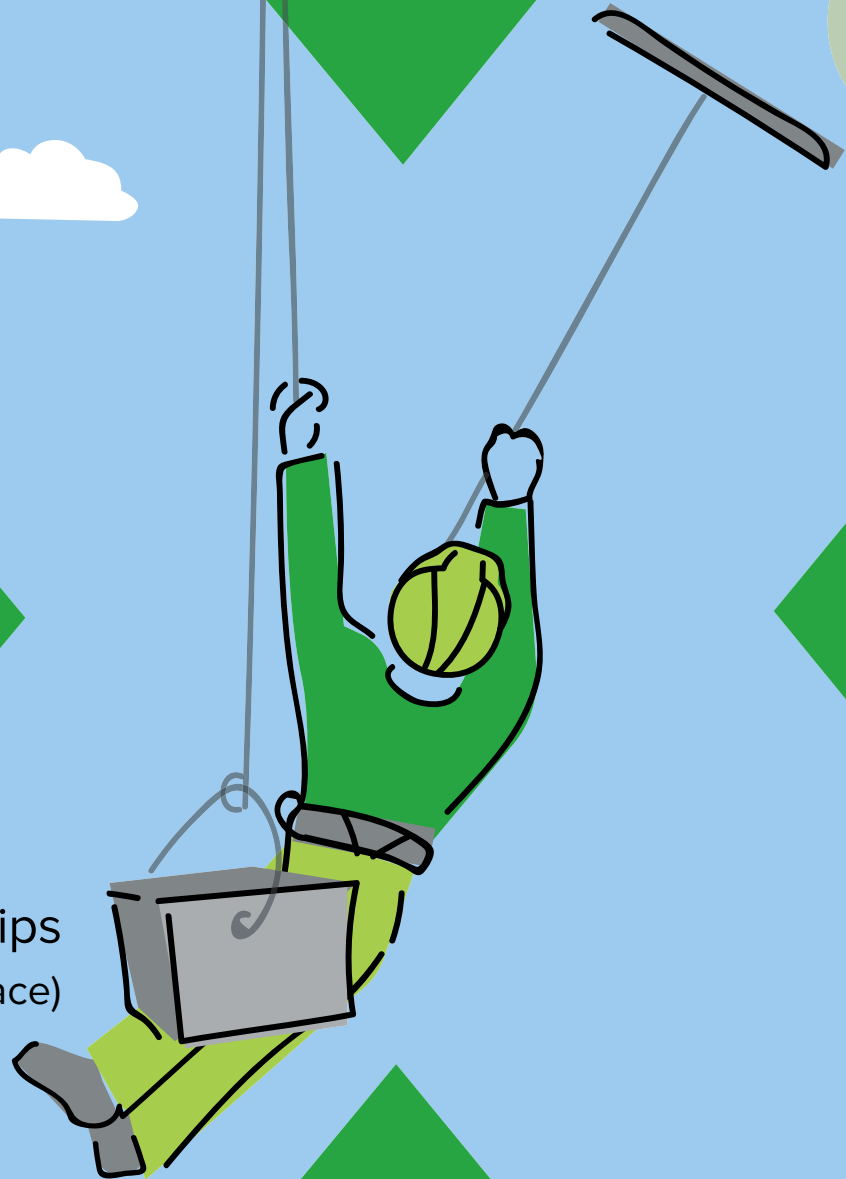


# The transparent managed security handbook

An antidote for failed MSSP relationships  
(and a way to avoid the frustration in the first place)



# About the handbook

At Expel, we're radically transparent — not just with how our service works but also with the way we do business. We hope that's immediately observable.

Whether you recently found us or you're a long-time customer, we're focused on making your experience orders of magnitude better than anything you may have experienced before in the security industry.

That's why we created this handbook. We think it's important that you understand our perspective on what transparent managed security is, how it compares to other approaches and the role it can play in helping you improve your security.

If you've got questions or think there's something we missed let us know.

# What's inside?

**Part 1:** Why are we still doing this? ..... 4

**Part 2:** What's so great about transparency? ..... 9

**Part 3:** Plot yourself on the security operations spectrum ..... 16

**Part 4:** Navigating the confusing managed security services landscape ..... 22

**Part 5:** Eight questions to ask managed security service providers ..... 28

Additional resources ..... 31

## **Part 1:**

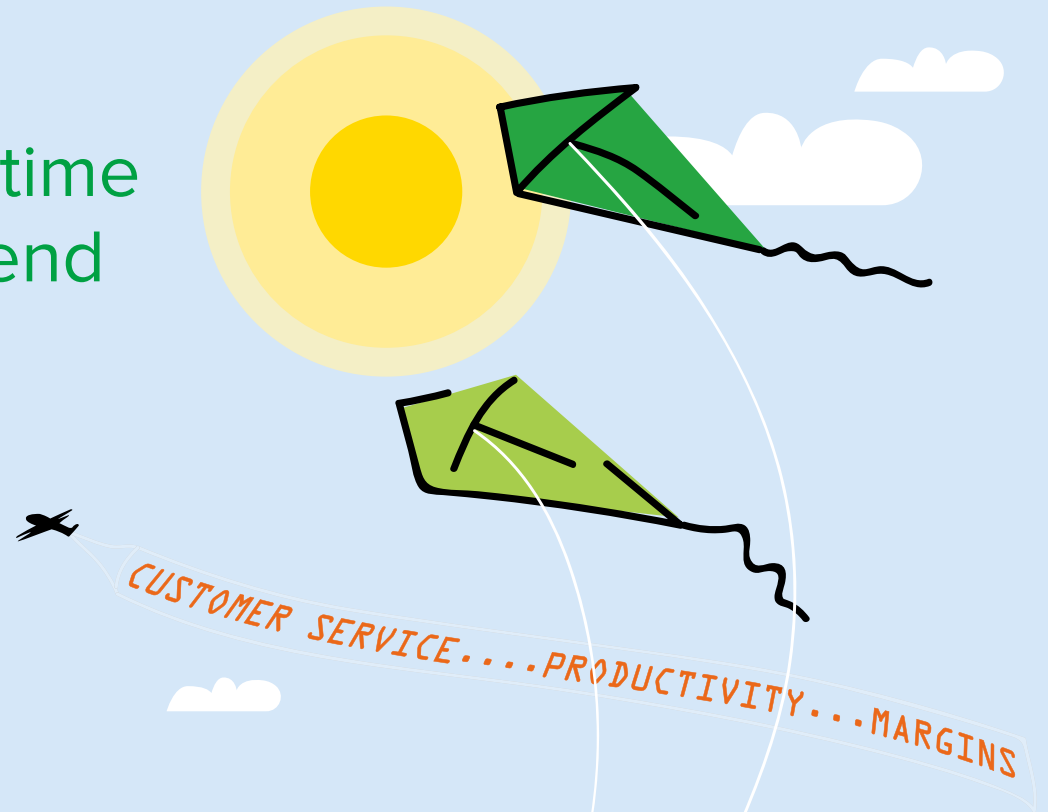
Why are we still doing this?

# Today's IT doesn't spend time racking servers... they spend time delivering value

If you're a CIO today, there's a bunch of stuff you used to do back in 2005 or 2007 that you don't have to do anymore. Pulling cables through data centers, wiring up production servers, swapping broken hard drives or managing cooling and electricity in your racks are just a few that come to mind.

Cloud services like Amazon Web Services, Microsoft Azure and Digital Ocean do that for you (probably way better than you can).

**Today, CIOs spend time close to where IT delivers value: with customers and business owners.**



# It's 2020! Why are grown security professionals still chasing alerts and wrestling with products?

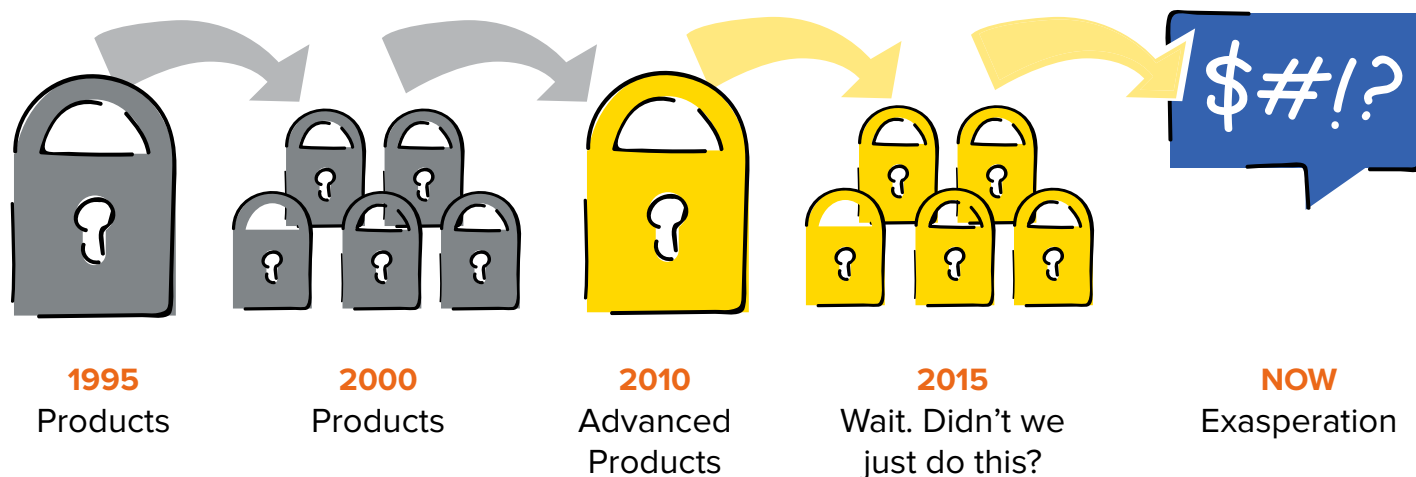
It's a good question. The poor CISO is still mostly stuck in the security equivalent of pulling cables, and swapping hard drives. Their world hasn't transformed in the same way it did on the IT side of the house. How come?

Well... for every problem over the last 20+ years it seems like there has been a new product. Then more products. Then advanced products.

Now we're drowning in a sea of products that generate alerts or (only slightly better) a managed service that repackages those alerts and deposits them back on your doorstep.

Either way, if you're in security, most of your day is spent looking at all of those alerts, trying to figure out what they mean... and probably buying more products to wire different alerts together to try to get to some outcome that actually delivers some value to the business.

## A brief history of security...



# What we believe



CISOs shouldn't spend energy wrestling with products and massaging alerts... they should pick their tech and then spend their time making decisions, and managing risks

# It's time to replace alerts with answers

We think a CISO's time is best spent making decisions and managing risk. They should be right up there with the CIO delivering tangible value... not mired in the crank-turning world of churning through alerts.

We created Expel to replace alerts with answers. If we do our job right, those answers should create space for you to do what you love about security (even if that's thinking about it as little as possible).



## From alerts... to answers

### What happened

Answers, written in plain English, that tell you exactly what happened, when and where it happened and how we detected it

### How to fix it

Immediate actions you should take to resolve the incident and/or reduce the risk

### How to improve

Recommended actions to improve your resilience and address the root cause of recurring issues



## **Part 2:**

What's so great about transparency?

# Have you ever noticed how much effort security vendors put into not being transparent?

Nobody intentionally opens a sales pitch by saying “I’m going to lie to you and hide things.” But that’s how too many relationships start between security vendors and end users. Just read a few of the exaggerated marketing claims in the vendor emails that swamp our inboxes.

The worse offense — at least in our opinion — is when that lack of openness carries through to the customer-vendor relationship after the ink is dry on the contract.

Sure, it’s important to make sure the bad guys don’t know exactly how the good guys are finding them. But when a product vendor or managed service provider finds something bad, their customers deserve to know exactly how they found it.

We don’t think that happens enough.

“ Purpose-built for security, [vendor’s products\*] detect and stop attacks these traditional security products miss and empower you to rapidly respond to threats in near real-time.

“ [vendor name\*] stops modern threats that make it past the perimeter. It solves the problem of alert fatigue...



\* Vendor names withheld to protect their identities

# trans·par·ent

## trăns-pâr 'ənt

### Adjective

1. Capable of transmitting light so that objects or images can be seen as if there were no intervening material.
2. So fine in texture that it can be seen through; sheer.
3. Easily seen through or detected; obvious: transparent lies.
4. Free from guile; candid or open: transparent sincerity.
5. Open to public scrutiny; not hidden or proprietary: transparent financial records.

Source: The American Heritage Dictionary of the English Language

# Transparency tears open the black box that MSSPs have hidden in for too long

In our hold-your-cards-close-to-your-chest industry, transparency is a pretty radical concept. But we couldn't imagine running a business any other way. After all, when has hiding things ever made a relationship stronger?

The more we talk to customers it couldn't be clearer that the black-box approach most managed security services take is a passionate frustration point — especially when it comes time to renew and there's no way to quantify what value (if any) they've gotten from their MSSP.

Transparent managed security puts all of the cards on the table so you know exactly what we're doing for you and can draw a straight line from the money you're spending to the value you're getting.

**With transparent managed security customers can see anything (or everything) our analysts are doing 24x7. In fact, analysts and customers share the exact same interface.**



## How transparency works

See exactly what our analysts are doing 24x7

Drill down to see all the raw data from your app's

Collaborate with our analysts (if you want to)

Measure improvement and hold us accountable

# Transparency also enables you to work in a different way with your managed security partner

You'll hear a lot of managed services talk about how they are "an extension of your team". In reality, that usually means they're handing you a pile of alerts to sift through. Transparency allows you to work hand-in-hand with our analysts. You can even assign them work.



## Watch investigations as they unfold

You see exactly how our analysts are approaching each investigation including their rationale, methods and what they've discovered to date.



## Take action even as the remediation plan develops

Don't wait until the investigation is over to do something. When we identify a critical remediation step you can act immediately.



## Track improvement and hold us accountable

Detailed dashboards let you measure how well we're doing, quantify the improvement and see how and why you're getting better.

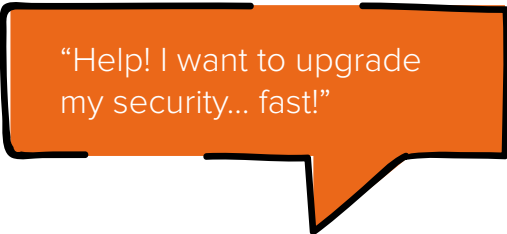
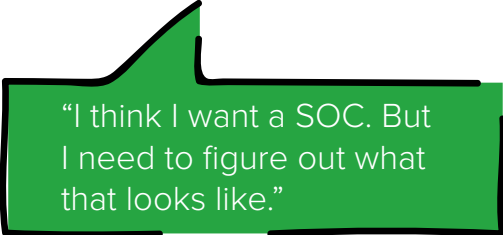



## Improve your resilience based on your own data

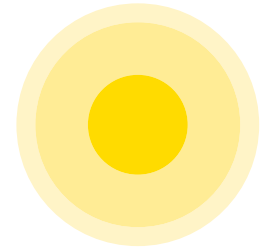
Use data from your own environment and past trends to prioritize actions and investments that can help you fix the root cause of recurring events or even prevent them from happening in the first place.

# Depending on your situation, transparency can help you in different ways

Transparency plays a different role depending on what stage you're at (and what your biggest risks and challenges are). Here's how transparency addresses three common growing pains security teams face as they grow from one, to five, to 50+ people.

	 <p>"Help! I want to upgrade my security... fast!"</p>	 <p>"I think I want a SOC. But I need to figure out what that looks like."</p>	 <p>"I have a SOC but we're mired in the minutiae."</p>
	<p><b>Rapid growth or a recent incident have spurred the need to upgrade security.</b></p>	<p><b>It's time to go to the next level. That means 24x7 monitoring and more mature processes.</b></p>	<p><b>You want to get more efficient but your best people are drowning in the day-to-day.</b></p>
<b>Common challenges</b>	<p>The security you want exceeds the budget and resources you have</p> <p>You can't find and retain the security experts you need</p>	<p>Adding 24x7 monitoring means a huge step up in people and processes</p> <p>Creating a SOC (or something like it) requires new tech to support it and new skillsets</p> <p>Growing into a SOC takes time and your needs will evolve even as you stand it up</p>	<p>Your tier-2 and -3 analysts are doing the work of tier-1 analysts...</p> <p>... that makes them frustrated. Add in a hot job market and you've got high employee turnover</p>
<b>How transparency helps</b>	<p>You get metrics that help you build a business case for the security products you already know you need but haven't been able to justify.</p>	<p>New analysts ramp faster and can work collaboratively with Expel analysts in the shared workspace as your SOC matures.</p>	<p>Confidently hand off tier-1 and tier-2 analyst work to Expel (and tier-3 when key staff goes on vacation) so your analysts can work on higher-value tasks. Transparency allows you to see exactly what the analysts are doing.</p>

# Transparency also makes it easier to talk to stakeholders who don't speak security



Security isn't core to most companies' cultures. And the inside-baseball security speak that security geeks use with each other doesn't help mere mortals understand what we're trying to say.

Since communicating is a key part of security, we believe it's our responsibility to equip you with the info you need to be transparent with your key stakeholders: the board, business owners, customers and suppliers.

That starts with facts, simple summaries, and recommendations written in plain English. If we've done our job right, keeping your key stakeholders up to date should be a cut-and-paste exercise.

## Everyday conversations become easier with transparency



## Part 3:

Plot yourself on the security operations spectrum



# You have security operations... even if you don't think you do

A security operations center (SOC) is a building. The stuff that goes on inside it is security operations. And you don't even need to have a SOC in order to be doing security operations activities.

In fact, we'd argue that everybody has security operations — whether it's deliberate or by accident.

Your security operations could be really sophisticated with an actual SOC facility complete with the fancy dark room, lots of desks and big screens.

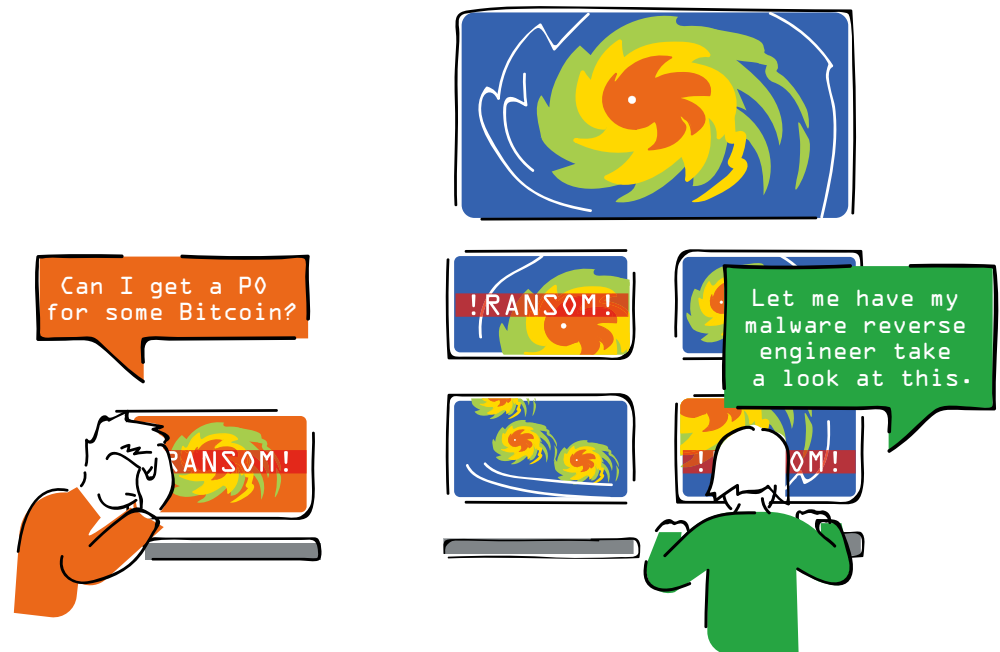
Or, maybe security operations is far simpler for you. Maybe it's even as simple as turning on the computer in the morning. Has ransomware has locked you out of the system? If yes, call CFO for ransom authorization. Pay it and get your data back.

Both are valid approaches to security operations. The next few pages help you understand where you're at and how you want to evolve your security operations program.

There's a wide spectrum when it comes to security operations programs

From simple...

To mature...

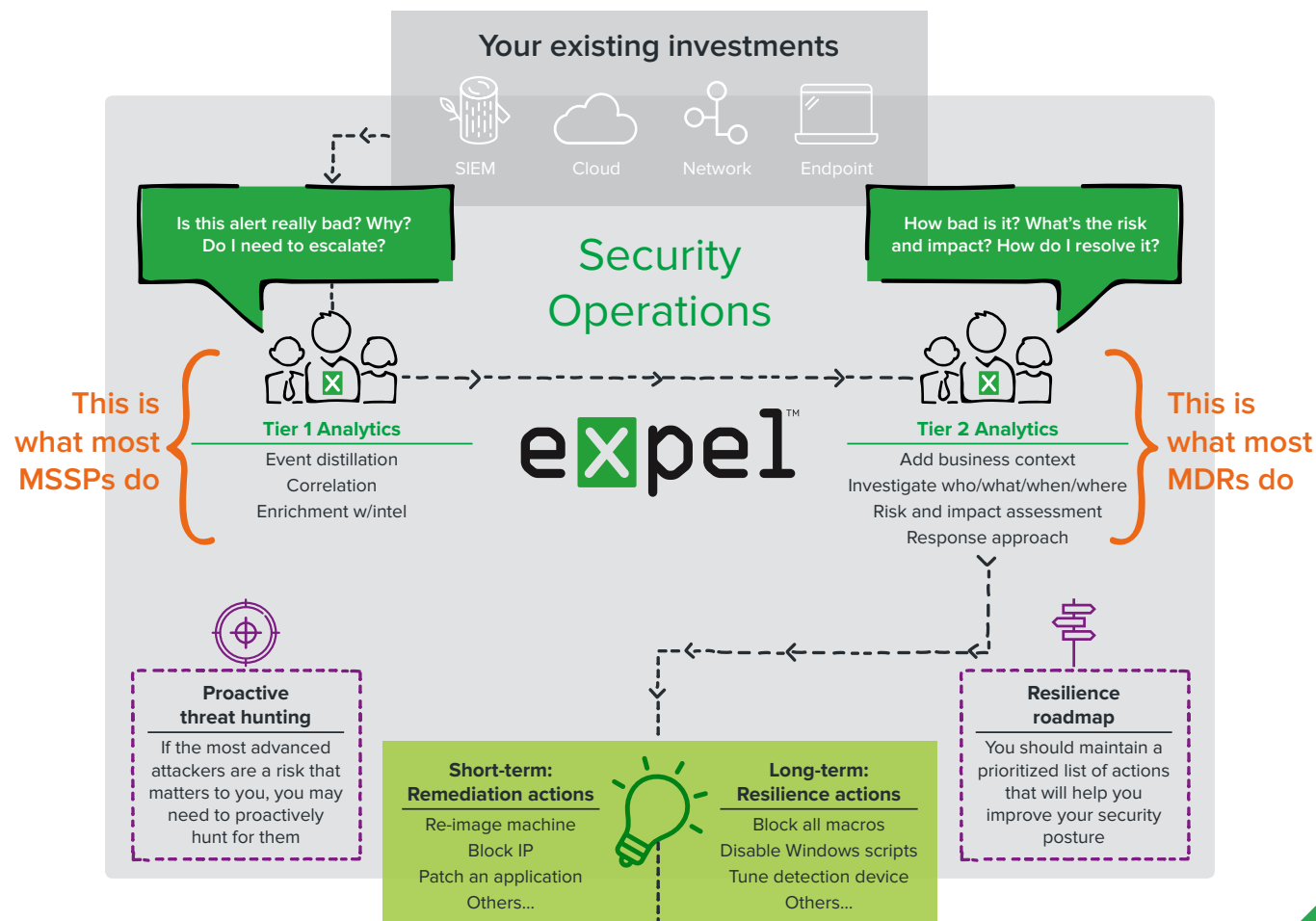


# What does a mature security operations program look like?

Let's start with the end state and work backwards. The core mission of security operations is to run the business so that it mitigates your key risks. If you don't know what your key risks are you should probably start there.

Those risks will guide how you monitor and respond to threats. Usually there are a couple flavors of analysis: Tier 1 is basically triaging and escalating alerts ("is it bad?") while Tier 2 focuses on investigating and developing a response plan ("how bad is it and what do I do?"). Well-resourced teams may also proactively hunt for threats.

The result of all of that work should be a set of short-term remediation actions to address immediate threats and longer-term resilience actions that help make you more secure over time.



# What we believe

#2

The core mission of security operations is to protect the business by mitigating the key risks you've identified

# Find where you fit on the security operations maturity spectrum



Chances are you're not doing everything in the picture on the previous page. That makes you normal. Heck... you may not even have a security team. The important thing is that you know where you are and where want to go as you evolve your security program. If you don't, chances are you'll end up buying and doing things that aren't the best use of your money and time.

## Security operations maturity model

	People	Process	Common Tech
<b>1. Getting Started</b>	There's no full-time security staff; security is managed by IT	<ul style="list-style-type: none"> <li>Processes aren't formally defined</li> <li>IT reacts to issues as they arise</li> </ul>	<ul style="list-style-type: none"> <li>Antivirus</li> <li>Firewalls</li> </ul>
<b>2. Committed</b>	You've got a CISO or a director of security and at least 1 person to work for him or her	<ul style="list-style-type: none"> <li>You've got policies in place; you're compliant; and you've started to test if your security controls are working</li> </ul>	<ul style="list-style-type: none"> <li>Adv malware detection</li> <li>Managed security services</li> </ul>
<b>3. Growing</b>	The team's grown to 5+ people — including a security operations manager	<ul style="list-style-type: none"> <li>You're starting to formalize roles and responsibilities including workflow and handoffs within the team and with IT</li> </ul>	<ul style="list-style-type: none"> <li>SIEM</li> <li>Endpoint detection and response (EDR)</li> <li>Managed security services</li> </ul>
<b>4. Getting SOCeY</b>	You've added Tier 1 and Tier 2 security analysts and defined an escalation process	<ul style="list-style-type: none"> <li>You're doing 24x7 monitoring, you've created playbooks and you're thinking seriously about a SOC if you don't already have one</li> </ul>	<ul style="list-style-type: none"> <li>Security analytics</li> <li>Network forensics</li> <li>Managed security services</li> </ul>
<b>5. Automating</b>	You've added a dedicated incident response and forensics team	<ul style="list-style-type: none"> <li>Your investments are focused on automating your processes and improving performance</li> <li>Hunting is someone's formal responsibility</li> </ul>	<ul style="list-style-type: none"> <li>Orchestration</li> <li>Security analytics</li> <li>Managed security services</li> </ul>



# Growing up is hard. But asking the right questions at each stage will smooth out the bumps

Moving up the maturity curve requires conscious choices and investments. Protip: keeping your staffing, processes and security tech in synch at each stage will prevent headaches. If they fall out of synch you'll likely find you've got nobody to look at the alerts your shiny new security appliance is spewing out. Or, conversely, you'll have a frustrated team that doesn't have the tools they need to do their job.

## Common challenges and questions to ask yourself at each stage of maturity

	Common challenges	Key questions and decision points
<b>1. Getting Started</b>	Complacency is the biggest hurdle here — especially if you've been lucky enough to avoid any serious security issues in the last year.	<ul style="list-style-type: none"><li>■ Does our current security posture meet the standard of due care?</li><li>■ What are the biggest security risks? What would the impact be?</li></ul>
<b>2. Committed</b>	Now you've got a huge to-do list and an even bigger wish list. But you don't have the staff or budget to do it. Prioritizing is key.	<ul style="list-style-type: none"><li>■ Should we hire more people or buy more tech? Or both? In what order?</li><li>■ Can we quantify the impact of our existing investments on reducing risk?</li></ul>
<b>3. Growing</b>	You've got more people (and tech) now. Churn is a real issue. You need to think carefully about how to motivate and enable them.	<ul style="list-style-type: none"><li>■ What metrics are most relevant for business owners and the board?</li><li>■ When it's time for SOC-like capabilities do we want to build or buy?</li></ul>
<b>4. Getting SOCeY</b>	You're big and mature enough now that you've got 100+ new vendors trying to sell new products. Picking the right partners is key.	<ul style="list-style-type: none"><li>■ How do I know if I'm getting better? What new risks are we facing?</li><li>■ What's the right balance between prevention, detection and response?</li></ul>
<b>5. Automating</b>	You've made it into the security one-percenter club. Congrats! At this point your focused on improving efficiency.	<ul style="list-style-type: none"><li>■ Where are the biggest bottlenecks in my processes?</li><li>■ How can I make my key talent more productive through automation?</li></ul>

## **Part 4:**

Navigating the confusing managed security services landscape

# Ever wonder how the managed security services landscape got so confusing?

If you've been to the RSA Conference or Black Hat over the last few years you've seen how the size of the expo hall has doubled or even tripled. The thing is, there are only a limited set of companies with enough people to use most of the products on display.

So what's an under-resourced security organization supposed to do? In the past you might have turned to an MSSP. But they haven't evolved or innovated.

To fill the gap (and meet customers' needs) a new category of providers has popped up: managed detection and response (MDR) services. They focus on finding threats that get past your MSSP.

Meanwhile product vendors — eager to sell their products to customers that don't have the people to run them — have added managed services to run their products.

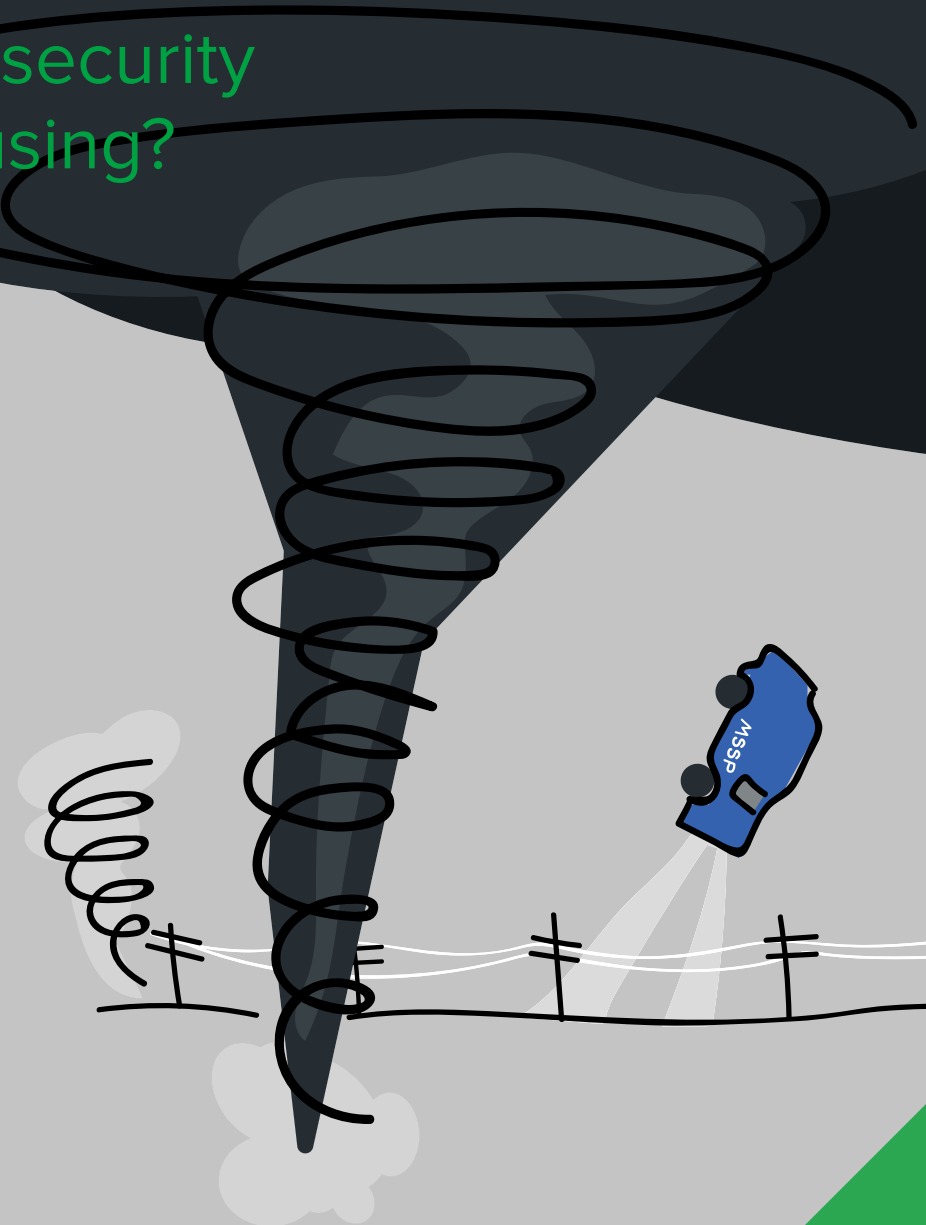
It's a confusing state of affairs.

## Three reasons managed security is so complicated

1  
There are too many products

2  
There aren't enough people to use the products

3  
Traditional MSSPs have failed to innovate



# “MSSPs failed to adapt services to actual customer needs.

It is not a stretch to state that MDR services are partially the result of MSSPs overemphasizing monitoring services and underemphasizing customized response actions while delivering services.

Far too many clients complain of templated email escalations based on signature detections with default suggestions such as “isolate the host and re-image the machine.” While five to 10 years ago clients were struggling to solve visibility and monitoring problems, security leaders in 2017 need investigations, not notifications. Sending notification that an alert occurred is far less valuable than remediating the issue that caused the alert in the first place.<sup>1</sup>

FORRESTER<sup>®</sup>

<sup>1</sup> The Market For Managed Detection And Response Booms In 2017, Forrester Research Inc., July 21, 2017



# Managed services come in lots of different flavors and sizes

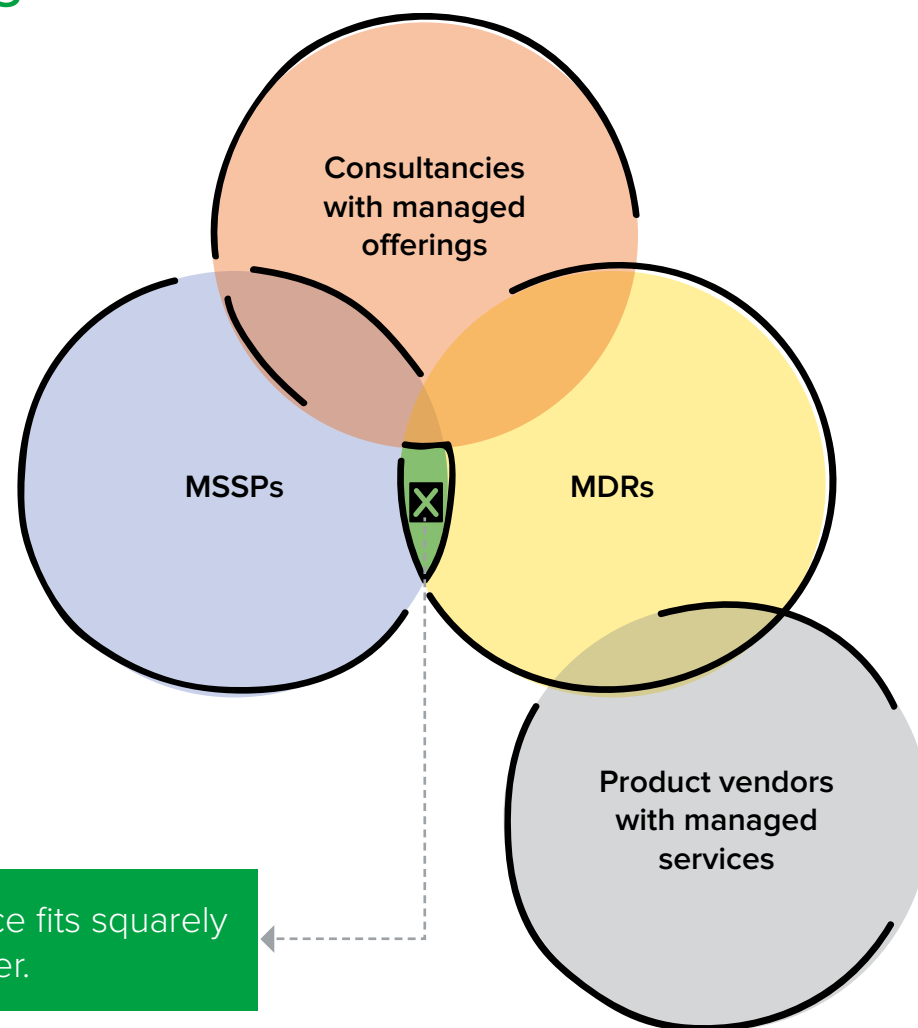
There are a bunch of ways you can slice and dice the managed security services market. We think this is the most helpful way to navigate among the different approaches so you can figure out which one serves your needs best.

**MSSPs** — These are the big vendors that have dominated the space for ages. *Ex. Symantec, SecureWorks and IBM*

**MDRs** — Niche vendors that detect and respond to threats that get through your tech (or MSSP). *Ex. Arctic Wolf*

**Consultancies** — Most major consultancies now offer a managed capability. *Ex. Accenture, Deloitte, EY*

**Product Vendors** — Endpoint detection and response vendors among others now provide a managed offering if you don't want to drive their products solo. *Ex. Crowdstrike*



Expel's transparent managed security service fits squarely in the overlap of what MSSPs and MDRs offer.



The overlap between managed security services and MDR is increasing, which is adding to the confusion in the market and making it difficult for buyers. MSS and MDR still have distinct characteristics that buyers need to understand.<sup>1</sup>

<sup>1</sup> Gartner, Market Guide for Managed Detection and Response Services, by Toby Bussa, Craig Lawson, Kelly M. Kavanagh, Sid Desphande. 31 May 2017.

# Our focus on transparency and resilience differentiates us from other MSSP and MDR vendors

Since everyone loves a good comparison chart, we've provided our take on how we compare to MSSPs and MDR vendors.

In short, Expel replaces what you'd spend on managed security service providers (MSSPs) and managed detection and response (MDR) providers combined.

And... in addition to replacing the alerts spewing out of your security appliances with answers, we'll also use the advanced capabilities in those products to hunt, investigate and respond.

Capability	eXpel <sup>™</sup>	MSSP	MDR
Security device management (firewall, SIEM, etc.)		?	
Vulnerability management		✓	
Security device monitoring	✓	✓	
Automated alert processing	✓	✓	
24x7 monitoring by a staffed security operations center (SOC)	✓	✓	✓
Log data collection and storage		✓	✓
Log data analysis	✓	✓	✓
Ability to use existing security stack (vs. vendor-mandated tech)	✓	?	
Advanced threat detection	✓		✓
Proactive threat hunting	✓		✓
Event/alert triage performed by an analyst	✓		✓
Incident validation and notification	✓		✓
Remediation guidance	✓		✓
Advanced data analytics to reduce false positives	✓		✓
Resilience recommendations to address root cause of repeat incidents	✓		
Transparent view into analyst activities via rich portal experience	✓		
Transparent metrics to measure progress and hold vendor accountable	✓		
Alerts enhanced and prioritized with business context	✓		

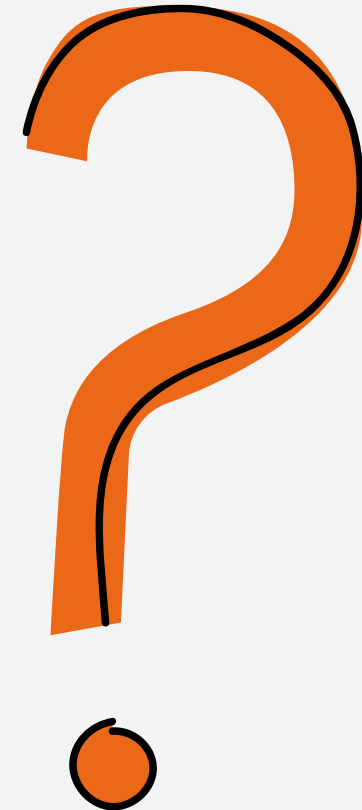
## **Part 5:**

Eight questions to ask managed security service providers

# Eight questions to ask managed security vendors

Now that you know how we view the managed security services market, you won't be surprised to hear we've got some ideas of questions you should ask providers as you're doing your due diligence. So... we leave you with these nine questions.

1. How will you integrate with my existing workflow and processes?
2. How long will it take to onboard?
3. How much work will it take for me to manage you?
4. If I break up with you am I going to have to replace a bunch of technology?
5. How will I be able to measure the value you're providing?
6. When you send me an alert will you tell me what triggered it?
7. When you send me an alert will you tell me what to do about it?
8. Will you give me advice over time on how to improve my security posture?





## MSSPs Are Trapped Behind The Scenes

Clients find MSSPs stuck in the days of security as a back-office cost center. These providers can justify why outsourcing your SOC is a great investment, but when asked how their services can transform security into a business-driven, customer-facing function, an uncomfortable silence follows.<sup>1</sup>

FORRESTER<sup>®</sup>

<sup>1</sup> Lessons From the Forrester Wave™: MSSPs, North America, Q3 2016, Forrester Research Inc., February 28, 2017.

Additional resources

# List of resources

## About the market in general

Where does security operations fit in your business?

[expel.io/security-operations](https://expel.io/security-operations)

Expel EXE blog

[expel.io/blog](https://expel.io/blog)

## About Expel's transparent managed security service

Product tour

[www.expel.io/managed-security/demo](https://www.expel.io/managed-security/demo)

Product overview

[www.expel.io/managed-security](https://www.expel.io/managed-security)



## Editor's note

The following buzzwords were consciously eliminated from this document in no particular order:

market-leading

next-generation

military grade intelligence

artificial intelligence

machine learning

scalable

robust

changing threat landscape

end-to-end

actionable

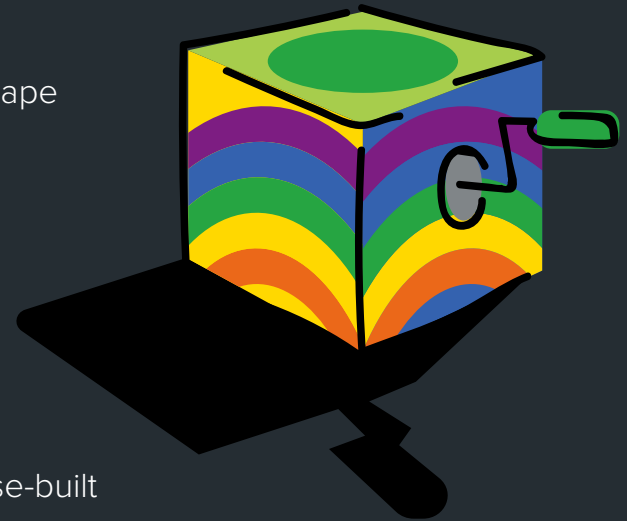
AI

real-time

best-of-breed

continuous and purpose-built

We did, however, tear open black boxes. Sorry about that.



(this is the last page)



Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place. To learn more, check us out at [www.expel.io](http://www.expel.io)