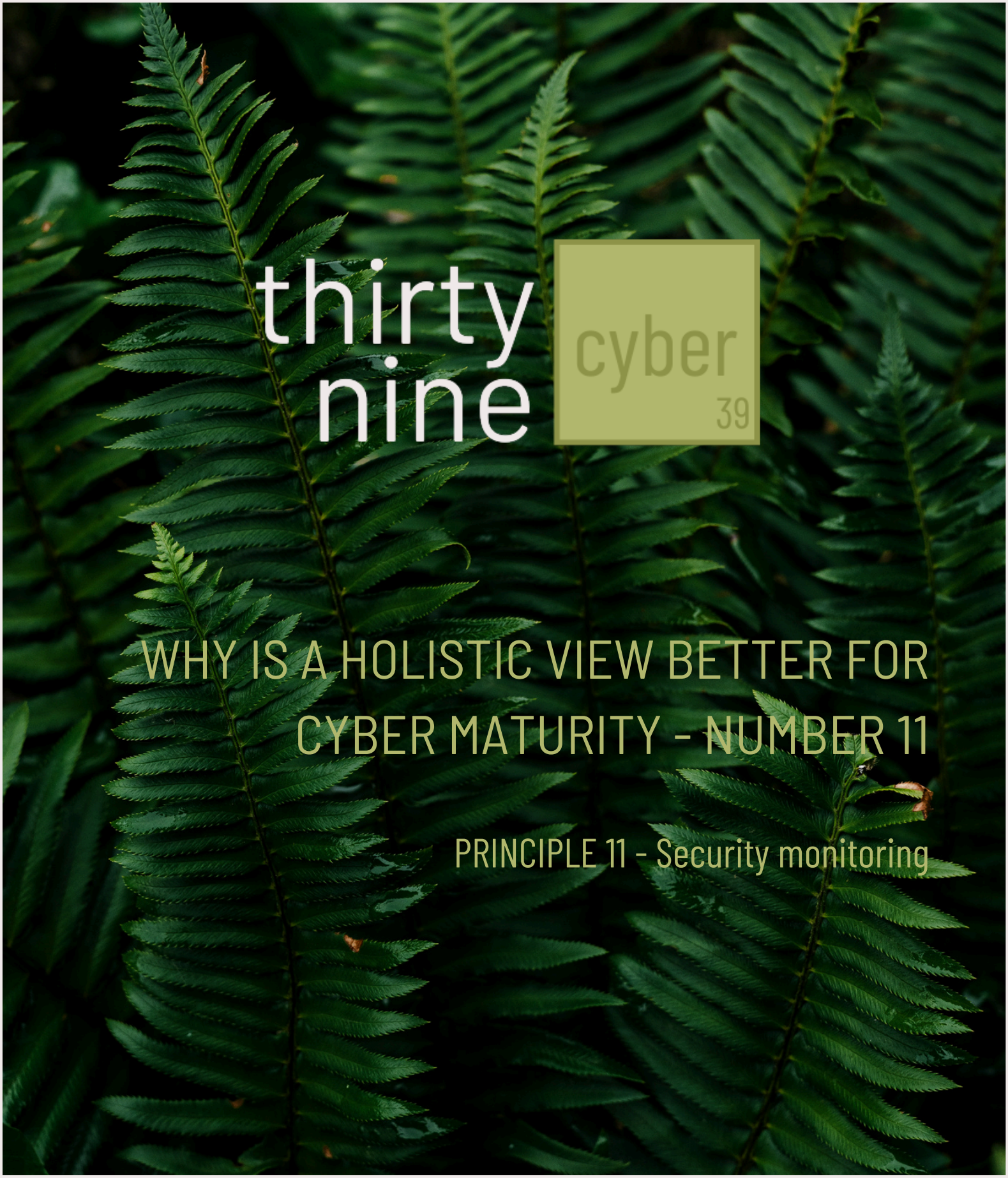

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 11

PRINCIPLE 11 - Security monitoring

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 eleventh principle in NCSC's CAF framework – Security Monitoring.
This subject is important and the cyber security market is overwhelmed with solutions that "fix" this, but are they all right for your business? this is an area that should be considered in depth before you take the plunge.

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. Why it's important, and more so, why you should consider monitoring and detection carefully.
2. Tips on how you can implement at your pace, not the vendors.
3. How to maximise monitoring solution effectiveness.

Still fancy reading it?

Ok, strap in.

Security Monitoring (& Detection)

Monitoring & Detection in simple terms

Monitoring is like having a 24/7 watchtower. It keeps an eye on your digital estate, all the comings and goings like emails, logins, file transfers, and network activity.
Detection, on the other hand, is what happens when the monitoring system spots something unusual or something that you have asked it to look for (rules). It's the alarm that goes off to say, "Hey, something's not right!" Maybe someone's trying to guess your Wi-Fi password or a file you downloaded is actually a nasty virus. The detection bit helps you act quickly to shut it down.

A malicious actor leverages 2 basic principles when employing an attack technique to meet their mission objective, avoid detection or execute rapidly.
for the second one, the attack is noisy, detection is obvious (as long as you are monitoring) your security teams primary focus is response, the first one however, well thats how your monitoring and detection team and the processes and technology you employ, really earn their keep.
CAF breaks this principle into 5 outcomes

a. Monitoring coverage - Do you monitor everything you should be monitoring (there are nuances here).
b. Securing logs - Do you ensure that the log data you retain for analysis can't be deleted, amended or viewed without authority.
c. Generating alerts - Have you used intelligence (business & threat) to set rules that create alerts when those rules are breached.
d. Identifying Security Incidents - You apply knowledge of the threat and your systems, to identify security incidents.
e. Monitoring Tools and Skills - you have employed the right tools & skills for your business, risk appetite and the threat

Why is the Security Monitoring principle important?

Security monitoring should be part of your defensive strategy but be mindful of what you are protecting

Here's why it's important:
Think of your organisation like an airport. Every day, people, freight, and information flow in and out, and whilst most activity is perfectly legitimate, there's always the potential for someone to try bringing in something harmful. Security monitoring acts like the airport's security team, carefully watching everything that passes through, identifying risks, and ensuring that any threats are stopped before they can cause incidents.

Reasons why it matters:

1. Detecting Threats Before They Escalate

Just as airport security might spot an unattended bag or suspicious behaviour, security monitoring helps identify unusual activity on your digital systems. Early detection of threats, like unauthorised access or strange data movement, can prevent small issues from turning into major incidents.

2. Ensuring Smooth Operations

Imagine if the airport's operations ground to a halt due to a security breach, it would be chaos. Similarly, a cyber incident can disrupt your organisation's ability to function, leading to lost productivity and frustrated stakeholders. Monitoring gives you visibility of an emerging incident enabling you to act to ensure your business stays operational.

3. Protecting Valuable Assets

In the same way that airport security protects travellers, staff, and infrastructure, security monitoring helps safeguard your organisation's most critical assets, whether that's sensitive customer data, intellectual property, or operational systems. It reduces the risk of breaches that could lead to reputational and financial damage.

4. Staying Ahead of Sophisticated Threats

Modern cyber threats are increasingly complex, often hidden in plain sight like bad stuff cleverly concealed in luggage. Monitoring systems are designed to give visibility of the bad stuff, such as unusual patterns of behaviour or anomalies in data.

5. Meeting Regulatory Requirements

Just as airports must comply with strict safety regulations, many organisations must adhere to industry-specific cyber security standards. Monitoring not only helps maintain compliance but also demonstrates a commitment to protecting customers and your brand.

Things to consider

There are some considerations to make when approaching Security Monitoring, this isn't exhaustive but may help you define a strategy

Considerations:

- Have a monitoring strategy. this is vital, you want to make sure that the monitoring approach you adopt is right for your business and protects the stuff that keeps your business alive, avoid waste by employing the functions you need not the ones you don't. Consider adoption and implementation in stages, start by protecting entry points and critical functions first and expand out to less critical later, this will help with service adoption and cost of ownership.
- Be intelligent in your approach. Profile the threat to your organisation, common low level threats should be a given but if you think you are a target for more sophisticated attacks from outside or inside your organisation then these need to be accounted for in your monitoring approach, this is not a one off exercise by the way and should be revisited often.
- Think about how it will function in your business. your business needs to be able to adopt the service, this is easier if the function is insourced (but very likely more expensive), when outsourcing, if you are not a 24/7 operation then employing a 24/7 service (which is wise) that needs to be able to interact with you should an incident occur, how it does this is an important consideration. This bit is a minefield and needs thinking through.
- Insource/outsource make the right choice. this is a cost/context consideration in the main, if it's insourced then deeper pockets may be required, if it's outsourced, how do you convey the context and criticality of your business model and the systems that support it.
- Measuring performance. It's essential to track monitoring performance, evaluating effectiveness and identifying areas for improvement. think about the purpose of the monitoring task and make sure the measures support it.
- Consider your mission. if it is to deter incidents then remember, most threat actors are part of an organisation that, like you, consider costs and value returned (return on investment), deterring can be achieved, therefore, by making it more costly for an actor to complete their objective (imposing cost). Making the actor use a more sophisticated attack technique increases the cost to them, if the attack is indiscriminate they will move on. if they really want what you have or disrupt your operation and are tenacious then compromise is likely and that's when incident response and rapid recovery are critical (we'll be talking about that later in the series).

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.