EXPERT PERSPECTIVES

corelight

EIGHT TENETS OF ELITE SOCS

From an interview with Richard Bejtlich

What's the secret of peak SOC performance?

After decades leading some of the country's top incident response teams in both the private sector and U.S. military, Richard Bejtlich, Corelight's Strategist and Author-in-Residence, says it's often undocumented practices that set a security operations center (SOC) or incident response team on a course to maximizing its effectiveness. "You need good evidence, including good network evidence. You need people who understand the evidence in terms of the conditions of your environment. And those people need the authority to act based on that evidence."

Bejtlich offers eight tenets for high-performing SOCs. "Some may be controversial," he says. "But each helped my teams anticipate threats and act fast, while developing and retaining great talent and building institutional knowledge."

Richard Bejtlich

has served as chief security strategist at FireEye, CSO of Mandiant, and director of incident response at General Electric, and worked as a military intelligence officer in the US Air Force. You can follow his work on his **TaoSecurity website**.

1 CUSTOMIZE SIGNATURES TO THE ENVIRONMENT

Rather than risk alert fatigue by running thousands of rules, start from scratch to create custom alert rules specific to the organization's conditions.

2 DON'T YOKE ANALYSTS TO A SINGLE TOOL OR WORKFLOW

Prevent burnout by allowing analysts space for "unstructured" work using various tools to solve diverse problems, while still clearly defining expected roles.

3 ALIGN DETECTORS' AND RESPONDERS' INCENTIVES

Incentivize detection analysts to resolve what they can, and work with qualified responders when they max out their current skill set.

4 BUILD A MULTI-SOURCE VERSION OF EVENTS

Combine 3rd party information, network security monitoring, log and application data, and endpoint data for comprehensive situational awareness.

5 PEOPLE ARE NOT NUMBERS

Use titles such as "Event Analyst" and "Incident Handler," rather than "tier 1" or "tier 3" to encourage employees to view the SOC's mandate strategically.

6 FACILITATE ANALYST CROSS-TRAINING AND PROMOTION

Give talented analysts opportunities to work in development, infrastructure, intelligence, and other roles, beyond their initial core competency.

7 VIEW THREAT HUNTING AS AN "INDICATOR-FREE" DETECTION

Discuss threat hunting as an essential tool in the incident detection kit that every analyst should learn to use creatively, rather than as a function performed by a separate team.

8 PRIZE AND ACKNOWLEDGE ANALYSTS' EXPERIENCE

"AI is a powerful tool for improving analyst productivity, but if you're replacing people with AI then your process likely needs refactoring," Bejtlich says. "There's currently no replacement for creativity and familiarity with the protected environment."

corelight.com