The Guide for

Stress Less Cybersecurity

for Lean IT Security Teams

Learn

- Why stress-less security isn't about the size of your team, but how you deploy it.
- The SIX Key Components to a successful stress-less security strategy.
- How you can stay ahead of cyber attackers without straining your team.
- Why the constraints of the past can be turned into advantages for lean security teams.

The State of Cybersecurity

Lean IT security teams have plenty to be alarmed about. The most sophisticated, aggressive, and destructive cyber attacks in history have all occurred in recent years, claiming major corporations and government agencies alike as victims. If the most elite security teams in the world can't stop these attacks, what hope is there for everyone else?

More than you think! Recent history proves that the size of the security team matters less than the strategy it deploys. Having the right tools and tactics are what's important – not a giant staff or massive budget.

In reality, lean security teams have never been stronger. A new generation of cyber defenses levels the playing field and makes stress-free cybersecurity attainable for any organization.

To understand how drastically things have changed for the better, it helps to compare the constraints of the past with the capabilities of the present. This ebook makes one thing clear: lean security teams ARE NOT at a disadvantage any more.

The six components of stress-free cybersecurity

Prevention

Stopping attacks before they start

Always Behind the 8 Ball

Prevention has always been the goal of cybersecurity, but that proved elusive for the lean security teams of the past for several reasons:

- Zero day attacks and emerging threats couldn't be detected by signature-based technologies that had never seen them before.
- Security technologies required constant updates to stay ahead of attacks, which was a time and labor-intensive undertaking that often went neglected.
- Prevention was about seeing a threat early and stopping it immediately. Even when the first succeeded, the second often failed.

Proactive Protection

Today's lean security teams are well-equipped to prevent attacks long before they cause any damage whatsoever:

- NGAV offers powerful protection against ransomware, phishing attacks, fileless exploits, supply chain attacks, and many more.
- Enhanced visibility reveals attacks on the horizon, along with the most effective, efficient, and expedient way to address specific attacks.
- Automation can be used to identify red flags sooner and more consistently than any number of security professionals doing the same thing.

Detection

Identifying the earliest evidence of attack

Raising the Alarm Too Late

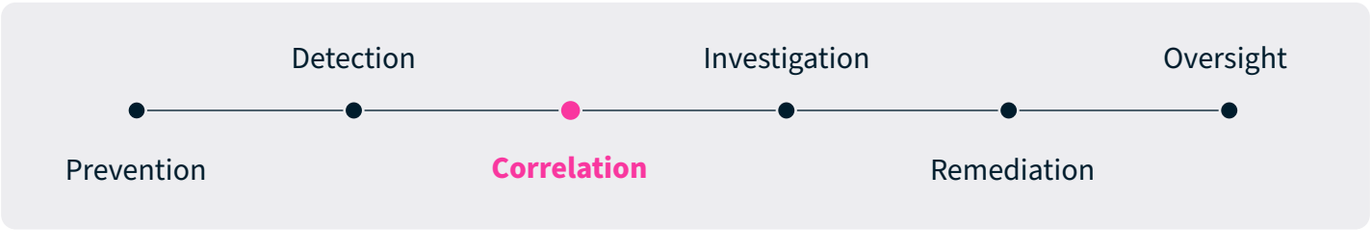
When lean security teams from an earlier era managed to detect threats at all, the warning signs were often overdue and incomplete. Here's why:

- Understaffed teams lacked the people power to monitor every single attack vector at all times.
- Evasive attacks used sophisticated technical and psychological tactics to obscure their malicious intent, leading to attacks that went unnoticed for days, weeks, or months on end.
- Improving detection policies and protocols required more expensive technology and ever- evolving threat intelligence that was difficult to collect and laborious to act upon.

Catching Anything and Everything

Impending attacks are now apparent with tools that scour the threat landscape in 360 degrees and sound the alarm only when something requires attention and intervention:

- EDR and NDR technologies monitor the full depth and breadth of the attack surface 24/7.
- Managed detection and response (MDR) providers supplement lean security teams with expertise and oversight they wouldn't have otherwise.
- Detections that have very few false alarms liberates lean security teams to focus on what matters instead of wasting resources on what doesn't.



Correlation

Comparing signals to gather threat intelligence

Losing the Signal Through the Noise

Correlating signals to anticipate and understand attacks has long been a thorn in the side of lean security teams for the following reasons:

- Older technologies could not gather signals from all relevant sources – files, users, networks, and hosts – leaving large blind-spots in the attack surface and adding technology was beyond budget limitations.
- An overwhelming number of signals exceeded what security teams of any size could analyze fast enough to stop attacks. Endless false alarms only obscured the view even further.
- Other security obligations made it difficult for lean teams to invest the time and focus necessary to correlate signals, meaning many attacks arrived by complete surprise and compounded their damage as a result.

Superior Security Analytics

Developing threat intelligence has never been easier thanks to technological advances that make correlation almost effortless:

- Extended detection and response (XDR) improves upon previous capabilities by offering full visibility into multiple points of telemetry. Nothing escapes scrutiny.
- Monitoring technologies handle the heavy lifting of correlation – identifying, integrating, and analyzing signals – instead of putting this burden on the security team.
- Security analytics transforms correlation into actionable intelligence that guides where, when, why, and how the security team responds for maximum effect.

The six components of stress-free cybersecurity

Investigation

Understanding the nature of attacks

Lost in the Dark

Minimizing attack damage and preventing a repeat offensive requires an in-depth investigation into what happened. Historically, that was tough for lean teams:

- Limited visibility into networks, endpoints, and elsewhere made it hard to collect evidence and develop a complete picture of what happened.
- Scrambling to restore the status quo left little time and resources to conduct a thorough investigation. Many problems got “solved” without being fully understood.
- Lean teams often lacked the diverse technical expertise and investigative experience to get to the bottom of what went wrong.

The Sherlock Holmes of Cybersecurity

Modern security teams don’t have to conduct investigations with new approaches that automate, optimize, and outsource how the clues are gathered.

- Integrated capabilities for endpoint detection and response, user behavioral analytics rules, network detection rules, and file analysis bring the scene of the crime into full view.
- Automated investigation technologies can be used to determine the root cause of a threat, identify the full scope of the attack and then remediate all attack components – all done in minutes without any human intervention.
- MDR service providers can serve as a cyber SWAT team: A kind of frontline SOC that lean security teams can rely on to immediately investigate attacks, rank risks, prioritize next steps, and coordinate remediation.

Remediation

Neutralizing attacks and mitigating the damage

A Bad Situation Gets Worse

The cost and duration of cyber attacks has grown worse every year because security teams, especially the lean ones, have faced recurring obstacles to fast, effective remediation:

- Struggles at the detection and correlation levels caused some attacks to go unnoticed until after the worst damage had been done, making them the hardest to remove and remediate. The rise of ransomware is the prime example.
- Rushed investigations and partial visibility led to an incomplete understanding of the attack, which in turn led to a drawn out remediation effort with incomplete or uncertain results.
- In an all-hands-on-deck scenario, lean security teams were constrained by the number of people and the depth of expertise they could direct at the problem, which often required significant manual intervention.

A Defense That Eclipses the Offense

For today's lean security teams, it's realistic to expect to block most attacks, stop those that evade the initial defenses, and neutralize any that reach their final target:

- Automated remediation tools following customized playbooks apply an immediate solution to the problem and leap into action without needing manual intervention from the security team.
- Threat intelligence based on the most complete, current, and accurate data available makes it clear what remediation entails, and then makes it quick to execute customized counter measures.
- The backing of an on-demand MDR provider ensures that the remediation effort has whatever resources it requires: experience, expertise, intelligence, extra people, or otherwise.

The six components of stress-free cybersecurity

Oversight

Monitoring and managing security systematically

A Shortsighted View of Cybersecurity

Operating without complete oversight into everything happening inside and around the IT infrastructure is perhaps the oldest problem facing lean security teams:

- Disconnected technologies led to a fractured understanding of cybersecurity, both the threats at hand and the defenses in play. A siloed approach only made everything else more difficult and less effective.
- Many advanced threats escaped the view of last-generation monitoring technologies, making the most dangerous attacks the hardest to see.
- Without integrated tools to enable oversight, teams with limited security staff struggled to get the complete picture. Information gaps and security lapses were the standard.

Complete Visibility, Automatically

Multi-layered security solutions empower lean security teams to see everything at once so that security activities proceed with a complete understanding of the situation at hand:

- Platforms such as XDR with integrated technologies can provide a broad and deep perspective into all corners of the attack surface, collected onto one platform for top-down oversight.
- MDR providers round out the capabilities that lean security teams bring to the table so that no team is understaffed, outclassed, or incomplete in any way.
- Tools built with an emphasis on the user experience upgrade what oversight looks like by highlighting urgent alerts, presenting information organically, and streamlining access to everything.

A New Context for Lean Security Teams

The term “lean” tends to be a pejorative, describing everything the security team doesn’t have: staff, expertise, disposable budget, advanced capabilities, etc. At least, it did in the past. Thanks to advances in cybersecurity tools – and the techniques and tactics they employ – it’s time to rethink what it means to be lean.

Lean does not mean lacking any longer. On the contrary, lean now refers to security teams that are unencumbered by exhaustive manual workloads, strained visibility, and frantic remediation efforts. Instead of being defined by the capabilities they’re missing, they’re defined by the obstacles, obligations, and inefficiencies they avoid.

From here forward, lean security teams will be known for athleticism in the face of attacks. Informed by exceptional threat intelligence, aided by automation, and backed by a series of smart defenses, lean teams are perfectly-equipped to stay agile when up against anything. Larger security teams may not have that luxury for the simple fact that larger ships are harder to steer.

In the age of XDR, security teams will strive to go lean. Why rely on oversized teams and bloated budgets when it’s possible to do a lot with a little? Lean teams only need one addition to solidify their advantage: the right cybersecurity platform.

The Era of Stress-Free Cybersecurity Has Begun

Make no mistake, cybersecurity will always be stressful, and the defenses will never be ironclad. Expecting otherwise would be a dangerous mistake. That being said, cybersecurity doesn't have to be stressful in the way it was before.

As the preceding pages make clear, yesterday's lean security teams faced immense pressure to defend their tech stack from towering threats using an incomplete toolkit at best. It was a classic David vs. Goliath scenario – but rarely did the underdog win. Stress over when an attack would arrive and how much damage it would cause was constant, and at times crippling.

Not anymore. Security teams must remain on guard, of course, but they don't need to feel overwhelmed or outgunned. With a suite of integrated cybersecurity solutions working in concert to illuminate threats, automate defenses, and optimize outcomes, defending an organization no longer feels like a losing battle. Even the smallest teams are up to the challenge.

The era of stress-free cybersecurity begins now. Lean security teams can focus all their time, attention, and resources where they matter with the backing of tools that handle the most consuming and complex aspects of cybersecurity. Stress-free cybersecurity is about maintaining the advantage – not about making up ground.

Cynet – Pioneering Stress-Free Cybersecurity

Built for lean security teams, Cynet XDR combines mission-critical capabilities onto a single unified platform. The fundamentals of cybersecurity – preventing, detecting, investigating, remediating – have never been easier or required less in terms of time, staff, and budget.

Cynet XDR encompassing EDR, NGAV, NDR, UBA Rules and Deception technologies provides comprehensive breach protection on one platform. When combined with an all-seeing Incident Engine that automates investigation and remediation, plus a leading 24/7 MDR provider, Cynet's platform represents a complete solution for cybersecurity. You can rest assured that all the pieces are in place.

Learn More