

NGSO key contacts



Chris L Crevits
Partner/Principal • St Louis
NGSOR Leader
chris.crevits@ey.com
+13142901786



Adam Malone
Partner/Principal • Atlanta
Threat Detection and
Response Leader
adam.malone@ey.com
+14048175028



Noelle Hardy
Managing Director • Columbia
Application Security Leader
noelle.hardy@ey.com
+13017851040



Keith Mularski
Managing Director • Pittsburgh
Cyber Threat Intelligence
Leader
keith.mularski@ey.com
+14126440612



David P Trollman
Senior Manager • Detroit
SOC Transformation Leader
david.trollman@ey.com
+13136288407



Rishi Pande
Senior Manager • Chicago
Application Security Leader
rishi.pande@ey.com
+13128792697



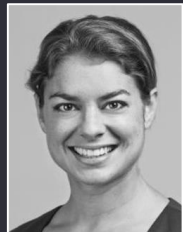
Haris Shawl
Senior Manager • McLean
Cyber Threat Intelligence
Leader
haris.shawl@ey.com
+15715658511



James Dunn
Sr. Manager • Dallas
Incident Response Leader
james.dunn1@ey.com
+12149690694



Tiger Jaser
Senior Manager • Philadelphia
Advisory, Risk, Cyber Security
Vulnerability Management
Leader
tiger.jaser@ey.com
+16152522199



Elizabeth Cartier
Senior Manager • Hoboken
Incident Readiness Leader
elizabeth.cartier@ey.com
+12015514271



Alex Andrucioi
Senior Manager • Houston
Threat Emulation Leader
alexandre.andrucioi@ey.com
+17137504808

EY Cybersecurity

Next Gen Security Operations and Response (NGSO&R) Service Catalog

Americas cybersecurity practice leaders

Domain	Name	City	Email	Phone
Cyber Leader	Dave Burg	McLean	Dave.Burg@ey.com	(703) 887-8337
DPP	Kyle Harvey	New Orleans	Kyle.Harvey@ey.com	(225) 252-4311
IAM	Chris Hall	Pittsburgh	Chris.Hall3@ey.com	(724) 396-3677
SRC&R	Justin Greis	Chicago	Justin.Greis@ey.com	(312) 342-4202
NGSOR	Chris Crevits	St. Louis	Chris.Crevits@ey.com	(618) 407-1093
AE&ET	Joshua M Axelrod	Portland	Joshua.Axelrod@ey.com	(503) 414-7961



NGSO&R Overview

EY's Next Generation Security Operations and Response (NGSOR) services and solutions help build a more secure and trusted working world by helping our clients protect their business with proven strategic and tactical solutions to defend, detect, respond and recover from cyber attacks



Questions we aim to answer



- ▶ Do I have an active intruder or malware infection in my environment?
- ▶ What threats might be targeting me?
- ▶ What capabilities and investments should I make to transform my threat detection and response capabilities?
- ▶ What strategic and tactical improvements must I make to improve my cyber defenses?
- ▶ How do I build more secure products and software?
- ▶ Is my organization properly prepared to respond to a cyber compromise?
- ▶ What is the scope of my cyber incident?
- ▶ Have I successfully eradicated the intruder/infection from my environment?
- ▶ What vulnerabilities do I have in my managed assets and what must I do to remediate them?

- SOC Transformation**
 - ▶ SOC assessment, strategy and roadmap
 - ▶ SOC build / transform
 - ▶ SOC technology requirements analysis/selection
 - ▶ SOC governance, playbooks, metrics and reporting
 - ▶ Co-source SOC
 - ▶ Managed Threat Detection and Response Service
- Cyber Threat Resiliency**
 - ▶ Cyber threat resiliency assessment
 - ▶ Threat hunting
 - ▶ Cyber threat defence assessment
- Cyber Threat Intelligence**
 - ▶ Threat intelligence as a service
 - ▶ Threat landscape assessment
 - ▶ Threat footprint assessment
 - ▶ Threat research on demand
 - ▶ Threat intelligence program consulting
- Incident Readiness**
 - ▶ Incident readiness and maturity assessments
 - ▶ Cyber crisis simulation (e.g., table tops)
 - ▶ Incident response governance, playbooks, metrics and reporting
- Incident Response**
 - ▶ Incident response retainer
 - ▶ Incident management consulting
 - ▶ Incident containment, eradication and recovery assistance
 - ▶ Cyber incident post-mortem analysis

Threat Detection and Response



Vulnerability Discovery and Response

- Threat Emulation**
 - ▶ Internal, external, wireless, applications and mobile attack and penetration testing
 - ▶ Red Team threat emulation assessments
 - ▶ Cloud security assessments
 - ▶ Product security assessments
- Application Security**
 - ▶ Application Security Assessments
 - ▶ Secure application architecture assessments/ threat modelling
 - ▶ Application security program build
 - ▶ Secure digital/ DevSecOps
 - ▶ eLearning for Secure Application Development
 - ▶ Managed Application Security Service
- Vulnerability Management**
 - ▶ Program maturity assessment
 - ▶ Asset discovery and profiling
 - ▶ Enterprise vulnerability management program governance design
 - ▶ VM program improvement strategy and roadmap
 - ▶ Cyber exposure assessment
 - ▶ Scanning technology implementation and optimization
 - ▶ Vulnerability and secure configuration scanning
 - ▶ Vulnerability remediation assistance
 - ▶ Vulnerability response and risk mitigation support
 - ▶ Managed Vulnerability Discovery and Response Service