VECTRA®
SECURITY THAT THINKS

WHITE PAPER

Incident response maturity: Time to grow up

TABLE OF CONTENTS

> "The biggest frustration to me is speed, speed, speed. I'm constantly asking the team what we can do to be faster and more agile."
>
> **– Adm. Michael S. Rogers, then director of the NSA and head of U.S. Cyber Command, when asked by Congress about nation-state actors meddling in the 2016 U.S. presidential election**

Vectra® protects business by detecting and stopping cyberattacks.

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is *Security that thinks*®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

Incident response and the need for speed

When a cyberattack occurs, most aspects of the threat are not under the control of a targeted organization. These range from who is targeting them, what is the motivation, where and when the attack occurs, how well-equipped and skilled that attacker might be, and most critically, the persistence of the attacker to achieve the ultimate goal.

The only thing under the control of an organization is how quickly they can detect and respond to an attack.

Cutting short attacker time and access to critical assets is a paramount risk mitigation investment. The less time an attacker has access to resources, the less likely the damage or impact to the organization.

Reducing access time also increases attackers' costs and forces them to develop new techniques and ways to adapt to reach their goals. The longer it takes an attack to succeed, the lower the return on investment to the attacker.

That is why a mature incident response process provides the benefit of faster response to reduce the amount of time an attacker has access to organization resources.

Incident response metrics: Measuring risk across time

Everything in a mature incident response plan should be oriented toward limiting the time and access cybercriminals have during an attack. The way incident response is measured should directly correlate with that requirement.

Time is an effective criterion for quantitatively measuring and communicating the value of an investment in people, process, and technology as a form of business risk mitigation.

At an organizational level, dwell-time – the duration a threat actor has in an environment until detected and removed – can be measured accurately in a thorough investigation.

After an initial infection, all breaches follow the same blueprint of attackers gaining privileged access, extending the compromise across the network, and stealing or destroying data. This provides a clear understanding of where cybercriminals spend their time in the attack lifecycle.

Dwell-time provides a high-level metric that is quantifiable and can be leveraged to calculate the effectiveness of a security strategy and overall posture. Many organizations now track industry dwell-time benchmarks published in reports that can be used as a meaningful baseline to measure against.

To measure people, process and technology in a security operations group, time metrics based on visibility, tool efficacy, and team performance work well for simple measurements. These include three key areas of time.

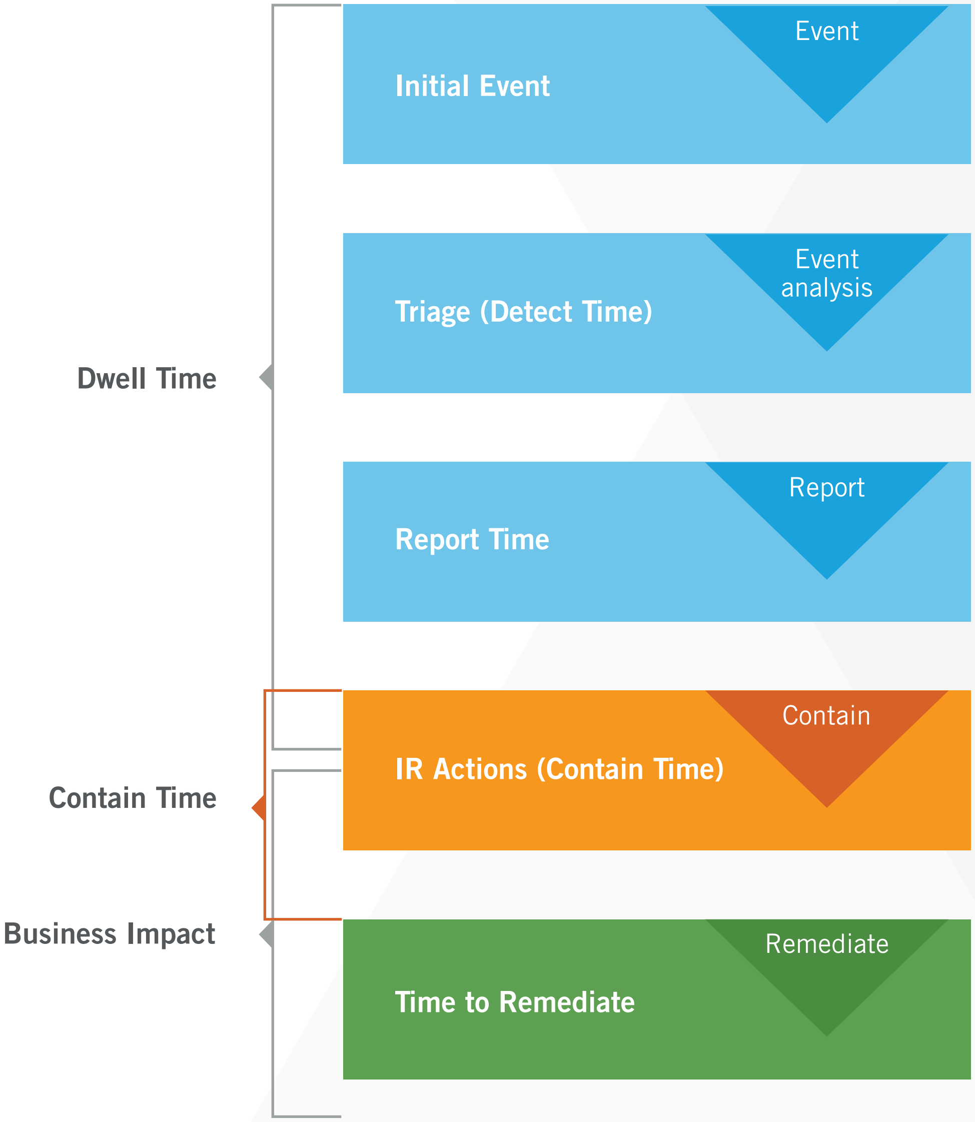
Time to detect. The time it takes to become aware a problem exists in an environment and an alert is raised. While often the most cited metric, detecting an incident is not the same as knowing what is important.

This metric helps with understanding the scope of the attack surface and how quickly detection tools and threat hunters can find a problem.

Time to know/acknowledge. The time between an alert being raised and when an analyst acknowledges that alert as a risk and begins an investigation. Where time-to-detect provides threat awareness, time-to-know is central to risk awareness.

Most SOCs are overwhelmed with alerts and struggle with assigning priority and severity to incidents. This means time is wasted investigating false alarms. Time-to-know gives insights into tool efficacy to prioritize threats with meaningful data in the context of risk.

Time to respond/remediate. This helps with understanding team performance and how well they are limiting the time attackers have access to the environment.



Dwell Time + Contain Time = Unauthorized Access Time to Asset

Incident response maturity and path to success

The core goal of incident response is to reduce attacker dwell-time as a form of risk mitigation but organizations must first define the level of risk to be mitigated.

It is important to consider incident response maturity and capabilities in relation to threats relevant to the business and the scope of impact these threats can create. Business risk awareness requirements define metrics and security spend to achieve appropriate response times.

In 2013, James Webb, CISO of Appalachian State University, proposed an incident response maturity model on a time axis, which Vectra® has adopted and evolved as part of our advisory security practice.

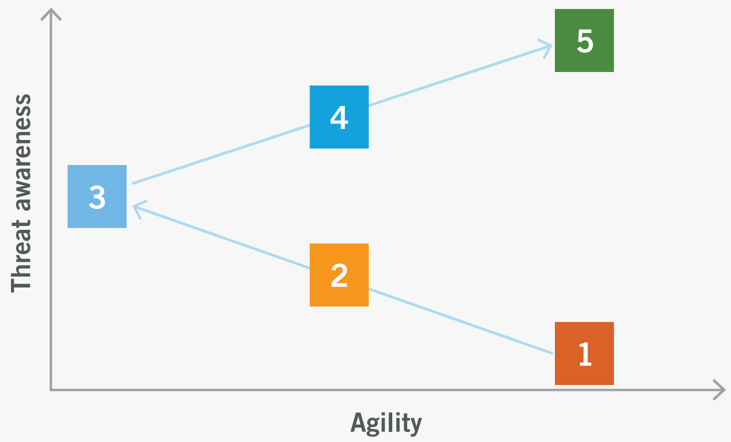
This model considers two core capabilities that are critical to incident response success:

Threat awareness/visibility. The ability to have accurate and reliable information about the presence of threat actors, their intentions, their historical activities, and how defenses relate to them. Time-to-detect and time-to-know are crucial.

Response agility/performance. The ability to quickly and sufficiently isolate, eradicate and return the business to normal operations. This involves the time-to-respond.

Most security maturity frameworks imply the adoption of tools to provide linear capabilities as a layered security approach. That methodology potentially leads to overlap and redundancy, which often has a negative impact on threat awareness and response agility. It also highlights tradeoffs between detection and response capabilities that occur at every level of maturity.

By relating these two attributes to the incident response process, maturity and capability can be defined and measured across the five stages of the maturity model based on the desired level of risk awareness.



Maturity	Typical Detection	Typical Response	Risk Awareness
Predictive Defense	Internal (Hunting, Deception) + External	Highly Proactive	Very High
Intelligence Driven	Internal (Hunting) + External	Threat/Adversary Driven	High
Process Driven	Internal (Hunting) + External	Service Driven (SLAs)	Medium
Tool Driven / Signature Based	External	Tool Driven	Low
Reactive / Ad-hoc	External, User Report	Reformat, Reinstall, Restore	Very Low

Levels of incident response maturity

Reactive/ad-hoc. This is the whack-a-mole approach, where the organization responds to threats only after they emerge. The detection of internal threats is usually from an external source.

Unfortunately, too many organizations still rely on this method of response when they discover a compromised asset. Restoring the system from backups makes it easy to be agile and quickly reclaim business functions.

However, threat awareness is low with no real knowledge gained about how the system was compromised or why and what it was used for after the compromise.

Tool driven/signature based. At this phase, organizations adopt tools that look for potential compromises in the environment. These are often signature-driven tools like antivirus software and IDPS, which provide some automated alerts about potential compromises from known threats.

The remediation of these compromised systems is also driven by tools that are designed to clear a system of compromise, which is incidentally not a good idea. Agility begins to diminish and leads to an ad-hoc response approach.

Process driven. At this phase, organizations adopt formal incident response roles, processes and governance structures. It often includes multiple sources of threat detection and alert correlations that map to phases in the attack lifecycle.

For many organizations, this is the ideal state of operations. Attacks are detected, analyzed and addressed in a cost-effective and repeatable manner.

Although formalized processes slow down agility, it is irrelevant because the volume of attacks tends to be low and most incidents are benign internal user errors or policy violations. The primary deficiency with this model is that dealing with targeted attacks requires more than just good processes.

Intelligence driven. For many large organizations, intelligence-driven incident response is a big goal due to the prevalence of targeted attacks.

This incident response level requires having a more detailed and up-to-date understanding of threat actors, including their objectives and motivation as well as their tools, tactics and procedures (TTP) profile. To achieve this goal, it is advisable to correlate with external knowledgebases like the MITRE ATT&CK framework.

The knowledge of adversarial disposition is then used to architect security defenses and detection controls in a manner that allows discrete actions to be taken to disrupt, degrade and deny the ability of adversaries to reach their objectives.

Predictive defense. Also known as active defense, this stage represents the convergence of incident response processes and an adaptive defense architecture that can be used to waylay adversaries when they enter, operate and move within protected environments.

One of the key characteristics of this model are capabilities that allow adversarial deception and denial of operations. Threat hunting is the ultimate expression of a proactive defense.

Incident response plan alignment

While time is the most important factor in incident response, time is also money.

How much to spend and how much threat awareness or agility is required to mitigate business risk depends on the unique needs of an organization. These needs differ based on size, industry and compliance requirements.

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident response process. Prioritization requires an understanding of the threat and risk to the organization. The classification of that risk drives the necessary maturity level of the organization.

Choosing the appropriate level

The level of maturity an organization must reach for incident response is based on the requirements for such a capability.

Industry-specific threats, risks and compliance requirements dictate the needs of an organization. Looking at the needs of other organizations in the same industry helps identify a good starting point for a target maturity level.

For example, a small company operating in the logistics business will not have the same requirement – or ability – to respond to cybersecurity incidents in the same way as a major corporate organization in the finance sector or a government entity.

In contrast, organizations with highly recognized brands or valuable intellectual property must enhance threat awareness by proactively hunting for attackers while maintaining the agility necessary to respond fast to the threats they find.

This goes beyond a maintained plan, concrete roles and responsibilities, lines of communication, and response procedures. A formal SOC plan and process is not enough to address the risk of targeted attacks.

Incident response and knowing when to automate

Measuring and improving total time of response is easier said than done. The reality is many organizations do not know their existing state of readiness to be able to respond to a cybersecurity incident in a fast, effective manner. And most don’t know what their level of risk awareness needs to be or an appropriate level of response.

More critically, even when the risk is known, lack the personnel or staff inefficiencies will not result in an effective program. A big percentage of a security analyst’s time is spent addressing unexpected events that an existing process cannot handle.

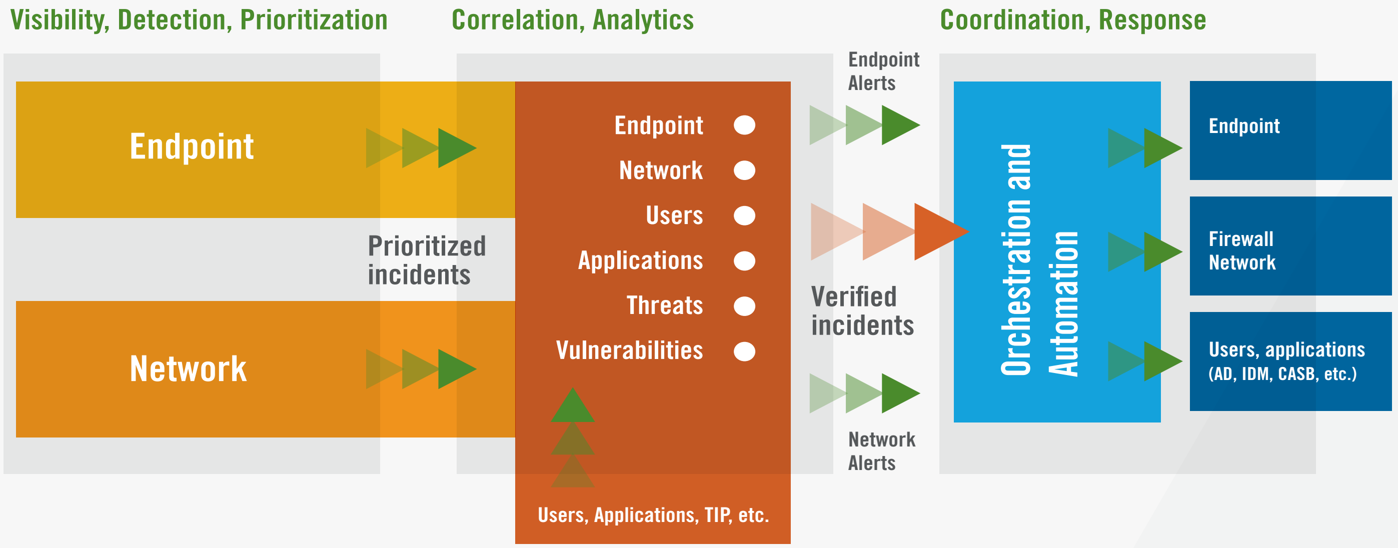
Security analysts perform a tremendous amount of tedious, manual work to triage alerts, correlate them and prioritize them. They often spend hours doing this only to learn that the alert is not actually a priority.

In addition, performing tedious, manual work introduces human errors. People excel at critical thinking and analysis, not repetitive manual work. Organizations have no recourse but to hire more people, reduce the workload or both.

Achieving the desired response time for a high level of threat awareness requires a thorough understanding about what tasks to automate and more importantly, when not to automate.

An efficient incident response process will keep people in the loop without giving them all the keys to the machines. Instead, the goal is to free-up the security analyst’s time to focus on higher value work that requires critical thinking.

The model below has three stages that show how automation can be applied to a detection and response process. It breaks down this way:



1. Visibility, detection and prioritization of attack indicators from endpoints and networks.
2. Analysis of endpoint and network data correlated with other key data sources.
3. A coordinated attack response across endpoints, networks, users, and applications.

Stage 1: Visibility, detection and prioritization

The network and its endpoints provide visibility and detection capabilities. They build upon visibility and detection data to provide the initial prioritization of an incident and immediate alerts.

Automation of the detection and triage process at this stage reduces the total number of reported events by rolling up numerous alerts to create a single incident to investigate that describes a chain of related activities, rather than isolated alerts that a security analyst has to piece together.

Assets and accounts central to an incident are contextualized and prioritized for threat and certainty. This information is then handed off to the next stage.

Stage 2: Correlation and analytics

In this stage, network and endpoint data are correlated with data from user, vulnerability and application management systems, as well as other security information like threat intelligence feeds.

The goal is to verify what was prioritized from the network and endpoint data and to prescribe the correct response based on severity and priority. This stage requires human analysis to make decisions based on environmental context and business risk. Highly refined and verified alerts are passed on to Stage 3.

> Achieving the desired response time for a high level of threat awareness requires a thorough understanding about what tasks to automate and more importantly, when not to automate.

Stage 3: Coordination and response

In this stage, playbook automation receives the prioritized response. This includes endpoint and network alerts generated by network detection and response (NDR) and endpoint detection and response (EDR) tools based on their respective analytic capabilities.

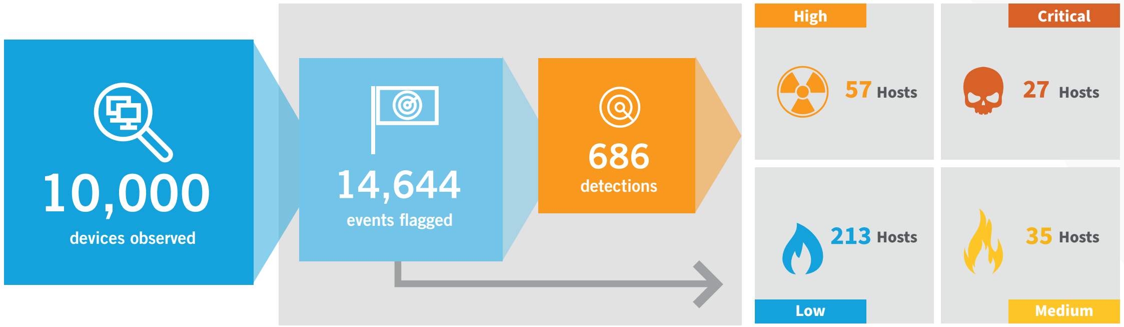
Automation and orchestration playbooks leverage the data provided from correlation and analytics. These playbooks coordinate an attack response across endpoints, networks, users, and application management systems.

The responses are executed at machine speed to mitigate the attack spread and can include human decision points to throttle the level of automation to appropriate levels for the situation.

The high degree of integration and interoperability between these platforms enables organizations to implement detection and response in a very practical and manageable configuration.

This minimizes the number of security tools and applications that are necessary to address the entire *detect*, *decide* and *respond* security cycle. This implementation also provides a higher level of maturity than most organizations currently achieve.

The approach does not just work in theory. It works in the real-world using NDR. We can look at metrics from existing organizations that deployed the Cognito® platform from Vectra to see the average workload reduction for detecting, triaging and prioritizing events by a Tier-1 security analyst.



Workload reduction from triaging, correlating and prioritizing events into incidents

For every 10,000 devices and workloads monitored in one month, the average peak count of host severity flagged 27 critical and 57 high-risk detections. These devices and workloads present the greatest threat to an organization and require a security analyst's immediate attention.

Over a 30-day period, this works out to roughly one critical detection and two high-risk detections per day that require immediate attention. While other events may occur, few are of actual interest and should be escalated to senior analysts or business units for deeper investigation.

Behavior-based machine learning algorithms are incredibly useful in performing repetitive work at speeds faster than humans can possibly achieve around the clock and without errors.

Machine learning delivers the deep insights and detailed context about in-progress cyberattacks, which enables security analysts to do the critical thinking to verify and to respond quickly to an incident. This is achieved by using a high-fidelity signal, which filters out the noise that leads to false positives.

This in turn reduces the skills gaps and barriers of entry into security operations as a junior analyst while freeing up the time of highly skilled senior analysts to focus on threat hunting and acting as risk advisers to business units.

For more information please contact a service representative at info@vectra.ai.

The takeaways

Remember these three key points:

1. Time is the most important metric for detecting and responding to attacks before damage occurs. Stopping persistent and targeted attacks requires rapid detection and response.

2. Increased threat awareness and response agility are the outcome of a mature incident response process. Understanding risks in relation to the appropriate levels of threat awareness and response agility is vital.

3. Machine learning works best when applied to specific tasks. It is well-suited to automating tedious, repetitive tasks while leaving the critical thinking and complex analysis to people.

Email info@vectra.ai vectra.ai