+44 345 094 0945
www.waterstons.com
Article

Static vs Dynamic capability

Breadcrumb

1. Home /
2. Print /
3. Pdf /
4. Node /
5. Entity Print

Insight navigation

- Latest insights
- Latest news
- Articles
- Case studies

Download PDF

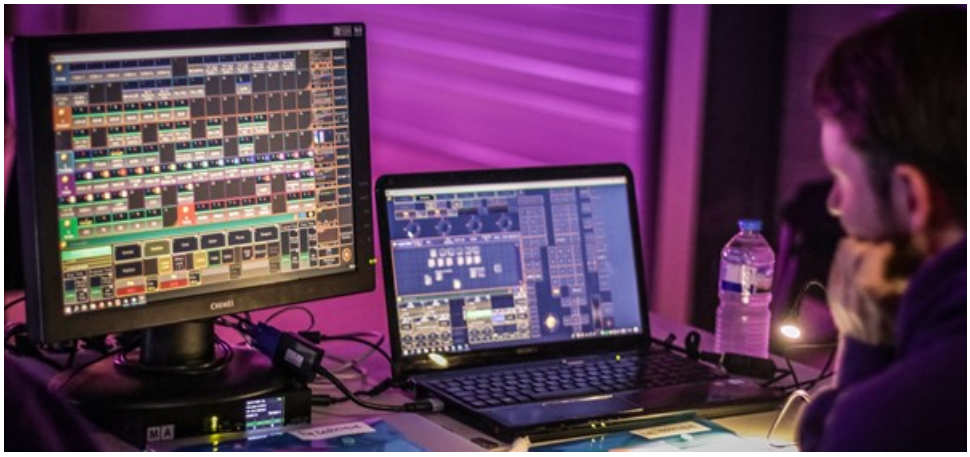
Jul 2021

Static vs Dynamic capability

Producing predictable outcomes from unpredictable circumstances

Categories Cyber Resilience, Managed Security, Security Solutions

Jul 2021



On a high enough level, all entropy is dissolved. This principal, while recursive in nature provides the basis for my belief that an organisation's technical capability can be judged solely on its static and dynamic capability. Static being any intelligence or information built over time inherent to the organisation, be it process, documents or anything you would consider intellectual property. Dynamic capability on the other hand being the people in the organisation, what they are capable of and in what capacity they are empowered to act.

While an organisation may have exceptional process, without staff able to carry it out, be it through a lack of training, bandwidth or empowerment. The process may as well be written in another language. Similarly, if the staff have the bandwidth, training,

and empowerment, without process or documentation, situations will not be addressed in a coherent manner and there is no predictable outcome.

This is all high level, but bear with me, I'm about to get to the juicy security stuff. Let's say Hackerman is in your network. He has accessed a few servers, only really poked around undetected in preparation for an attack. Now, Hackerman in all his wisdom has used an off the shelf piece of malicious software to help gain higher access and in doing so, has flagged an AV alert which has come through to your IT Service Desk or Security Operations Centre.

> "Who picked the alert up and what did they do next? No matter the security incident, this is always how the narrative begins."

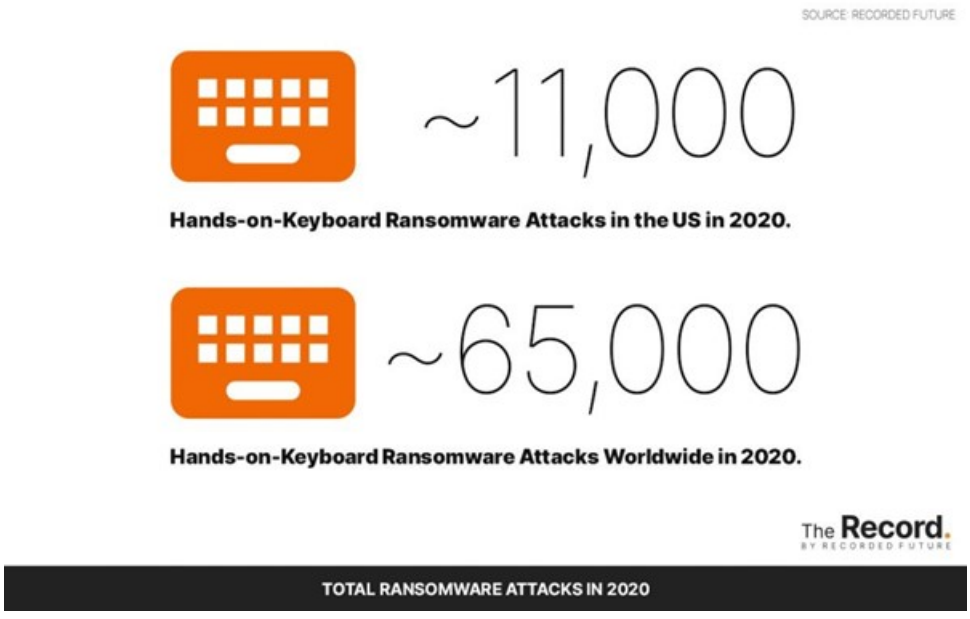
So, let's start with the best-case scenario, the staff member who picks it up knows some security basics, they understand some of the Cyber Kill Chain or know of some common tools used by attackers. Immediately, they know this is serious and needs their attention. From here they look toward the internal documentation containing the process to handle these alerts which in turn points them to a playbook that has been tried, tested and improved over time.

From here, they confirm the problem. An incident is raised and stakeholders are notified. As per the playbook a predefined Cyber Security Incident Response Team is now involved and in turn that team executes its playbooks to understand the breadth of the attack. The team will discover and analyse all persistence and changes made in the environment, contain and eradicate the threats and recover the environment for handover back to the organisation or client. Super clean and organised with a predicable outcome.

In this scenario, the people involved have clearly predefined roles, they understand their tools and how to use them and at a high level, they understand the anatomy of the threat, however they are only capable of producing the result they do due to the process and documentation in place and lessons previously captured. There is no need to Google "How to use Autoruns", jump from server to server to find the VPN access logs or understand server restore process, it is all there ready to go. and in most cases automated.

Now, say this same scenario were presented to a less experienced team member with little to no security process or documentation from the start. Unable to immediately identify the threat and not having process in place to help do so, the priority may be set incorrectly, alert fatigue may even have them deem it a false positive. From there, regardless of who picks it up, the response time is hindered. Once actually identified, and understood, since no trained response team exists and required roles haven't been defined, likely a major incident will be raised and stakeholders from across the business will be involved at random, each requiring a separate briefing.

Once actual identification begins, without experience, process, or knowledge to draw from, the team likely won't be capable of identifying the extent of compromise or discovering persistence and regardless of clean-up, are unable to eradicate the threat from the environment. From here, having deemed the threat eradicated and handing back to the organisation or client, they have essentially now alerted Hackerman allowing time to react.



source: https://therecord.media/ransomware-tracker-the-latest-figures/

While this scenario sounds unlikely, especially for an organisation that has yet to experience it, in 2020 alone, this exact scenario has been noted to play out at least 65,000 times. With TheRecord.media estimating 65,000 hands on keyboard attacks

globally, this only accounting for ransomware crews. If you break that down that's an average of 178 businesses, hospitals, schools etc experiencing this every day. 1246 per week.

While I try my best to not take an alarmist approach to these situations, objectively speaking, this problem is provably telescoping in nature and stands to grow exponentially. Remembering that Static and Dynamic capabilities drive organisational response to security, so too does it drive a threat actor's ability to operate. With each successful or thwarted attack, lessons are learned by both sides, only in the case of the threat actors, they are learning approximately 1246 lessons per week.

Given all of this, static vs dynamic capability, common scenarios, statistics on attacks etc, I personally believe Small to Medium sized Businesses partnering with Managed Service Providers provides a lot more than outsourced services, it bolsters any team with the combined static and dynamic capabilities of an entire organisation that deals almost exclusively in IT and Security. Like my previous point, working daily with so many organisations, teams, technology stacks, etc, we learn thousands of lessons per week, be it our staff, knowledge base or process. It's honestly the reason I refuse to leave this space and I suspect the same of most clients that have spent decades in our care.

If you'd like to learn more about our offering or have a chat about what we could do to help secure your organisation, drop a line to info@waterstons.com.