secureCENTRX

Precision Information Security

Fundamentals in InfoSec – With a Difference

- **Security Audits & Assessments –** Risk-based information security controls development
- **Penetration Testing –** Continuous, Alternative Intelligence-driven state-of-the-science proof points
- **Software and Systems Testing** – An area of deep domain expertise, including Threat Modeling
- **Managed Security Operations-** For organizations that do not fund a full Infosec staff

Why secureCENTRX?

secureCENTRX

Culture of Excellence

Expert Knowledge

Ethical, vetted white-hat practitioners

Premier industry certifications

In-depth Experience

60+ projects/year

Hundreds of collective person-years of experience

Focused only on information security

Innovation: *tactics, techniques, and procedures*

Integrity: *trusted by enterprises & security vendors*

Methodology: *highly structured processes*

Quality: *relentless pursuit of proactive security*

Trust*: never assumed, always earned*

Offensive Security: *prevention over reaction*

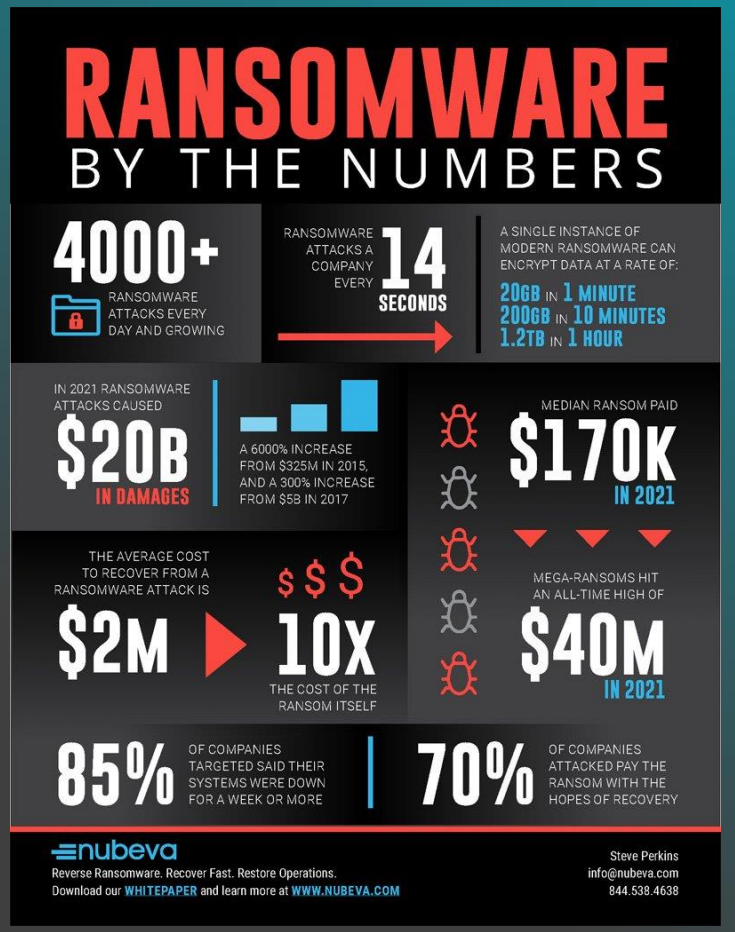
secureCENTRX is a privately-held information security consulting firm

Financial, Information Security Vendors, Software Manufacturers, Retail, Healthcare, Manufacturing

Harsh Reality

"Ransomware is getting ugly" – Bruce Schneier

- Ransomware and Persistent Threats are increasing exponentially
- 82% increase over 2020 (2,686 successful attacks: Crowdstrike)
- 58% Ransomware victims paid; 14% paid more than once
- 58% of victims took more than a month to recover
- Costs
  - Downtime and disruptions to business
  - Brand reputation
  - IT time, resources and services
  - Legal expenses
  - Cash - $$$$$$
    - Colonial Pipeline - $4.4 million
    - CNA - $40 million
    - Kaseya - $70 million
    - Mid-size business averaged $812,000



Advanced Persistent Threats

An illegal, long-term connection to a victim's network

Your network hangs in the balance

"One ought to design systems under the assumption that the enemy will immediately gain full familiarity with them." - Claude Shannon

- Nation-states are using APTs to attack IT, telecoms, utilities, industry control systems, aviation, automotive, academic, pharmaceutical, government and security sectors around the world.
- SolarWinds was a supply chain attack compromised about 100 companies and 12 government agencies including Microsoft, Intel, Cisco, the Treasury, Justice and Energy departments and the Pentagon
- REvil Ransomware-as-a-Service (RaaS) organization, most recently attacked meat supplier JBS, which ultimately paid $11 million to get its processing plants back online.
- Kaseya was a REvil APT that infected more than 1,500 organizations.

secureCENTRX

Precision Information Security

Testing and Response

Vulnerability Management
Penetration Testing
Red Teaming
Major Incident Response
Program Development
Ransomware Defense

Securing Software

Secure Development
Threat Modeling
Penetration Testing
Web Application Firewalls
Program Development
Ransomware Defense

Governance, Risk and Regulatory

Audit Support
Risk Programming
Assessment
Policies and Procedure
IT Control Framework
InfoSec Management System

Security Operations Center

7x24x365
Extended Detection and Response
Security Incident Response Management

secureCENTRX

Unique Offerings

- **True Red Teaming** – Adversary Emulation: incident preparedness and response programming
- **Software and Systems Testing** – inlcuding advanced Threat Modeling
- **Ransomware Prevention Programming** – A curated, comprehensive institutional shift in action
- **vCISO consulting –** References available upon request
- **Secure Software Development Lifecycle** – Uniquely qualified practitioners with advanced tools
- **Process Management –** risk-based approach to ISMS aligned to business objectives
- **Cyber Awareness Training –** environment-based content to be automated with metrics baked in
- **Managed Security Operations-** High-caliber TTP for firms who do not fund a complete InfoSec team

Adversary Emulation

True Red Teaming

Security & Vulnerability Assessment
M-Theory Group's RECON: **BLACK**

Cybersecurity Health Check

- Network Vulnerability Scan
- Autonomous Penetration Testing
- Vulnerability Assessment Report
- External testing of systems: web applications, API endpoints, Cloud, external/publicly facing assets
- Internal testing of systems: Active Directory, Windows, Linux, Firewall, and other internal systems
- Remediation Guidance

Single package for baselining through advanced TTP and Expert Security Practitioner prioritization

M-THEORY

Tooling -

TechnologyPartners

Innovative and disruptive infosec solutions
Scalability through
Automation
Alternative intelligence
Tactics, Techniques, and Procedures
Productized Information Security Services
In-house Security Operations Center

Acreto - SASE
Beauceron – CyberAwareness Training
Horizon3 – Autonomous Penetration Testing
Titaniam Labs – Data-in-Use
Cybertrap – Deception Technology
Zero Touch -
Avocado Systems – Threat Modeling at Runtime
Cycode – Secure Software Development Lifecycle

Forgerock – Identity Access Management
Polyswarm – Threat Intelligence Feed
Shiftleft.io – Software security
Hypori – Mobile Device Management
Rumble.run – Asset and vulnerability discovery
Allgress – Governance Regulatory Compliance
Gurucul – SIEM, SOAR, Behavior Analysis
TriagingX – Ransomware at Runtime

We are secureCENTRX

When Absolute Security
Matters Absolutely

Kelly Robertson, CEO
krobertson@securecentrx.com