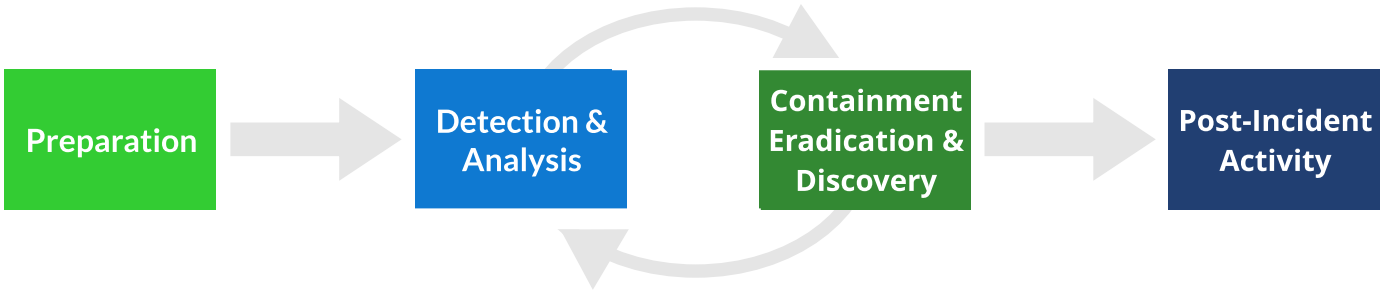
Infocyte

If they try it, we'll stop it.

INCIDENT RESPONSE

Infocyte is the only solution that will guarantee first hour response to your security events.

Incident response is the action(s) taken during a security event and immediately following that event. A good incident response capability allows you to effectively identify, mitigate the damage, and reduce the cost of a security event, while finding the root cause to prevent future attacks. Most organizations are not equipped to respond to a security event properly with their existing tools. Infocyte provides responders the information and context to make effective decisions and the power to enact those decisions across the entire network before the damage occurs or sensitive information is lost.



The NIST recommended phases for responding to a security event or incident

KEY STEPS FOR SUCCESSFUL INCIDENT RESPONSE

ASSEMBLE YOUR TEAM

Assembling a team of the right people, with the right skills and expertise is key. Ideally, you will have this team prepared and determined in advance. Depending on the event and the size of your organization, corporate communications, human resources, and your legal department should be looped in.

DETECT AND DETERMINE PATIENT ZERO

Once your team is assembled and aware of the security event, the first goal should be determining the cause of the breach. Was it a compromised user account or other source?

CONTAIN

Once the source or entry vector is determined, the goal is to isolate and contain any potential damage as quickly as possible. This can include isolating affected endpoints, ip blocks, and password resets.

RECOVER

Restoring needed services is the next critical step to ensure business continuity. Performing system or network validation, testing to ensure all systems are operational is the recommended first step. Next, re-certify components that were compromised as operational and secure.

KEY ELEMENTS OF SUCCESSFUL INCIDENT RESPONSE (CONTINUED)

ASSESS DAMAGE & SEVERITY

Assessment post-event is a critical part of the incident response process and as is preventing similar events in the future. The cause of an event also often determines next steps and whether an attribution investigation should occur.

NOTIFICATION

Some incidents will require notification if sensitive data is copied, viewed, or stolen by an unauthorized person. If this is the case, notify affected parties.

EVALUATE RESPONSE EFFORT & DISCUSS PREVENTION

Evaluating a response effort post-event helps organizations learn what processes worked, what didn't and how to better prepare for and prevent future security events.

INFOCYTE COMMAND WITH ACTIVE RESPONSE GUARANTEE

The first hour is critical to a successful response plan. This time should be considered as all hands-on deck, and Infocyte will be there guiding the way. In the first hour, Infocyte experts will work to uncover the scope of the attack and any additional threats, provide real-time critical information to a customer's team, and help secure the environment from active threats on devices from within the Infocyte platform.

Infocyte is confident in our process, procedures, and product. When fully deployed in the environment, we will find what other products miss.

Because our product is so powerful, when paired with our knowledgeable experts, we can guarantee results in the customer's time of need. If Infocyte does not provide tangible value in the detection, response, or resolution of a security engagement on covered devices, Infocyte will happily return the prorated balance of the customer's agreement.

Learn more:
www.infocyte.com

ABOUT INFOCYTE

Founded by the leaders of the United States Air Force Cyber Incident Response Team (AFCIRT), Infocyte is the globally trusted leader in proactive threat detection and incident response. The world's leading security and incident response companies use Infocyte's platform to proactively detect and respond to vulnerabilities and threats within their customers' endpoints, data centers, and cloud environments. Infocyte's team and partner ecosystem help organizations maintain compliance, stop ransomware and account takeover, reduce risk, optimize security operations, and scale security teams. Infocyte is the faster, simpler, smarter way to detect and orchestrate response to sophisticated threats. Learn more at infocyte.com or follow us on Twitter @InfocyteInc.