Comcast Business

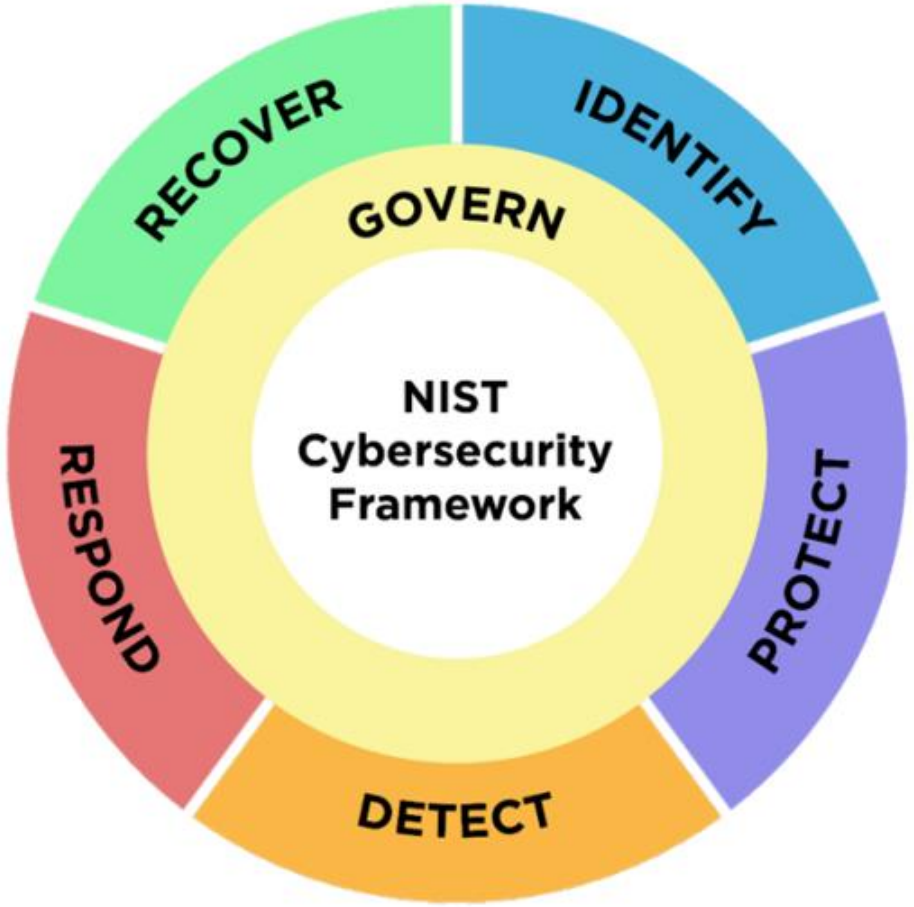
Advanced Security Solutions

Rich Korn

Senior Security Solutions Specialist

NIST Cybersecurity Framework

Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Cybersecurity Supply Chain Risk Management
	Roles, Responsibilities, and Authorities
	Policies, Processes, and Procedures
	Oversight
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication



COMCAST BUSINESS

Comcast Business Managed Security Services

Threat Monitoring and Response **TMR**

Fortinet Edge Devices

Monitors FW and UTP Components

24/7 Detect and Response

EDGE SECURITY & VISIBILITY

Adds security monitoring and response for SD-WAN sites

Endpoint Detection and Response **EDR**

Laptops, desktops, and servers

Malware and Ransomware Prevention

Device Security 24/7 Detect and Respond

DETECT & MINIMIZE IMPACT

Next-gen endpoint threat detection and response capabilities for users and server assets

Managed Detection and Response **MDR**

Monitors Entire IT Environment

Covers Endpoint, Servers, Network and Cloud

24/7 Detect and Respond

PREVENT & DETECT

Designed to monitor the entire IT environment with multiple layers detection & response in a single solution

COMCAST BUSINESS

How the Security Operations Center (SOC) Works

Core Responsibilities

- 24/7 Prevention and proactive security monitoring with fast incident response for identified threats with remediation advice based on business impact [CONTEXT MATTERS!!!]
- Continuous data enrichment with rule curation, AI/ML automation and integration combined with SOAR
- End-to-End MDR & EDR analysis with reporting to identify threats with remediations, KPIs for top threats, risk categorization, with MITRE ATT&CK
- Threat intelligence, collect & curate intel, identify suspicious behaviors and detect existing IoCs
- Threat hunting - proactively search for IOCs, retroactive searching, curate new threat detections, and internal investigations

Protecting the Endpoint

Anti-Virus vs. EDR

Anti-Virus

- Signature-based
- Reactive
- File scanning
- Warnings

EDR

- Real-time threat detection
- Behavior-based
- Automated remediation
- Forensic capable

MDR Features

Log Management and Search		Analyze the most complex data and find insights faster with InsightIDR's cloud-native data lake, diverse log collection capabilities, custom log parsing, and flexible search and reporting.
Dashboards and Reporting		Access pre-built dashboards and reports out-of-the-box or create your own custom ones to best suit your organization's needs.
Investigation Console		View your aggregated alert data in InsightIDR's investigations console to quickly search your active investigations and gather the context you need to effectively prioritize, sort, and respond to alerts.
File Integrity Monitoring (FIM)		Collect File Integrity Monitoring events with the Insight Agent so InsightIDR can attribute users to file modification activity. You can then create alerts based on certain file log events to notify you when one of your users modifies a critical file or folder. Compliments existing FIM Tools.
Intrusion Detection System (IDS) & Network Traffic Monitoring		Monitor for malicious activity and policy violations on your network with an Intrusion Detection System (IDS) device.
Curated Threat Detections Library		Leverage InsightIDR's curated threat detections managed by Comcast & Rapid7's threat intelligence teams. Capitalizing on our open-source community engagement, spanning known and unknown threats, and utilizing advanced attack surface mapping and proprietary machine learning, InsightIDR offers you wide threat coverage across your environment.
Attacker Behavior Analytics (ABA)		Hunt for unique attacker behavior with ABA detection rules. With our ever-growing detection library, you'll be covered against even the newest of threats.
User and Entity Behavior Analytics (UEBA)		Identify compromised credentials, lateral movement, and other malicious behaviors with User Behavior Analytics detections.
Deception Technology		Deploy deception technology in the form of honeypots, honey files, honey users, and honey credentials to learn how attackers are attempting to access your systems.
Enhanced Endpoint Telemetry		Unlock comprehensive attack details, proactively hunt for threats, and tailor custom alerts to align your specific security policies and standards with Enhanced Endpoint Telemetry.
Enhanced Network Traffic Analysis		Access raw network flow data and rich metadata collected by the Insight Network Sensor with Enhanced Network Traffic Analysis. This metadata includes IP addresses, ports, content-based application recognition, and metadata attributed to specific users and devices.
Core Automated Response Workflows		Respond quickly and confidently with automated out-of-the-box workflows, including endpoint containment, Insight Agent containment, and more.