Facing up to complexity

How to deal with complex cyber-incidents caused by modern sophisticated threats

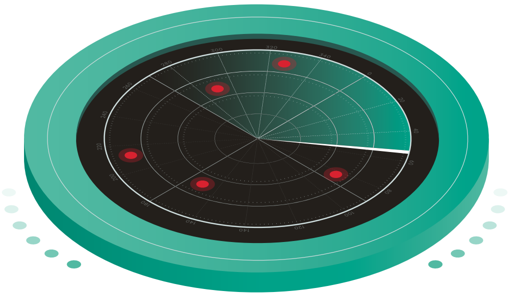
kaspersky BRING ON THE FUTURE

It may not always be possible to halt a threat before it penetrates the security perimeter, but it's absolutely within our power to prevent the attack from spreading and to limit or exclude the resultant potential damage. And, when it comes to complex or targeted attacks, speed of incident resolution is critical.

However, complex incidents present very specific challenges, because they typically involve many aspects of the organization's infrastructure that's under attack. In a sense, this presents the dilemma – how do we know where to start, when seemingly everything matters most?

In this paper we're going to look at the five key barriers to successful complex incident resolution. But first, let's start with interrogating the idea of complexity itself, and what it means for cybersecurity professionals.

What, exactly, is a complex incident?



A complex incident might more clearly be defined in opposition to a simple incident. It would be remiss not to mention that the global Covid-19 pandemic is the epitome of a complex incident – it involves multiple systems: countries, organizations (governmental and business), communities, schools, sectors, families and individual human beings. To say nothing of the fact that the virus acts as a complex incident within the bodies of people who become very sick with it; its effects extend beyond the respiratory system to include the cardiovascular, renal, dermatalogic, neurological, immune, and even psychiatric systems.

Complex cyberspace, complex threat landscape, complex cyber-incidents – a natural progression?

It's worth pointing out that the growing complexity of cyber incidents is directly related to the growing complexity of growing corporate IT systems and, indeed, of cyberspace itself. In fact, according to ENISA (the European Union Agency for Cybersecurity), *Emerging Trends January 2019 to April 2020 Threat Landscape Report,* "The interconnectedness of various systems and networks enables cyber incidents to spread quickly and widely, making cyber risks harder to assess and mitigate." In other words, the more complex corporate IT infrastructure, the more it is at risk from complex cyberattacks, making the challenge of complex incidents even more acute for large, inherently complex enterprise-level organizations.

Yet the natural correlation between complex environments and the complex incidents extends beyond the specific complex enterprise system. Cyberspace itself is defined by ISO/IEC 27032:2012 as a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form". In other words, what we face are in fact three layers of complexity: cyberspace, the enterprise IT environment, and cyber incidents. Complicating this landscape further is the fact that these three layers are interconnected and interdependent, each becoming increasingly complex in order to achieve its goals:

Cyberspace – increasing reliance on interconnected devices, systems and processes in order to support daily business and leisure life, leading to increasing complexity of the environment

The enterprise IT environment – experiencing an expanding attack surface resulting from an expansion in the number of interconnected devices, systems, and processes (including supply chain) and, simultaneously, a steep growth in the complexity of cyber incidents it faces, as well as the cybersecurity configurations necessary to fend them off

The threat landscape and the actors within it – on the one hand responding to increasing complexity in both cyberspace and the enterprise environment, and on the other, specifically leveraging that complexity in order to launch highly sophisticated, advanced attacks (involving lateral movement of an order not possible in the days of simpler target systems).

The bitter truth is that, of these three, it is threat actors who have most quickly found ways to reduce the barrier of complexity – by resorting to Malware-as-a-Service, among other things:

> “Nowadays, barriers to entry for would-be cyber criminals are falling rapidly because the attackers have a range of (technical) capabilities and substantial resources at their disposal, since malware and malware-as-a service have become more easily and cheaply available through various means and sources (such as Dark Web and Deep Web). As a result, a variety of advanced techniques and tools (e.g. social engineering techniques and zero-day exploits programs) are available and can be used by cyber criminals to initiate advanced targeted attacks.”
>
> Papastergiou, S., Mouratidis, H. & Kalogeraki, EM. **Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures.** Evolving Systems (2020).

The good news is that there are ways that enterprises can significantly, effectively, and decisively, reduce the barrier of complexity, and we'll be investigating this further in the paper. Before we do that, we're going to look at the five key barriers to successful complex incident resolution.

The five barriers to successful complex incident resolution

We know that it's fully within our power to stop the progress of, and limit the damage caused by, complex threats even once they've penetrated the corporate perimeter. For starters, it's worth remembering that the majority of the Initial Access tactics within the MITRE ATT&CK enterprise framework are still relatively traditional.

That spear phishing should still be a primary Initial Access tactic, even for APTs, within the context of global pandemic chaos, should give us pause for thought. Firstly we should consider quite how many attacks could be prevented by automating routine cybersecurity tasks that block initial access. But also, it highlights the fact that attack penetration (with exceptions such as zero-day exploits) is not what makes an incident *complex*.

Complexity begins with tactics such as lateral movement, the establishment of backdoors, and with various modes of payload delivery and stealth. But what stops IT security teams from being able to exercise their power and expertise to prevent an incident from becoming a complex incident? And, once the incident has become complex, why is it often so very hard to mitigate and resolve successfully?

Barrier #1: The complexity of cybersecurity systems in and of themselves

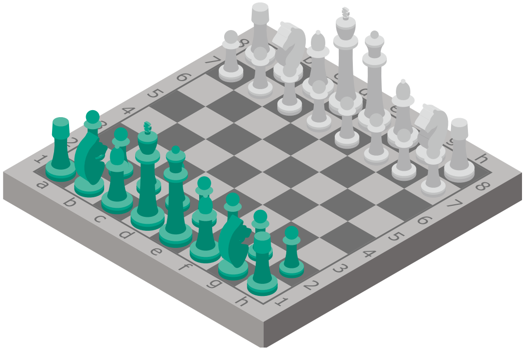
To an outsider, an average enterprise cybersecurity configuration is as bewildering as the cockpit of a stealth fighter jet. Not, of course, that there is any such thing as an average enterprise, or an average cybersecurity configuration, of course. Multiple tools, dealing with highly specialized specific security tasks, a range of control consoles, and reams, and reams of constantly alerts. We've already looked at how this complexity came about – it's an obvious evolution in response to the growing complexity of enterprise IT-security infrastructure on the one hand, and the threat landscape on the other.

It is, therefore an ironic and terrible tragedy that the complexity of the cybersecurity configuration too often becomes an actual barrier to the successful resolution of the very complex incidents they ought to address. This complexity thwarts successful mitigation and resolution in the following ways:

- Teams are drowning in tools, investing precious time acting as 'interpreters' between disparate solutions. Cybersecurity tech stacks (and tech stacks in general) have often become virtual Towers of Babel – with seamless, smooth operation being hindered by the fact that different tools speak different 'languages.'

- Where cyber incident data is gathered in small samples from a variety of non-integrated data sensors on potential penetration points, teams often miss the big picture, and are therefore unable to realise that a complex incident is underway before any obvious entry signs appear. In other words, the incident is not fully understood and this can ultimately lead to damage.

- The need for constant manual processing that comes from addressing alerts non-systematic and non-consistent incident response process drains precious energy, causing crucial alerts to be missed, and devoting too much attention to false positives.



Barrier #2: Poor, or irrelevant threat intelligence

Threat Intelligence must pass a three-part acid test if it's even going to begin to fulfil its promise of delivering in-depth visibility into cyber threats targeting your organization:

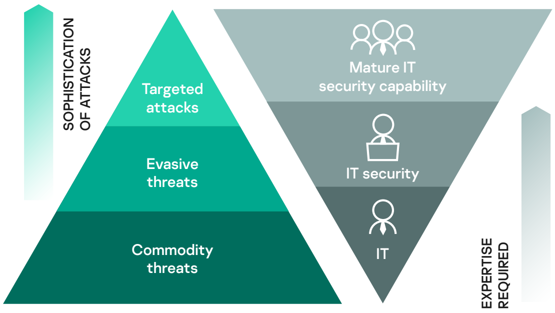
- Is it comprehensive?
- Is it accurate?
- Is it current?

Yet passing this test is only the first step. The barrier that too many enterprise-level organizations face today is that while they do have access to threat intelligence that is comprehensive, accurate, and current, they are missing a crucial piece: relevance. Any IT security professional familiar with the range of threat intelligence feeds available today will be more than aware of this.

Relevance is perhaps one way of saying that quality is more important than quantity, but this is only partly true. Threat intelligence must come from a source that offers both, and must be channelled or process through a holistic cybersecurity system that itself curates and creates relevance for that specific organization, for that specific moment, and for that specific environment. Relevance is not a one-off endeavor, it's an ongoing process, involving a feedback loop between integrated elements within a cybersecurity configuration.

Contextually relevant threat intelligence, integrated with other detection and threat hunting mechanisms, finds meaning and context automatically, saving precious time by delivering clarity from the get go.

Barrier #3: A historical tendency to over-focus on simple commodity threats

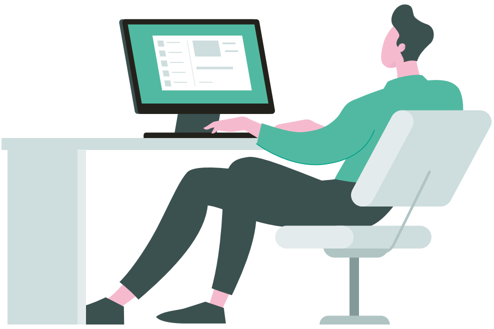


Simple commodity threats still represent a very high percentage of all the threats that any organization will face. In that sense, it's no wonder that the tendency of over-focusing on such threats is still endemic even within large IT-security-matured organizations.

However, the cost of incidents associated with these threats is negligible compared with that of the potential damage caused by the remaining percentage – which includes devastating complex assaults like targeted and APT attacks.

The other reason why some IT security teams still over-focus on simple threats (at the expense of complex incidents) is more obvious. It's human to want to focus on a straightforward problem that is easy to solve. Furthermore, one reason why simple threats are so straightforward is that even the most basic, poorly structured cybersecurity configuration might still do a fairly good job of automatically detecting them, while at the same time not offering enough automation when it comes to resolving them. Thus, simple threats can occupy too much space, demanding attention that they ought not to need, at the expense of focusing on complex incidents that are far more lethal.

Barrier #4: The cybersecurity talent crisis



A quick glance at the Cyberseek Heat Map, an initiative started by the US National Initiative for Cybersecurity Education (NICE) reveals the extent of cybersecurity talent crisis. While Cyberseek only deals with gaps in the American context, it serves as a very useful (and sobering) glimpse of a global shortage.

As of January 30 2021, there are 521,617 job openings for cybersecurity professionals in the US, against a total employed cybersecurity workforce of 941,904. That's a national average supply-demand ratio of 1.8.

While this is good news for cybersecurity professionals in terms of job security (and now would be a very good time to encourage your high-school age children to pursue a similar career), it's not good news when it comes to the quality and efficacy of working life.

Most analysts conclude that the cybersecurity talent crisis is due to failures in education and training, but this insight won't help organizations on the ground. Until these failures are addressed and remediated (in part by initiatives such as Cyberseek), organizations need to deal with this barrier by maximizing the power of their existing IT security teams, providing the tools, support, guidance and back-up they need to be able to successfully resolve complex incidents.

Barrier #5: The problem of speed

This last barrier to successful complex incident resolution links the preceding four together. In the face of complex challenges such as zero-day exploits, non-malware attacks, fileless attacks, and living-off-the-land attacks, speed is everything.

A complex incident doesn't necessarily begin in a complex way, as we have seen with the continued prevalence of spear phishing as a tactic for gaining initial access. The devastating (and expensive) consequences of far too many complex incidents could have been prevented had the team in question only been able to respond fast enough.

This is not of course to suggest that there is ever a point in the evolution of a complex incident when it becomes 'too late in the day', just that as time ticks on, so too does the level of complexity. It might sound over-simplified to state that, when it comes to complex incidents, speed is everything. But provided we qualify what we mean by speed, it is absolutely true.

Speed doesn't mean constant firefighting, or being a hair trigger and responding fast to any alert that demands our attention. It means speed of accurately executing all essential detection and response processes, decisively and consistently. This includes proactive threat hunting, root cause and retrospective analysis, remediation, mitigation and incident response, among others.

What does the future hold for organizations facing complex incidents?

The beginning of 2021 seems to be about the worst time in recent memory in which to try to answer any questions about the future. After all, the pandemic is, in itself, a complex incident and one for which our tools, systems and professionals were not equipped. But there are still some things we know for sure. For example, we know that APTs and other complex attacks will continue to evolve, and we know that **teleworking is likely to continue to grow**, even after the pandemic has been resolved. Our Global Research and Analysis Team (GReAT) of world-leading cybersecurity researchers, have made the following **predictions for APTs in 2021:**

- False flag attacks (such as Olympic Destroyer) will reach a new level
- Ransomware will be increasingly targeted
- New online banking and payment vectors will emerge
- We'll see more infrastructure attacks, and attacks against non-PC targets
- Increased attacks in regions that lie along the trade routes between Asia and Europe
- Increasing sophistication of attack methods
- A further change of focus towards mobile attacks
- The abuse of personal information: from deep fakes to DNA leaks

The prospect of such complex incidents hovering over the heads of IT security professionals doesn't need to signal doom.

Returning to ENISA's Research Topics January 2019 to April 2020 report, we find a kernel of hope and a hint of where to focus our efforts as we seek to successful resolve complex incidents: the human dimension:

"Cybersecurity is still seen as the practice of protecting networks, information systems and data (NIS). This definition needs to be further expanded beyond technical issues to include socio, behavioural and economic concerns and the different roles performed by the parties involved. This should constitute a priority in future cybersecurity research and innovation discussions. A better understanding of the human dimension is key in the definition of any cybersecurity strategy so that security decisions are taken to meet their needs, skills and expectations."

For our purposes, the 'parties' mentioned above refer to IT security professionals, as well as the business leaders to whom they are accountable. We may not be able to recruit all the cybersecurity talent we need, so the question becomes, how do we nurture what we already have?

Expert tech in expert hands

The first step is to understand that even the most highly IT-matured organizations are not expected to tackle complex threats and APT attacks. It's a global problem, constantly shifting across regions and sectors, and too many teams are stymied in their efforts to successfully resolve complex incidents, by the barriers we've looked at in this paper.

That's why we encourage all of our enterprise customers to ensure that they diligently address what we see as the three pillars of any successful complex incident strategy. Namely, security teams must be:

- **Equipped:**
  Cybersecurity is one area of expertise where even a skilled worker can legitimately blame their tools. Protection from multivector attacks and other complex incidents requires a unified consolidated platform that gives total visibility, eliminating obstructive siloes and preventing 'alert fatigue' and other routine tasks within the incident response process.

- **Informed:**
  The existing advanced expertise of IT-matured organizations must never be taken for granted. After all, the cybercrime horizon is constantly shifting and expanding. Ongoing education and powerful threat intelligence from reliable cybersecurity partner are absolutely crucial.

- **Reinforced:**
  Should a complex incident or APT be discovered, even the most advanced IT security analysts should have access to external support for 3rd party insight, security assessment, managed threat hunting and incident response. While complex incidents resulting from APTs are usually highly targeted, they rarely target only one victim. External expertise can shed a multi-sector global light on the likely paths of an APT, and deliver actionable advice on the most decisive way to eliminate it from the system.

Revolutionize the way your IT security experts take control of complex incidents

Revolutionize the way your IT security experts take control of complex incidents with Kaspersky Expert Security: a comprehensive defensive concept that equips, informs and guides your team in their fight against the most sophisticated and targeted cyberattacks. It's an Extended Detection and Response (XDR) platform featuring a perfectly matched combination of industry-leading tech, elite threat intelligence, human expertise, training, and services, backed by the greatest minds in cybersecurity. Our holistic approach nurtures your team's cybersecurity power over multi-dimensional threat discovery, effective investigations, proactive threat hunting, delivering a rapid, centralized response to the full spectrum of modern threats

Find out more at go.kaspersky.com/expert

Cyber Threats News: www.securelist.com
IT Security News: www.kaspersky.com/blog
Threat Intelligence Portal: opentip.kaspersky.com
Technologies at glance: www.kaspersky.com/TechnoWiki
Awards and recognitions: media.kaspersky.com/en/awards
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

kaspersky

**BRING ON
THE FUTURE**