The good, the bad, and the ugly were all revealed right in front of us.

As we wrapped up the week, I asked the team for immediate attention on the most critical gaps while planning prioritization sessions for the following week.

This week felt like a wild chase. The team actually enjoyed putting on their hacker shoes for once. Now that I'm feeling pretty good, I plan on spending my weekend binging *Mr. Robot* season 4. Next week we'll focus on fixing stuff.

Think like a hacker. Emulate attacks to test defenses and identify the security gaps that pose the highest risk to your business. Build resilience through continuous test-remediate cycles.



Week Five

Prioritize Critical Fixes



I started this week feeling grateful - and ready to tackle the supersized hay bale of findings we unearthed during last week's tests. The plan? Correlate Pentera's exploitability data with vulnerability data, which we already gathered from Nessus and Wiz.

When we cross-referenced Pentera's validated attack paths with CVSS scores and posture data, a clear pattern began to emerge. A small group of vulnerabilities dominated the verified attack vectors. These weren't just theoretical risks - they were real, exploitable weaknesses. The Pentera "Achievement Scores" gave us a clear picture of where to focus our remediation efforts. It was all about pinpointing the best "bang for the remediation buck."

Some findings shocked the team. Our supposedly isolated development environments turned out to have pathways into production. Even more surprising, we uncovered anomalies in systems we had thought were tightly controlled under golden image policies. Turns out, posture drift is very real. Over time, even well-maintained environments decay - and we had the evidence to prove it.

The most surprising results came from looking outside-in; we discovered old domains we had thought were long gone; web services with expired certificates; older servers that were rolled out into production without proper SSH authentication. They were all left anonymous for anyone to access. We also realized one of our contractors did not request a decommissioning of their servers for a past project. Low and behold, Remote Desktop Protocol was exposed without any hardening! There was also a forgotten development utility that was accidentally released to production. It was humbling.

Adding to the mix, we got the results from the manual penetration test conducted in Week 2. I was shocked to discover the pentesters were able to hack us in more than one place, and it was a pretty easy gig. I am determined to invite them back at the end of this process and wipe those smirks off their faces.

After five days of grueling analysis, we handed the IT team a cleaned-up remediation list through a fresh new ServiceNow workspace and queue sets. Gone were the outdated tickets and noise. We gave them a fresh start with clear priorities.

I made sure the IT team understood how the list was composed. We showed them real-world attack paths to drive home the urgency of the fixes. I also prepared them for the long nights ahead of all of us. Patching vulnerabilities is rarely glamorous, but it's necessary.

To keep ourselves honest, I asked my team to determine the baseline scores from all systems (Pentera, Armis, Wiz) as a benchmark for tracking progress. Baselines are critical. Without them, you can't measure improvement or prove you've moved the needle.

Here are the types of findings we prioritized this week (I can't believe we had so many deficiencies to date!):

Product	Sample of found security gaps
Cloud (Source: Pentera Cloud)	Misconfigured IAM policies, excessive permissions, exposed cloud storage buckets, a publicly accessible database, many hardcoded secrets in source code and plain text in files, EC2 instances that were susceptible to role extraction and lateral movement to serverless functions, misconfigured security groups, open network ports, outdated OS and libraries in virtual machines migrated to cloud, lack of MFA enforcement in part, unpatched container images, excessive access to cloud resources, misconfigured Kubernetes clusters, secrets stored in plaintext and vulnerable network configurations.
On-prem Network (Source: Pentera Core)	Misconfigured firewalls, overly permissive network rules, weak or default passwords, unrestricted RDP access, misconfigured VPN gateways, insecure SNMP configurations, plaintext credentials in configuration files, exposed credentials in scripts, lack of critical network segmentation to match organizational structure, weak encryption protocols, expired SSL/TLS certificates, unencrypted database connections, misconfigured Active Directory permissions, possible Kerberoasting, relay attacks, unrestricted PowerShell execution, weak service account permissions. ...and...

	<p>Hardcoded credentials in applications, exposed SSH keys, vulnerable network services, missing endpoint protection, insecure LDAP configurations, unauthorized access to file shares, vulnerable web applications, SQL injection vulnerabilities, exposed Windows Management Instrumentation (WMI) services, brute-force attack vulnerabilities, insecure Kubernetes configurations, exposed backup files, sensitive data stored in plaintext, misconfigured privileged access groups, misconfigured EDR policies, and insecure remote access configurations.</p>
<p>External Attack Surface (Source: Pentera Surface)</p>	<p>Exposed web servers, publicly accessible admin panels, SSL/TLS misconfigurations, expired web certificates, open ports with critical services, cross-site scripting (XSS), sensitive data exposure in responses, DNS misconfigurations, vulnerable third-party libraries, publicly exposed databases, databases allowing remote connection, weak or default credentials, exposed remote desktop services (RDP), open FTP servers, FTP with anonymous access, misconfigured S3 buckets, lack of web application firewalls (WAF), SQL injection vulnerabilities, exposed server logs, exposed test scripts or debug information, remote file inclusions (RFI), Local File Inclusions (LFI), Server Side Request Forgery (SSRF), open authentication interfaces (WMI, WinRM, SMB, RDP, SSH), insecure SNMP configuration, secrets exposed in web application, vulnerable WordPress plugins and themes in use, and internal machines exposed to the internet.</p>

This week was exhausting but productive. I'm proud of how my team came together for this challenge. Next week will be all about remediation. Now onto my weekend plans! I promised my kids I'd read them **Castle Defenders** by Pentera (yes, they even have a kids' cyber book!) and **The Lion, the Witch and the Wardrobe** starring Mr. Tumnus the faun.

Prioritize remediation by exploitability and severity. True risk-based prioritization is about fixing what attackers can use as part of a complete attack vector.



Week Six

Remediate the Critical Stuff



All of the work I'd put into my first five weeks on the job had finally begun to pay off. The team was energized, motivated by the clear direction we're heading in, and I could see the momentum building.

On the flip side, I identified three nay-sayers in the herd - those who can't (or won't) adapt to the changes we're making. This week, I decided it was time to part ways with them. It's never fun, but barn cleaning is sometimes necessary to keep the herd moving forward.

HR was aligned with me on this, and while saying goodbye to people is never easy, it also creates opportunities. I believe that a few promotions from within will bring fresh energy to the team and reinforce the culture we're building - proactive and committed to risk-based posture management.

As critical remediation progressed, I spent time meeting with my colleagues in Application and Cloud IT. My goal was to spread the word about our shift to prioritizing exploitable gaps over the endless chase of theoretical vulnerabilities. People were cautious, as they usually are with change, but there were no showstoppers - which I took as a win.

We began working closely with our blue team in an iterative mode. Once they remediated or mitigated an issue, we ran Pentera again as a quick validation test. It's like rechecking the fence after fixing a weak spot - you need to know the fix holds and that you haven't created a gap somewhere else.

The team even printed out custom T-shirts this week. They proudly wore them around the office, displaying our new mantra:

VALIDATE

REMEDiate

REPEAT

It's simple, but it captures the rhythm we're settling into. Fix the issues, test the defenses, and keep refining until we're as secure as we can be.

One example stood out this week. We found a high-risk misconfiguration in an S3 bucket during last week's tests. It had public access enabled - an oversight from an old deployment pipeline. The fix was straightforward, but Pentera's rerun flagged a new issue: an IAM policy that still allowed excessive permissions. Without the quick retest, we might have missed it. This cycle of validation and remediation is already proving its value.

The iterative process forces the team to stay sharp. Every fix gets double-checked, and nothing is assumed to be resolved until we prove otherwise. It's a mindset shift, and I could already feel it taking hold.

The changes are sticking, and the results are showing. The next step is to keep pressing forward and add more structure and procedure to the department. No special plans for the weekend.

**Validate every
remediation step.
Verify that the fix
actually works and not
just a ticket closed.**

Tip of The Week



Week Seven

Setting Up Reporting and KPIs



This week, I faced a slightly different challenge – metrics and reporting. While I’m comfortable headbutting vulnerabilities and chasing down attack paths, setting up KPIs felt like navigating a new mountain trail. Still, I knew it was critical to track our progress and prove the value of our work. After all, if you can’t measure it, you can’t manage it.

I broke the metrics into four main buckets to keep things organized:

#1 Exposure Visibility:

- **Asset Coverage Rate** - The amount of the estate tested
 - 80% coverage with a goal of 90% of systems scanned and tested.
- **Asset Coverage Frequency** - Average number of tests per asset.
 - High Value Assets (critical to business operations, sensitive data) – Weekly tests
 - Moderate Risk Systems (Internal servers, Employee workstations) – Monthly
 - Low Risk Systems (test environments) – Quarterly
- **Asset Expansion** - Testing new infrastructure deployed across different attack surfaces
 - Critical assets – Testing to discover whenever deployed
 - External assets – Testing to discover new external attack surface assets weekly
 - Cloud assets – Testing to discover new cloud assets upon acceptance and monthly thereafter

#2 Remediation Metrics:

- **Patch Deployment Rate** - Time to deploy patches
 - Patches for critical vulnerabilities should be deployed within 48-72 hours after release.
 - Critical assets should be deployed within 24 hours.
 - Mean Time to Patch should be less than 15 days for all vulnerabilities
- **Time to Remediate Vulnerabilities (TTR)** - Defined by severity
 - Critical Vulnerabilities - Remediated within 48-72 hours, 24 hours for High Value Assets
 - High Severity - Remediated within 7-15 days
 - Medium Severity - Remediated within 30 days
 - Low Severity - Remediated within 60 - 90 days
- **Remediation SLA Compliance** - Percentage of critical vulnerabilities patched within defined SLAs.
 - Critical & High Severity - 90% - 95% SLA compliance
 - Medium & Low Severity - 80% - 90% SLA compliance
 - Overall SLA Compliance - 85% - 90% across all severity levels

#3 Risk Exposure Metrics:

- **Critical Exploitable Gaps Open** - The number of exploitable vulnerabilities found
 - After establishing the baseline of exploitable vulnerabilities, a reduction of 30% for each iterative test
- **Exposed Attack Paths to High-Value Assets** - The amount of attack paths discovered
 - Exploitable attack paths to critical assets should be reduced by 20% in each iteration of a test after establishing the baseline
- **Resilience Score** - Percentage of improvement in posture scores over time
 - Attack emulation exercises should be thwarted at an increasing percentage until 90% compliance, to remain at 90%

With these KPIs, my goal was twofold - ensure we stayed accountable and continuously reduce exposure. I emphasized to the team that security isn't a one-and-done activity but a constant cycle of testing, fixing, and verifying.

I spent most of the week meeting with the IT and SOC teams, walking them through the metrics and setting up dashboards in ServiceNow™ and Splunk™ to track progress. I wanted real-time visibility into our posture, not just reports gathering dust.

One win this week was mapping the KPIs back to our CTEM (Continuous Threat Exposure Management) strategy. The metrics reinforced our focus on frequency, exploitability, and prioritization, giving us a structured way to measure whether we were meeting the SLAs we'd set.

The team was receptive, and a few of them even suggested additional metrics we'll look at next quarter, like API security coverage and supply chain risk scores. The goats are catching on!

At the end of the week, I reminded everyone of our goal: be better than we were last week. Progress is the name of the game, and these KPIs will help us track it. This weekend my in-laws are coming over. I'm gonna bake my famous goat cheese pie. No rest for the wicked.

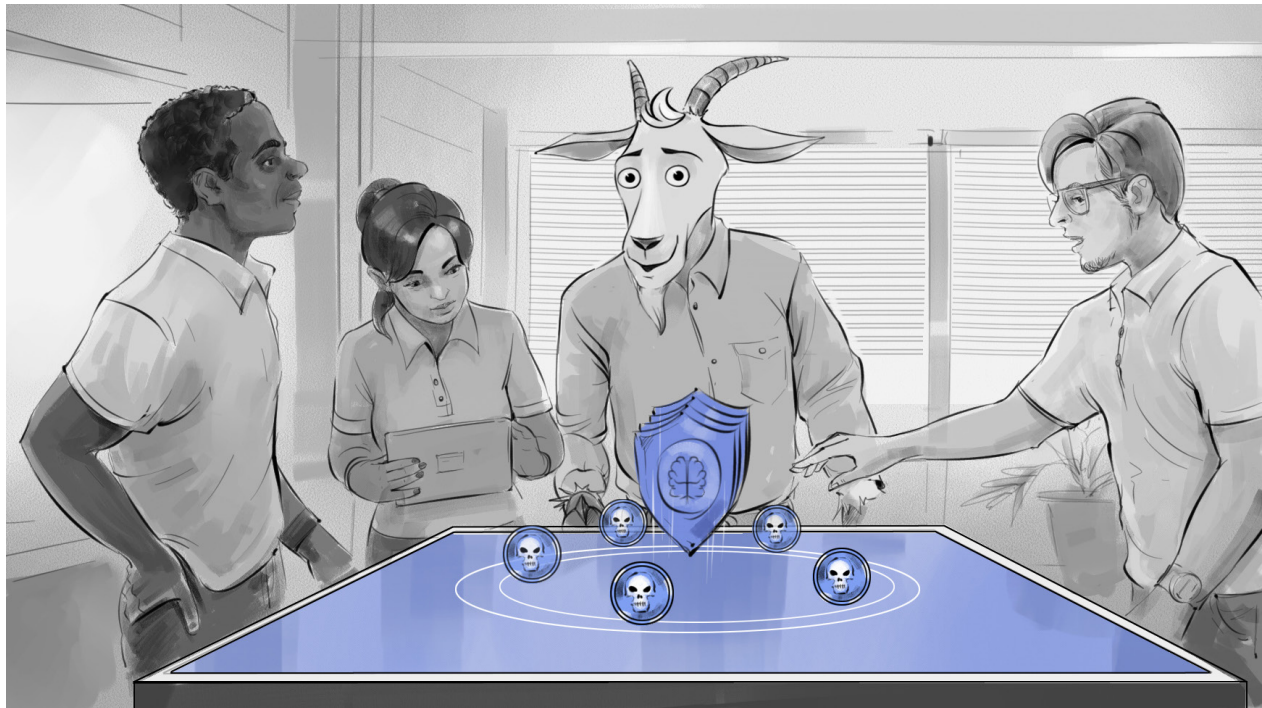
Put forward a few KPIs so you can measure, manage, and communicate CTEM progress. Security is about continuous improvement.



Tip of The Week

Week Eight

Integrated Threat Intelligence



With our KPIs firmly in place, it was time to add the ‘T’ in CTEM (Threat). Grazing, Inc. already had a solid threat intelligence subscription with Recorded Future™, but now we needed to integrate it more deeply into our CTEM framework.

We started by feeding Recorded Future’s Indicators of Compromise (IOCs) - including IP addresses, domains, hashes, and URLs - directly into our Splunk™ SIEM. These IOCs were automatically correlated with logs and events ingested into the SIEM, allowing us to spot and respond to threats in real-time. It felt good knowing we had eyes on our attack surface.

But we didn’t stop there. Identity threats had been on my mind for quite a while, so we expanded our focus to leaked and stolen credential intelligence. We leveraged Pentera’s Credential Exposure module, which taps into info-stealer feeds. This data is tested against the organization credentials in the Active Directory on the inside and the web app interfaces from the outside. The goal is to prevent account takeover (ATO), protect identities, and neutralize possible abuse of stolen credentials and compromised data from the dark web.

The results were sobering. Our tests uncovered dozens of compromised credentials floating around dark web marketplaces - some exact matches, others close enough that any password-cracking engine could easily extrapolate them. It was like finding holes in the fence and realizing some of the herd had already wandered too close to danger.

The most shocking discovery? We found the CEO's password available to grab in the data. It was partially based on his hometown in Minnesota ("Duluth123!") and cracked faster than a goat can leap a fence. It was both a wake-up call and a great teachable moment for my team, who immediately reset his password.

We took swift action around all other leaked credentials. All compromised credentials were reset, and our corporate policy hardened, including updating our password policy to prevent personal details from being used in employee credentials moving forward. We also tightened-up our MFA enforcement using OneLogin, reducing the session duration to a 24-hour cycle. The goal was to close gaps and make it as tough as we could for attackers to exploit our stolen data.

Our employees weren't happy with these changes, to say the least. We had to hold a company-wide meeting to explain the rationale behind the MFA. With the CEO and CIO backing us up, we explained that leaked credentials were actually one of the reasons for the breach we encountered. That's why, moving forward, we all have to tighten the reins on our passwords, so to speak.

We're at such a better place after this week. We have stronger defenses and better visibility into identity risks. The integration of threat intelligence has helped us make better use of our data and challenge our defenses more effectively.

Next week, we'll tackle ransomware resiliency. But for now, I'm feeling good about my herd's security posture (I may even get some sleep over the weekend, hopefully alert-free!)



Make sure you don't leave out threat intelligence when it comes to adopting the CTEM framework. Use it to drive real-time detection, and test-challenge credentials in use.

Tip of The Week

Week Nine

Grow Ransomware Resiliency



When it comes to cyber threats, the top three priorities are:

Priority 1 - Ransomware Priority 2 - Ransomware Priority 3 - Ransomware

Ransomware poses a unique threat because it cripples operations quickly. By the time you detect and respond, the damage may have already been done. Grazing, Inc. lost millions from our recent ransomware breach. It led to downtime, lost customer data, long recovery process, extensive customer support efforts, and damage to our reputation. Let's just say that ransomware is now top of mind at Grazing, Inc.

Ransomware isn't a single event. It's a kill chain with multiple stages where we can intervene. A typical ransomware attack unfolds like this:

- 01 Initial Access -**
Entry via phishing, exploits, or compromised credentials
- 02 Execution -**
Malware is downloaded, deployed, and executed
- 03 Privilege Escalation -**
Attackers gain higher-level access

- 04 **Lateral Movement -**
Spread across systems and networks
- 05 **Data Exfiltration -**
Sensitive data is stolen (optional double extortion)
- 06 **Encryption -**
Files are encrypted, rendering them inaccessible
- 07 **Extortion -**
Ransom note demands payment for decryption keys or to prevent data leaks

We focused this past week on testing the seven kill chain stages by conducting multiple purple team exercises. The outsourced SOC team was in the loop, tracking Indicators of Compromise (IOCs) produced by Pentera's ransomware emulation. We ran tests in controlled environments, gradually increasing the stealth settings to test the SIEM's ability to detect more advanced techniques.

The latest evasion techniques, such as those used by LockBit3, were a big focus. We also tested against fileless attacks, like Emotet, which avoid traditional signature-based detection. Pentera's emulation of these scenarios was thrilling to watch.

One thing that stood out was how much tuning was required. Initially, the SIEM was too selective, flagging obvious attack patterns but letting some stealthier ones slip through. By the end of the week, we had adjusted thresholds and improved detection rules to catch both the obvious and the subtle.

We also validated our ability to isolate infected systems quickly and practiced our incident response playbooks. I'll admit it felt good seeing the team respond with precision and confidence. But we're not done yet. Ransomware variants evolve constantly, and Pentera's library of attack scenarios updates regularly. We need to keep running these exercises and expanding to more environments to stay sharp.

The week ended on a high note. We blocked and tackled most scenarios successfully, and the team celebrated with a well-deserved happy hour. Nothing like a toast to resilience.

Off for yet another weekend filled with family, friends, and some well-deserved rest.



**Ransomware is a kill chain, not a switch.
Test every stage of the attack path
regularly, tune your detection systems,
and remediate controls that can stop
the kill chain mid stride.**

Tip of The Week

Week Ten

Educate Users (Even the Stubborn Ones)



This week, we tackled what I consider the trickiest vulnerability of all - our employees. No matter how many controls and technologies we put in place, a single click on a phishing email can unravel everything. Given that our latest breach began with this exact scenario, we knew we could not discount the human factor in our CTEM strategy.

We rolled out a structured security awareness program using KnowBe4™ and a training platform. The modules covered phishing recognition, password hygiene, and safe browsing practices. Admittedly, it wasn't all smooth sailing. There was some pushback, especially from the "I've worked here 20 years and never clicked anything suspicious" crowd. There'll always be resistance to change, as I've mentioned before, but in this case everyone in your organization is on security duty. I made it clear to our employees that they must take our security training seriously and come to me with any suspicious emails or links.

To drive the point home, I hung posters in every hallway and breakroom. My personal favorite read: "Don't Let Hackers Graze in Your Digital Pasture." Subtle? Maybe not. Effective? Absolutely.

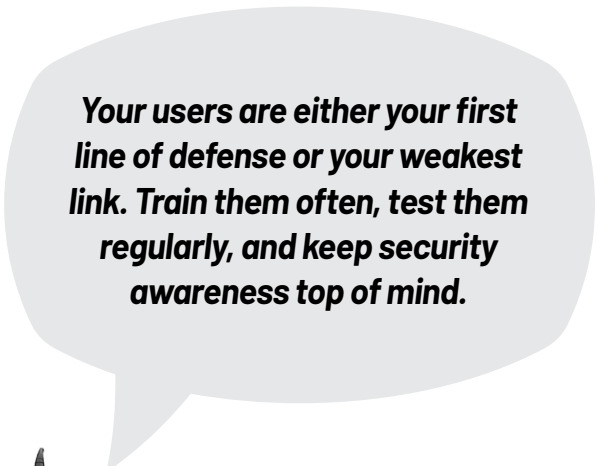
By midweek, the results started to show. Early tests revealed a 27% click rate on simulated phishing emails. By Friday, after multiple training sessions and discussions, we brought that number down to 12%. Not perfect, but a significant improvement- and a step closer to building a culture of awareness. We even used the phished credentials found in the automated tests we ran with Pentera. This way, we were able to gauge the user-persona risk of what the phished identities were. Luckily, the blast radius was not large and nowhere near our critical assets.

However, we didn't stop there. To measure progress, we commissioned a second external manual penetration test to see how far we'd come. The first test we did during my second week on the job had left us humbled. It exposed low-hanging fruit that attackers could exploit easily. This time our pentesters came back with fewer achievements to flaunt. The smiles on their faces weren't as big, and that was the best compliment we could ask for.

One highlight from the test was seeing the impact of our new MFA policies. Even when testers socially engineered stolen credentials, the extra authentication layers shut them down cold.

While we made great strides, I know this is just the beginning. Cybersecurity education isn't a one-and-done effort. People forget, newbies join the company, and attackers evolve. That's why we've committed to a bi-annual refresher training course and quarterly phishing simulations within the organization.

This weekend, I'm gonna be sure to speak to my kids about cybersecurity awareness. It's never too early.



Your users are either your first line of defense or your weakest link. Train them often, test them regularly, and keep security awareness top of mind.



Tip of The Week

Week Eleven

Present a Grassroot Plan and Budget to the Board



This week was all about securing the resources to keep our organization safe. I had to make the case for our cybersecurity roadmap, covering everything from ransomware prevention to damage control, while convincing the board to back it up with the budget we needed.

I started by presenting the plan privately to the CIO. A boss is a boss, and I needed her buy-in before going any further. She asked challenging questions, pushed back on a few numbers, but overall, she appreciated the direction we took.

With her feedback in hand, I adjusted a few slides and presented them to the CEO the next day. He was impressed but wanted us to validate the plan with a couple of board members before the official board meeting. I was glad for the opportunity to prepare for the big day.

Then came the day for the big meeting with all 12 board members. It felt a little cinematic, me being the 13th goat in the room on a Friday. The stakes were high, but so was my preparation.

I laid out the current state, benchmarks for acceptable risk, and a multi-year plan focused on ransomware prevention and rapid recovery. I emphasized unification and standardization across our 82 production facilities, because a fence is only as strong as its weakest board (pun-intended).

The budget included headcount, technology investments, and milestones I aimed to hit after an initial stabilization period. I made sure to frame the numbers with industry benchmarks, showing that companies our size [invest more in cybersecurity](#) (\$1.27M a year), and it was time we did too.

It was clear from Pentera's posture-over-time graphs that our progress had been tremendous. One of my key exhibits was a comparison of the two penetration tests we ran over the course of these 11 weeks. As a result of those visual benchmarks, the board felt confident that the investment would be successful.

I prepared an [ROI analysis](#) in collaboration with Pentera's customer success team to strengthen the case. In addition to reduced risk costs, it also highlighted savings on third-party expenses and cyber insurance and increased productivity through improved testing frequency and coverage. Armis and Wiz were also positioned as table stakes so that we could move forward safely.

At the end of the presentation, I tied everything back to the breach. I reminded the board that protecting Grazing, Inc isn't just about avoiding costs – it's about safeguarding our reputation and keeping operations going.

The board didn't ask too many questions, which I took as a good sign. I left the room before the final decision was made.

Later that day, my CIO pulled me aside with a smile. "Congratulations, Gary," she said. "You got the check you were hoping for."

My wife and I are celebrating the news together. Feeling GOAT-tastic!

When presenting to executives, show data, benchmarks, and ROI to make the case. A clear story supported by metrics is hard to dismiss.



Tip of The Week

Week Twelve

Establishing the CTEM Program



Exactly 12 weeks after I started, we've achieved our goal! A Continuous Threat Exposure Management (CTEM) program has been implemented at Grazing, Inc. This isn't just a framework but a roadmap for resilience. The journey to this moment was full of challenges, late nights, and vulnerability.

At the core of the program is structure. Here's what we've built:

01 Asset Inventory and Classification

- Now we know exactly what we're defending, down to the last endpoint, server, and cloud instance. Our asset map no longer serves as a guess but instead serves as a source of truth.

02 Ten Security Validation Use Cases

- Ransomware Emulation: Testing defenses against the most dangerous threats.
- Web Application Testing: Validating external and internal app security.
- Vulnerability Assessments: Prioritizing fixes based on exploitability.
- Configuration Reviews: Ensuring systems stay hardened over time.
- Red Team Exercises: Simulating adversary behavior to test responses.
- Access Control & Privilege Audits: Mapping blast radius for identity attacks.
- Network Segmentation Testing: Confirming segmentation blocks lateral movement.
- EDR Validation: Making sure endpoint defenses fire when needed.
- Patch and Update Management Validation: Verifying that patches close gaps.
- Backup and Recovery Validation: Testing the last line of defense.

03 Annual Audit Schedule

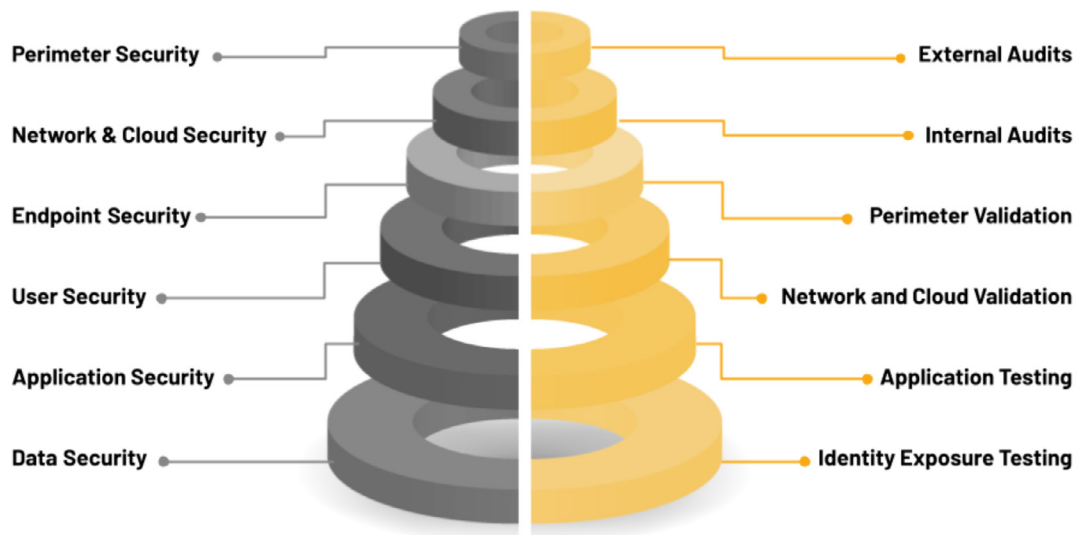
- Annual Penetration Testing: External experts validate our security controls.
- Third-Party Risk Assessments: Vendors and partners don't get a free pass.
- Policy and Compliance Audits: Staying in check with regulations and standards.
- Backup and Recovery Validation: Ensuring we can bounce back fast if disaster strikes.

04 Ongoing Employee Training

- Bi-Annual Phishing and Social Engineering Simulations: Keeping the herd sharp.
- Annual Online Training Refreshers: Reinforcing awareness and habits.

Defense in depth - sure!

...And CTEM, well - that's "Validation in Depth!"



The best part of all? It's continuous. As a result of automation and scheduled testing, we're proactively maintaining hygiene across our IT estate instead of just reacting to incidents. Think of your IT as a Japanese garden, where every detail is trimmed, tended, and ready for whatever a malicious actor might do.

Seeing how far we've come makes me proud. Twelve weeks ago, we were in the process of recovering from a breach. With today's CTEM program in place, we are not just protecting our organization, but also setting ourselves up for success.

This weekend, I think I'm planning a long, long family vacation. Maybe Thailand?



Cybersecurity isn't a destination; it's a journey. Build processes that evolve, validate continuously, and never stop improving.

Tip of The Week

Closing Note



These have been an intense 90 days. Twelve weeks ago, I wrote here that I'd lean into this journey and be proactive about it. And I truly have.

I don't mean to gloat (or goat), but my colleagues tell me my last name Grit suits me, congratulating me on my team's achievements. And as part of our security stack, we've already cleared the path for Armis, Wiz, and Pentera to be implemented.

Here's hoping I helped Grazing, Inc make a turn for the better and distance itself from yet another ransomware attack. I am grateful for the trust my management and team place in me. I still have a lot to do, but my 90-day diary ends here with my motto: Be proactive.

And for those of you whom I have reached out to - I strongly encourage you to develop your own CTEM program and to be sure that your entire security infrastructure is constantly validated. Even in the presence of wolves, that's how you keep your herd safe.

Baaaaahhhhye!

Gary Grit 🐐

Backstory

Pentera’s “Diary of a Cyber GOAT” guide is a fictional story inspired by real-world experiences from our customers’ CISOs. Each element in the diary reflects a chapter from the journeys we’ve shared with these cybersecurity leaders. Our mission is to collaborate with enterprise cyber professionals to improve their readiness against modern cyber threats and help them reduce their exposure.

Trademark Disclaimer

All company names, trademarks, and registered trademarks mentioned in this article are the property of their respective owners, and are used for descriptive or informational purposes only. Their inclusion does not imply any affiliation with or endorsement by them.

Copyright ©2025 Pentera. All rights reserved.

This document is the property of Pentera and is protected under copyright law. Unauthorized reproduction, distribution, or use of this material is strictly prohibited. For permissions or inquiries, please contact Pentera.

Thanks to our Contributors

We would like to extend our heartfelt thanks to [Zach Lewis](#) and [Shawn Baird](#) for their invaluable contributions to this guide. Your deep cybersecurity expertise, hands-on experience, and thoughtful feedback were instrumental in refining this guide. Your support has been essential in ensuring its accuracy and relevance—thank you for keeping us on track and helping us deliver something truly impactful.

Thank You!

Appendix



Don't Assume. Validate. Because tested security is trusted security

Pentera is the market leader in Automated Security Validation, empowering companies to proactively test all their cybersecurity controls against the latest cyberattacks. Pentera identifies true risk across the entire attack surface, prioritizing and guiding remediation to effectively reduce exposure. Pentera's security validation platform is essential for Continuous Threat Exposure Management (CTEM) operations.

Key aspects of Pentera's exposure management approach include:

- **Automated Attacks:** Conduct continuous penetration testing across the entire attack surface, mimicking attacker techniques to identify exploitable vulnerabilities and misconfigurations in your security defenses.
- **Prioritize based on real risk:** Score the vulnerabilities based on their exploitability and potential business impact, so you can focus resources on the most critical exposures. Provide relevant teams with clear recommendations for effective mitigation.
- **Comprehensive attack surface mapping:** Get full visibility of external and internal assets to uncover blind spots across your networks, endpoints, and cloud environments.
- **Integration with security ecosystem:** Seamlessly integrate Pentera with your existing security tools to streamline workflows, enhance remediation efforts, and automate vulnerability management processes.

Pentera's approach ensures organizations can proactively manage their exposure, minimize risks, and strengthen their defenses against active cyber threats.

For more information: [Pentera.io](https://pentera.io)



Armis, the cyber exposure management & security company, empowers organizations by operationalizing CTEM with Armis Centrix™, a platform that sees, protects and manages ALL assets from the ground to the cloud. By assessing an organization's entire attack surface, Armis provides a comprehensive view of all assets, both managed and unmanaged, physical and virtual, helping organizations understand their cyber exposure and prioritize what needs attention based on potential business impact.

Through AI-powered automation, Armis streamlines the vulnerability remediation lifecycle, by identifying, prioritizing and fixing security issues efficiently within existing organizational frameworks. Armis' unique early warning intelligence also allows organizations to act proactively, reducing risk before they turn into attacks. By offering unmatched visibility, security, and control, Armis enables organizations to effectively manage their attack surface, address risks, and respond to threats in real time and continues to provide the most comprehensive platform for enabling and operationalizing CTEM programs.

For more information: armis.com



Wiz is a cloud security company that enables organizations to rapidly identify and remove critical risks in their cloud environments. Wiz CNAPP is the platform to secure your cloud from code to runtime. Transform your cloud security operating model with a single platform that enables collaboration between developers and security. Founded in 2020, Wiz has become the fastest-growing software company globally, serving hundreds of organizations worldwide, including over 45% of the Fortune 100. For more information, visit wiz.io.



Recorded Future, a subsidiary of Mastercard, is the world's largest threat intelligence company. Its Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. By indexing the internet across the open web, dark web, and technical sources, Recorded Future offers real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward.

For more information, visit recordedfuture.com