OmniSOC

A shared cybersecurity operations center for higher education and research

OmniSOC is a 24×7×365 shared cybersecurity operations center (SOC) that is sector-specific for higher education and research. OmniSOC collects cybersecurity data from partners; integrates this data with other threat intelligence; conducts proactive threat hunting; and monitors, triages, and analyzes security events. This pioneering initiative accelerates the pace of mitigation for dynamic threats by reducing the time from first awareness of a cybersecurity threat anywhere to mitigation everywhere for its members. OmniSOC was founded by Northwestern University, Purdue University, Rutgers University, the University of Nebraska-Lincoln, and Indiana University.

A sector-specific SOC has become an essential element of a higher education information security strategy. The danger is clear and present: IBM's *2018 Cost of a Data Breach* notes that higher education organizations average 217 days to find a threat and 84 days to contain it. In 2019 alone, 89 U.S. universities, colleges, and school districts became victims of ransomware attacks, followed by at least 30 in the first five months of 2020. Successfully targeted institutions range in size from Tier 1 universities to smaller, private colleges, with known ransom payments exceeding $3.1M.

Higher education institutions, such as SUNY and UT Austin, have validated the need for a higher education/research sector-specific SOC, responding with system/state-wide SOCs. In 2018, the National Science Foundation created the ResearchSOC, building on the OmniSOC, to provide SOC capability for its Large Facilities and research projects.

OmniSOC provides a cost-effective response to three key inconvenient truths:

- Pouring more money into building out higher ed local security teams does not grow efficiency in scale or accelerate pace and will not materially address the changed cyber-threat landscape.
- Information technology is broken in terms of security and no fix is on the horizon; humans do human things; and the nefarious actors are organized, industrialized, and growing in sophistication.
- If an institution's pace of information sharing and remediation is measured in days, then it is using the wrong unit of measurement for the pace of the cybersecurity risks that higher education confronts today.

It is against this reality that OmniSOC provides an approach to cybersecurity that dramatically accelerates the pace of risk mitigation. Investments in core cybersecurity capabilities and staff will always remain important, but the game has shifted to scale and pace. OmniSOC's sector-specific cybersecurity addresses both within a common risk framework.

ESSENTIAL FEATURES

Bringing greater sophistication to higher education threat detection and response. OmniSOC enhances the work of local campus security professionals to provide greater real-time, sophisticated threat detection, analysis, and action for its members.

Leveraging collaboration to identify and respond to threats more quickly. OmniSOC helps higher education institutions reduce the time from first awareness of a cybersecurity threat anywhere to mitigation everywhere through real-time data aggregation, collaboration, information sharing and interconnectivity.

Providing a specialized cybersecurity service specific to higher education's cyber environment. OmniSOC looks through the common lens shared by higher education professionals. Individuals are members of the higher education community with experience operating in and meeting the specific challenges of that community.

Von Welch ◆ OmniSOC Executive Director ◆ vwelch@iu.edu ◆ omnisoc.iu.edu

KEY SERVICES

Leverage State of the Art Cyber Threat Intelligence
Integrate strategic and tactical threat intelligence into analysis, processes, and technology to understand, identify, and counter threats and threat actors more efficiently and effectively. Create new, analyze and enrich existing, and share resulting threat intelligence.

Quickly Notify Member Incident Response Teams
Notify member incident response teams of adverse events or incidents that may require additional investigation or action. Provide relevant details, including context, timeline, and scope, in notifications to facilitate member team interpretation and action.

Communicate and Share Information
Provide timely, routine, and useful communications regarding threats and threat actors. Share effective operational practices, tools, and procedures. Report on organizational status, including operational and security metrics.

Conduct Proactive Threat Hunting
Proactively searches for threats that evade network and system defenses, including those undetected by existing security systems. Works with member institutions to assess full scope, impact, and severity of adverse events. Automates investigation and analysis using machine learning, visualization, correlation, scripting, and dashboards to streamline future threat hunting activities.

Analyze Security Events
Investigates cases escalated from OmniSOC tier 1 analysts. Performs in-depth analysis of security alerts and associated data feeds from member systems and networks. Determines what actually happened based on analysis, to validate or refute the potential adverse events. Works with member institutions to assess full scope, impact, and severity of adverse events. Automates analysis using custom signatures and dashboards to streamline future similar event handling.

Monitor and Triage Security Events
Provide tier 1, 24×7×365 monitoring of security alerts and associated data feeds from member systems and networks. Provide preliminary analysis of relevant events and triage based on the criticality/severity of the event, associated system, and/or service. Escalate events as appropriate to member incident response teams or OmniSOC tier 2 analysts.

PRICING

OmniSOC pricing is based on GB data / day total across all feeds, the need for virtualization structure, and number of days of retention desired, if over 30 days. Detailed pricing is available upon request.