Infosec Reborn

A new playbook to understand, adapt and overcome in the hyper-sophisticated threat environment of today's world.

CRITICALSTART

Executive Summary

In this paper, you will learn how to evaluate security risks and why legacy detection and response efforts are inadequate. Discover the different types of security postures and the critical importance of why every alert matters in today's high-threat environment.

Topics Include

How to evaluate your current risk and security posture.

Why anti-virus alone is no longer enough and how EDR tools and a SIEM platform can be your new best friends.

Learn why companies struggle to monitor alerts internally, and MSSPs' and MDRs' different approaches to solving the problem.

Discover how attackers and snatch teams are exploiting activities that only trigger low and medium alerts, and how this can be a desperate vulnerability for your organization.

See the definable impact for yourself when using the right tools and strategy can significantly shrink dwell time, while isolating and mitigating threats.

CRITICALSTART

It's Time to Rethink the Game

There's a new plan available to uplevel your security posture. You need better strategies, processes, technology—and most importantly—the right team and management to take breach prevention to a place that's ahead of the threats surrounding it. Consider this your roadmap for the necessary steps to take inventory of your current security environment and transform it into a breach prevention model that dynamically resolves issues before they can grow into a larger problem.

Evaluate Your Risk

One of the first steps is to deploy a vulnerability management program to create a risk register for your organization. This register is an assessment of vulnerabilities compared to the risk tolerance for your business. Risk tolerance is determined by factors such as potential liability that your organization could face, particularly in industries such as banking, insurance or healthcare, and the likelihood of an attack from a variety of threat vectors, such as criminal hackers or nation states.

This type of risk evaluation can impact the direction of security policies and procedures such as:

- What is considered a critical area of protection?
- When a patch is released for a critical area, will the SLA be 60 or 90 days?
- Will peak traffic be captured separately?
- Will logs be kept for a typical 14-day rotation or several months to trace back the source of an attack?
- Will logs be deleted or placed into cold storage?

> Another part of this process is an evaluation of asset management. Is the list of all assets within your protection environment, and outside of it, current and accurate? Keep in mind that an orphan system which has fallen off an asset list may have no endpoint protection monitoring or logs tracking activity, making it ripe for exploitation.

How Risks are Exploited

At CRITICAL**START**, we've seen significant advances in Ransomware. One particularly sophisticated example that demonstrates how vulnerabilities can be translated into a serious breach is snatch malware.

When a careless employee downloads this malware, it delivers a program known as Cobalt Strike that spreads across the enterprise, stealing credentials. This gives the snatch attackers active access to the corporate infrastructure, including key logging and exfiltrating data before the files can even be encrypted. Even after encryption, this malware can stay persistent in the network to prevent post-event remediation unless a ransom is paid.

CRITICALSTART

You Need More Than a 24x7 SOC

After a proper risk evaluation, most organizations are painfully aware of the need for a Security Operations Center (SOC) that runs around the clock to investigate and mitigate threats. But is the establishment of a SOC in and of itself enough? The short answer is no. Much more attention needs to be focused on who will manage the SOC, how will they manage it and what tools will they use.

First, is the Consideration of Tools

Endpoint Detection and Response (EDR) tools are one of the latest instruments to supplement prevention with detection and response capabilities. Anti-virus platforms provide an alert during an active attack, but sometimes well after the point where an effective defense can be deployed. By comparison, EDR tools watch for indicative behaviors of an attack.

Some examples include:

Configuration to create a list of acceptable tasks during a certain window of time, with tasks outside of this window triggering an alert.

Configuration of an alert for something as specific as the entering of a certain command line.

Beyond alerts, EDR tools can analyze the root cause of issues and track suspicious behaviors from the initial incident response all the way through to the final remediation.

> Keeping track of the alert from EDR tools is the job of a Security Incident and Event Management (SIEM) platform. SIEM can identify, monitor, record and analyze security events in real-time. It provides a comprehensive and centralized view of the security scenario of an IT infrastructure. Depending on the size of the organization, the amount of security logs that a team needs to ingest, process and use to identify threats can be massive. It may be manageable for a small business with only 20 endpoints, but anything more complex really requires a professional third-party to prevent staff burnout and ensure no threats are missed.

CRITICALSTART

Getting Support: Know the Difference Between MSSP and MDR

If you have made the decision to work with a partner to make sense of the data streams that impact the security of your business, the next decisions move along the spectrum of surveillance, analysis and action.

If you decide to work with an MSSP, this type of vendor will function similar to an outsourced SOC. They will take incident and event data from a SIEM and monitor it 24x7, as though you had increased your own staff to manage this function. While this enables you to eliminate the overhead of hiring staff internally, MSSP is a broad-based solution that does not dive deeply into the cause of alerts. Monitoring and notifications are about as far as this type of service typically goes. Incident response support is limited, and since you're basically feeding event information to the MSSP, you are now trusting a third-party with your data.

MDR vs. MSSP

	MDR	MSSP
Event Monitoring Augmentation	●	●
Vendor-run SOC	●	
Whitelist/Blacklist Approach	●	
Focus on high-priority alerts	●	●
Focus on medium-priority alerts	●	
Focus on low-priority alerts	●	
Dynamic incident response team	●	
Active response to stop threats in progress	●	
Transparency into actions taken	●	

CRITICALSTART

CRITICAL**START** Solutions

View our MDR Value Video, MDR ebook or speak with a consultant today at criticalstart.com/criticalstart-managed-detection-and-response

MDRs – a More Sophisticated Plan

By comparison, MDRs use their own SOC, solutions and infrastructure to really absorb alert information and provide a much deeper and more sophisticated response plan to identify both vulnerabilities and threats. This is followed by a dynamic, active mitigation of those issues. Here's how it works:

MDRs work with the client to develop a whitelist/blacklist approach that identifies normal actions and network events. This will establish trusted behaviors up front, so the team can focus on the real threats. It also provides the unique ability to pay attention to even small and medium alerts through an efficient model that shows exactly the information needed.

When threats are identified, an MDR utilizes their own response team. Working through endpoint tools, the team can identify the source of the threat back to the root cause. The MDR team can shut down comprised items such as a password before the attacker can move laterally through other devices in the system.

If the attacker entered through other means, systems can be isolated and quarantined before the event can spread or critical data can be compromised. Since this team can make an active response on behalf of the client, dwell time is dramatically reduced and attacks can be stopped before significant damage occurs.

After an event, the MDR team can share a detailed report with the client so they can understand what happened, what steps were taken and recommendations for corrective action in the future.

CRITICALSTART

Why Every Alert Matters

The reason working with an MDR partner can be essential is because we've found that many internal SOC teams are often overloaded. They focus their attention on critical alerts and maybe high alerts if they have the time. What we're finding is that attackers are being detected through medium, low and even informational alerts through a SIEM platform. A top-down approach simply is not sufficient in today's threat environment.

Here's an example:

1. An attacker obtains a guest password and uses it to log in. This may trigger an informational alert.
2. The attacker next tries to log into 50 machines, but that is still below a pre-set threshold so there is still not a significant alert.
3. The attacker next adds a domain account. This might trigger a high alert, but if there are too many logs to ingest, there is still a significant chance it could be missed.

> By this point, the attacker is well-entrenched in your network and the damage is underway.

Dwell Time: How Each Decision Makes an Impact

As the example above illustrates, medium and low priority alerts that are ignored can make a serious impact on dwell time. Making an intentional decision to focus on those alerts, and working with a partner that holds that focus, can keep dwell time down and reduce the effect of an attack.

Other measures you can take to control dwell time include:

- Following industry standards when deploying servers or devices such as laptops or tablets and implementing simpler measures such as stronger passwords to make your organization a hard target.
- Following security notifications from the industry and implementing recommended best practices.
- Selecting and configuring tools with a focus on how alerts are defined, prioritized and received.

> The key is to be proactive with your understanding of the security landscape as it stands today. Know that this landscape will change constantly, but there is also a baseline of best practices that provide the starting point for protecting against whatever this environment sends your way.

CRITICALSTART

Putting it all Together for Real-world Results

At CRITICAL**START**, we sometimes conduct penetration tests with new clients. One of our team members has been able to walk into a building at a client's location, proceed into a conference room, connect to the enterprise infrastructure and was able to control that infrastructure within the hour—without anyone noticing that our team member was even in the building! From there, this would-be attacker could have deleted active directories, back-ups or deployed ransomware across the system.

After setting up SIEM tools and using our MDR approach, this same attack is isolated, the port the attacker is using is disconnected, and any damage is prevented, with a dwell time of approximately 5 seconds.

Be Prepared for the Future

Right now in information security, we're seeing ransomware as one of the biggest threats facing business. Snatch teams go in quickly, spread ransomware as fast as possible, use shock factor to bully a company into paying, and then leave few traces behind.

Threat actors are becoming more advanced every day, developing both open and closed source tools to deliver ever more sophisticated attacks. This is why the latest tools that evolve to meet these attacks, supported by an approach to shrink dwell time to bare minimums, is more important than ever to stay ahead of a rapidly transforming threat matrix.

Want more information on CRITICAL**START**?
To see how we can help, contact us at criticalstart.com/contact

CRITICALSTART