Novus Security Program Details

- The Security Program is designed to establish the basics of a functional cybersecurity program for new and existing managed support clients of Novus Insight, Inc. (Novus). The chief goal of the program is to enhance and support the client's cybersecurity incident detection and response capabilities, using comprehensive tools and expertise to address the following elements of cyber incident response:
- Preparation
- Detection
- Containment
- Initial Investigation

Preparation

Novus helps organizations stop attacks before they happen by implementing security best practices in cloud services like Microsoft 365 or Google Workspace, and taking a modified, risk informed, version of the Center for Internet Security (CIS) Benchmarks to configure cloud environments to industry security best practices. Novus focuses on configurations related to email filtering, alert management, multifactor authentication, basic data loss prevention (e.g., financial data, such as credit card numbers, as well as social security numbers, etc.), and other recommended security best practices. Novus configures alerts form cloud environments to notify the Security Operations Center (SOC) if a "High or Critical" event has been detected related to identity, email security, data loss, or risky user behavior. In addition to the cloud security standards, Novus' security program applies security best practices, based on CIS Benchmarks, to Windows and Macintosh endpoints. Novus also implements 24/7 monitoring and response (supported by Huntress) on endpoints—in the event of a security incident, the 24/7 security operations team will isolate machines from the network to prevent the spread of an attack.

Furthermore, because every Novus client bears their own responsibility to safeguard against cyberattacks, Novus also provides discounted licensing for end-user basic cybersecurity training, and will consult with the executive leadership of each organization to establish and test a formal Incident Response Plan. Each of these elements support the pillar of Preparedness and are typically requirements of most cyber insurance providers.

Detection

Novus collects alert and event data from a variety of sources to ensure endpoints, network infrastructure, and user identity are actively monitored. As indicated above, cloud events and alerts from supported cloud environments (Microsoft 365 and Google Workspace) and endpoint alerts from Huntress are forwarded to the Novus SOC for investigation.
Alert sources and monitoring include:

- Endpoint alerts of enrolled assets are monitored 8x5 by the Novus SOC, and 24/7 by a third-party SOC (i.e., Huntress).
- Microsoft 365 and Google Workspace are monitored by the Novus security team per the managed support schedule (8x5, Monday-Friday, w/after-hours "on-watch" schedule).
- User reported alerts to the Novus helpdesk are monitored 8x5, Monday-Friday.

Containment

The primary containment goal of the SOC is to minimize the impact on the client's systems and data. During an incident, containment can be disruptive. While the precise activities associated with the containment pillar of incident response cannot be predicted beforehand, generally, clients must be aware that, if the situation calls for it, clients may be required to allow the SOC to disable accounts, revoke session credentials, isolate computers, and conduct other activities as necessary to ensure the incident remains contained. Clients must not interfere with the containment activities and must prepare their staff for potential disruption of work in the event of a cyber incident.

Investigation

As part of the containment process, the SOC will make every effort to maintain and preserve evidence to support additional investigation. Novus' role in an investigation is to determine the protentional scope of the incident, including affected assets, people, and systems, and ensure that additional containment activities are not required. At the point that the incident has been declared sufficiently contained, Novus will recommend that the organization's cyber insurance provider be engaged to conduct a more thorough investigation, including determining the legal, reputational, and regulatory scope of the incident. Detailed forensic investigations, data loss analysis, and any additional investigation beyond what is required to determine the incident scope and to provide for initial containment is outside the scope of Novus Security Services.

Terms and Conditions

- Scope of Services:
    - The Security Operations Center (SOC) will monitor, detect, and respond to security alerts and incidents on behalf of the client.
    - The primary goal of the SOC is to contain incidents and minimize the impact on the client's systems and data.
    - Upon detection and containment of an incident, the SOC will promptly document all relevant details and provide them to the client for further action.
    - The SOC will facilitate communication with the client's cyber insurance provider, providing incident details as required for additional investigation.

- Client Responsibilities:
    - The client must provide access to relevant systems, networks, and data necessary for the SOC to effectively monitor and respond to security incidents. This includes maintaining adequate licensing for monitoring, detection, and containment tools. The client must maintain appropriate cybersecurity measures as recommended by the SOC and their cyber insurance provider.
    - The client must promptly notify the SOC of any changes in their network infrastructure or security posture that may affect SOC operations.
- Minimum Technical Requirements:

        - The client's systems and networks must be equipped with up-to-date security software and configurations, including firewalls, intrusion detection/prevention systems, and antivirus solutions.
        - The client is responsible for maintaining systems to ensure they meet the requirements of the SOC monitoring, detection, and containment tools.
        - The client must implement logging and monitoring mechanisms to enable the SOC to detect and analyze security events effectively.
        - Access controls must be enforced to restrict unauthorized access to sensitive data and critical systems.
        - The client must have mechanisms in place for secure communication and collaboration with the SOC.
        - The client must maintain adequate Microsoft 365 and/or Google Workspace licensing. Without adequate licensing, the SOC will be unable to properly detect, contain, and investigate cyber incidents.
        - The client must maintain adequate log retention capabilities per legal and regulatory requirements.
- Minimum Insurance Requirements:
    - The client must maintain cyber insurance coverage with a reputable provider that includes coverage for incident response, forensic investigation, and potential liability arising from security breaches.
    - The client must provide the SOC with necessary information regarding their cyber insurance policy, including contact details for the insurance provider and policy numbers.
    - The client must adhere to any requirements or guidelines set forth by their cyber insurance provider and/or regulatory agencies regarding incident reporting and cooperation with third-party security providers like the SOC.
    - The client must maintain all technical and operational standards required by the cyber insurance provider.
- Confidentiality and Data Protection:
    - The SOC will treat all client information and data obtained during the course of providing services as confidential and will not disclose it to third parties without the client's consent, except as required by law.
    - The SOC will implement appropriate measures to safeguard client data against unauthorized access, disclosure, or alteration.
- Limitation of Liability:
    - The SOC's liability for any damages arising from its services shall be limited to the fees paid by the client for those services.
    - The SOC shall not be liable for any indirect, incidental, or consequential damages, including but not limited to loss of data, loss of revenue, or loss of business opportunity.

Out of Scope

- Incident Investigation Beyond Containment:

    - The SOC's responsibility is limited to detecting and containing security incidents. Detailed forensic analysis or investigation beyond containment is considered out of scope.
    - Any further investigation required beyond containment will be the responsibility of the client and their designated cyber insurance provider.
- Legal and Regulatory Compliance:
    - Compliance with legal and regulatory requirements, such as data protection laws or industry-specific regulations, is the responsibility of the client.
    - The SOC does not provide legal advice or ensure regulatory compliance, and any activities related to compliance assessments or audits are considered out of scope.
- Physical Security:
    - Physical security measures, including access control to facilities, surveillance systems, and security personnel, are not within the purview of the SOC's services.
    - The client is responsible for implementing and maintaining physical security measures to protect their premises and assets.
- Software Development and Code Review:
    - Development of custom software applications, code review, or secure software development practices fall outside the SOC's scope.
    - The client is responsible for ensuring the security of their software applications and conducting appropriate code reviews as necessary.
- Employee Training and Awareness:
    - Employee cybersecurity training and awareness programs are excluded from the SOC's services.
    - The client is responsible for educating their employees about cybersecurity best practices and promoting a culture of security within their organization.
- Incident Response Planning:
    - Development or implementation of incident response plans, including the creation of playbooks or response procedures, is not included in the SOC's services.
    - The client is responsible for developing and maintaining their incident response plans, tailored to their specific business needs and regulatory requirements.
- Incident Reporting:
    - Although Novus will provide an incident summary report to the client at the conclusion of containment activities, the client is responsible for adhering to all regulatory, governmental, law enforcement, insurance, contractual or other reporting requirements the client is required to comply with.
    - Novus is not responsible for client adherence to reporting timelines.
- Incidents Caused by Client Negligence or Misconduct:
    - Incidents resulting from the client's negligence, misconduct, or intentional actions are excluded from the SOC's liability.
    - The client is responsible for maintaining adequate security measures and adhering to security best practices to prevent security incidents caused by their actions or inactions.
- Third-Party Services and Products:

- Security incidents related to third-party services or products used by the client, including cloud services or software-as-a-service (SaaS) solutions, are excluded from the SOC's scope.
- The client is responsible for assessing the security and compliance posture of third-party vendors and ensuring the security and compliance of any services or products they utilize.