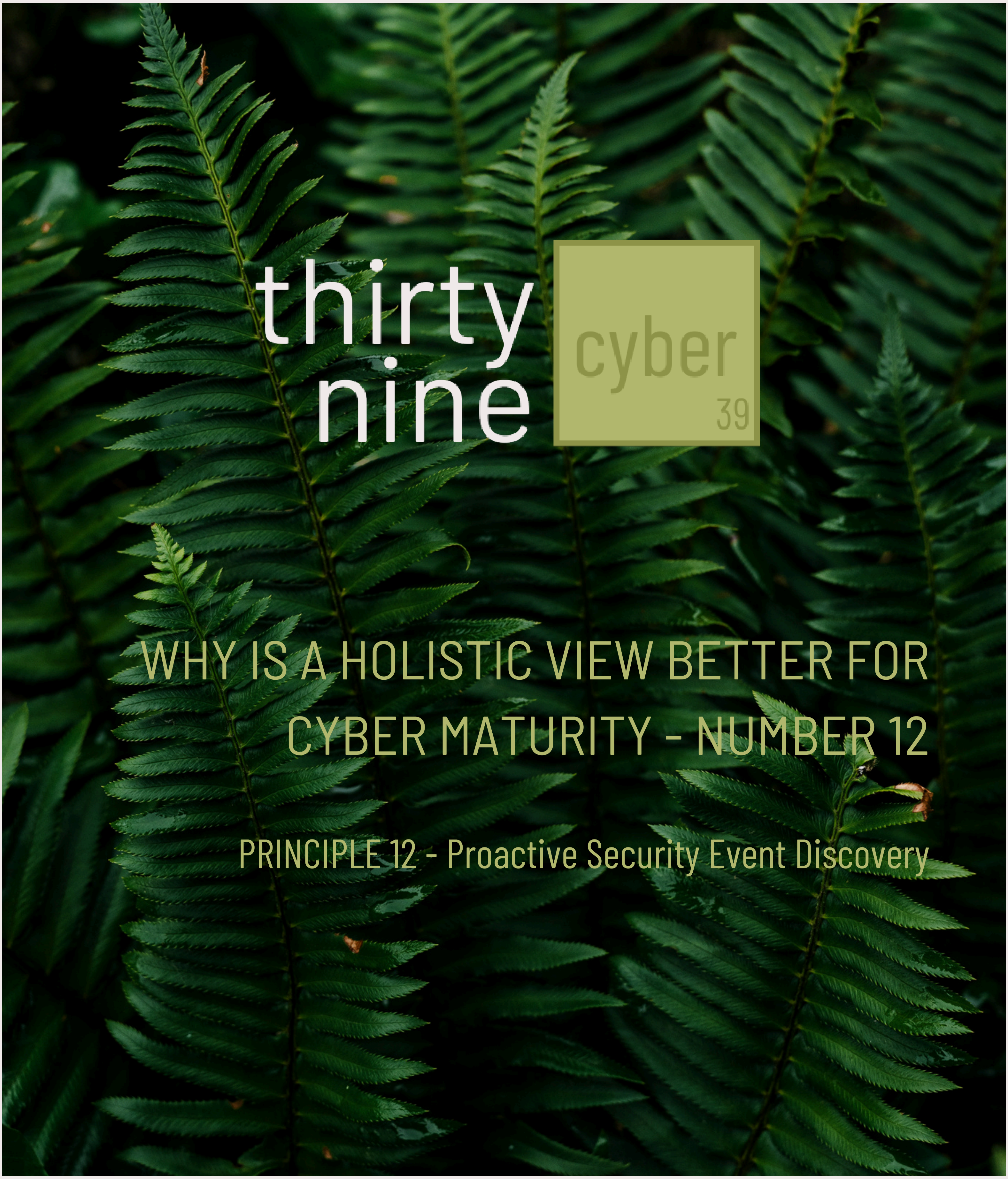

thirty nine cyber 39

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 12

PRINCIPLE 12 - Proactive Security Event Discovery

thirty nine cyber 39

ASSESS. ADDRESS. **SUCCESS.**

Enabling You to Make the Right Decisions About Your Security.

STUART.AVERY@THIRTYNINECYBER.COM

To the reader

Welcome to my opinion – covering the twelfth principle in NCSC's CAF framework – Proactive Security Event Discovery.
This principle is tied to the last principle "Security Monitoring". Adding monitoring tech into your digital environment is only half of the answer, you need to be proactive in detection as well, this blog explains why.

So here we go…

Key takeaways [TL; DR]

I have discovered that sometimes people don't want to invest in reading the whole document unless they have a good idea of what it covers – ok fair, so I have added a new bit to give you a summary view.

So, what's in it

1. Explains the difference between a reactive & proactive approach and why (IMO) humans are important in any solution
2. Gives some pointers on the basics that make proactive security event discovery easier to perform

Still fancy reading it?

Ok, strap in.

Proactive Security Event Discovery

What is it?

A well configured monitoring solution will, with the correct rules in place, detect anomalies that you have asked it to detect using scenarios (use cases) that are mindful of your security policies and alert when conditions arise that breach these policies or detects signatures that you have asked it to look for borne from threat intelligence you have received.
But where those signatures cannot be added either because the anomaly is new and unaccounted for (zero day) or the anomaly is behavioural not signature based then a more lateral approach needs to be taken.

There are technologies that claim to detect these but when applied can create a cottage industry of false positive triage that will blind your security team. Being proactive adds another layer of "clever" detection techniques and tends to lean on the human in the loop, threat hunting and behavioural baselining aided by technology and machine learning or AI are a couple of examples.
Proactive Security Event Discovery relies on lateral thought processes, systems tend to rely on logic and so additional techniques need to be applied, human curiosity is the real asset you should leverage.

CAF breaks this principle into 2 outcomes

a. System Abnormalities for Attack Detection: You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.
b. Proactive Attack Discovery: You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.

Why is the Proactive Security Event Discovery principle important?

Proactive Security Event Discovery makes the difference between a good monitoring and detection posture and a great one

Here's why it's important:
When implementing a monitoring and detection capability you should be mindful of how it will detect, not just known threats but also how it can help you identify emerging ones. emerging threats or "zero day" threats are the dangerous ones, they are difficult for reactive monitoring solutions to detect because there is little or no knowledge of the new vulnerability being exploited or the systemic indicators that give away the presence of the attack.

Reasons why it matters:

1. Cyber attack and defence is an arms race

It's useful to consider your posture and subsequent strategy this way, although it sounds alarmist (I get that). when a system vulnerability is discovered by an attacker it can cause a feeding frenzy, attackers move quickly to implement a technique to exploit the vulnerability before the system vendor can create a security patch to limit or eradicate the potential exploit. having a more proactive approach to discover behaviors or techniques being used by the bad guys fills the gap until a fix is released and keeps your organisation operational.

2. Discovering a well disguised malicious presence in your digital environment

A sophisticated actor may be able to gain access and sit undetected on your network, proactive hunting techniques around behaviour can be used to detect entities on the network that are behaving outside of an expected baseline or processes to spot "grey" entities created outside of policy

3. Using new Indicators of compromise or attack to review your log history

this sounds like closing the gate after the horse has bolted but it is a good way to limit the chances of, or at least discovering a resident malicious actor.

Proactive detection techniques elevate your defensive posture to counter sophisticated attack vectors, if your threat profile includes sophisticated threat actors then you should invest in this element. proactive detection is made easier if you have implemented a simple, well defined and configured environment, because if you know it and how it should behave then detecting behaviours outside of expectation is simpler.

Things to consider

There are some considerations to make when approaching Proactive Security Event Discovery , this isn't exhaustive but may help you define an approach

Considerations:

- Threat hunting should be part of what you do. If you you are investing on a SOC service then threat hunting should be on the SOC's to do list, this is where a SOC solution earns it's money, to be fair a well set up and configured system (security incident & event management - SIEM) can do most of the reactive stuff, modern tech will even respond systemically (security orchestration, automation & response - SOAR) but hunting proactively across the network to look for behavioural indicators of compromise or attack takes a curious mind and some lateral thinking, there is tech that claims to do this for you and even claims that AI will do this for you but the jury is still out for me.
- Make the monitored environment simple to baseline. Put some effort into ensuring the environment that will be monitored is managed properly with hygiene routines to reduce the attack surface and designed to use just enough technology, configured consistently and assets (including builds, controls and versioning) recorded properly and accessible to the SOC team.
- Every digital asset (tech) that you add, represents risk. Don't add it unless you need it, manage it properly if you have added it.
- Insource/outsource make the right choice. Whatever you decide, ensure that you have employed measures to ensure threat hunting is part of the process and that the right expertise is applied to make sure it's done well. ask the provider, if you're outsourcing, how this is done.
- Your SOC capability should demonstrate four main attributes. Curiosity - Authority - Visibility - Expertise. This is my summary, you can add more but these four in my experience underpin proactive SOC greatness.

Ok so I hope that all made sense, I'd love to hear from you if you agree or disagree, you can reach out to me at stuart.avery@thirtyninecyber.com

Like this? Please follow ThirtyNines LinkedIn page – https://www.Linkedin.com/company/thirtyninecyber and read more in this series as they are released.