BE PREPARED

EFFECTIVE INCIDENT RESPONSE READINESS

The official motto of Boy Scouts and Girl Scouts is “Be Prepared.” And for good reason! Being prepared increases the chances of success in the face of emergencies, when time is in short supply. Preparation includes scenario planning, assigning roles and responsibilities, and having the necessary tools and supplies on hand before they are needed.

Leverage an analytics platform to correlate this data, improve forensic analysis, and help prioritize events.

Put procedures in place in advance of a significant incident. Defined processes and roles establish focus and control. Ad-hoc efforts lead to ad-hoc results, which can leave dangerous gaps in an organization’s defenses.

An effective Incident Response team is an ensemble; a group of individuals with specific cyber security training, expertise, complementary skills, and a strong sense of common purpose. Be honest with yourself. Objectively assess your security stance against best practices. Enterprises that fail to evaluate Incident Response plans against new threats expose their systems, data and infrastructure to attack.

THE COMPLEX, DYNAMIC WORLD OF CYBER SECURITY IS NO EXCEPTION IF YOU WANT TO RECOVER QUICKLY FROM A PRECARIOUS SITUATION.

Employ a centralized or real-time monitoring/alerting system that provides visibility across logs, network packets, Netflow and endpoints.

Even the most competent cyber security team often needs help. Partner with an external expert in advance of a major incident… and put them on speed dial.

Proper incident detection, investigation, and analysis systems are essential for maximizing the skills of your security staff, and automating processes for maximum efficiency.

Key roles can be filled by service providers or contractors in lieu of, or in addition to a full-time staff.

Have a baseline of “normal” network traffic, usage and other operational details to help identify “abnormalities.” Institute or improve formalized incident response tracking and workflow.

Keep it fresh. Incident Readiness isn’t a one-time set-and-forget exercise. Regularly review and update. Continuous monitoring is best. At least monthly is recommended.

Define a detailed Service Level Agreement (SLA), a contract that identifies specific services to be delivered and performance metrics to be met, such as response time, cyber security objectives, and data breach liability.

Roles and responsibilities should be clearly defined, differentiating between the management of the security monitoring infrastructure, the management of incidents, and the management of security analysis.

Expertise should include incident detection, forensics, malware analysis, threat intelligence, and breach management.

A typical staff model might include a threat intelligence analyst, an analysis and tools support analyst, and a Tier 1 and Tier 2 analyst, all reporting to the security operations center manager.

Ensure that you leverage internal threat intelligence and have a reliable, continuous source of external threat intelligence to help detect as well as better understand the nature of an attack.

EQUIP THEM.

HAVE A HANDBOOK.

KEEP BACK UP ON STAND-BY.

ASSEMBLE THE RIGHT TEAM.

For procedures in place to be effective, a policy must ensure that personnel are trained and made aware of their responsibilities, which can leave dangerous gaps in an organization’s defenses.

ASSEMBLE THE RIGHT TEAM.

EQUIP THEM.

HAVE A HANDBOOK.

KEEP BACK UP ON STAND-BY.

Be honest with yourself. Objectively assess your security stance against best practices. Enterprises that fail to evaluate Incident Response plans against new threats expose their systems, data and infrastructure to attack.