Christopher Crowley

Occupation: Cybersecurity Consultant via Montance® LLC
Associations: Senior Instructor (SANS Institute), IANS Faculty

Known For: Security Operations Center (SOC) Management including Automation and Artificial Intelligence / Machine Learning, SANS Annual SOC Survey, Incident Response, and Mobile Device Analysis.

Summary

Christopher Crowley is an American cybersecurity consultant, educator, and author known for his specialized work in **Security Operations Centers (SOCs)**, incident response management, and mobile security. He is the founder of the cybersecurity consulting firm **Montance® LLC** and a Senior Instructor at the **SANS Institute**, where he has authored significant industry curricula regarding the design and management of security operations. He also serves as Faculty for **IANS Research**, a Boston, Massachusetts-based research and advisory firm, through which he provides consulting services to Fortune 500 companies.

Crowley is distinct in the cybersecurity industry for his academic background in the humanities, which he leverages to bridge the gap between technical operations and executive business strategy. He is the lead author of the **SANS Annual SOC Survey**, a primary benchmark for the information security industry.

Early Experience and Education

Crowley was raised in Massachusetts. His technical career began at age 15, when he **precociously secured his first job in IT** as a systems administrator for **Ultrix** and **VMS** (VAX/Virtual Memory System) environments at the **Massachusetts Microelectronics Center**, a government/private consortium for developing open source software for integrated circuit chip design and fabricating them in an on-premises photolithography facility. This early experience **pre-dates widespread internet adoption**.

He attended **Algonquin Regional High School** in Northborough, Massachusetts, graduating in 1991. He then attended **Tulane University** in New Orleans, Louisiana, where his academic path combined liberal arts with information systems:

- **Bachelor of Arts (B.A.) in English** (1991–1996)
- **Bachelor of Science (B.S.) in Computer Information Systems** (1997–2000)

The Hurricane Katrina Experience (2005): While working at Tulane University, Crowley was present during **Hurricane Katrina**. He played a critical role in the university's disaster recovery efforts, performing on-site data recovery and network restoration in the aftermath of the storm. This real-world crisis management experience profoundly influenced his later

teachings on incident response and business continuity.

Professional Career

Early Technical Roles (1997–2007)

- **WTUL New Orleans 91.5 FM (1997–2000):** Prior to entering the commercial sector, Crowley served as the **General Manager** of WTUL, a 24x7 volunteer-run, FCC-licensed radio station. He chose this role over paying employment due to his deep love of music and interest in non-commercial, community-driven endeavors.
- **Tulane University:** Crowley worked in network operations, handling early-era cybersecurity incidents, including investigations coordinated with the **FBI** regarding compromised university systems.
- **TerpSys (2007):** Served as a Network Engineer focusing on infrastructure stability for National Institute of Health's National Cancer Institute Center for Bioinformatics (NIH NCICB).

Federal and Enterprise Security (2007–2012)

- **U.S. Department of Energy (DOE) – Office of Science, Office of the Chief Information Officer:** Served as a Cyber Security Analyst, securing high-value government networks and research infrastructure. **Energy Enterprise Services:** Worked as an Incident Response Analyst, managing active cyber threats for energy sector clients.
- **U.S. Department of Defense (DOD) - Defense Information Systems Agency Field Service Operations (DISA FSO):** Training of staff and evaluation of USDOD computer network defense service provider operations.
- **U.S. Department of Defense (DOD) - Department of Testing & Evaluation (Office of the Secretary of Defense):** Special projects for evaluation and testing, and defensive uplift of USDOD assets.

SANS Institute (2006–Present)

Crowley is a **Senior Instructor** and a prolific author of courseware and within the Analyst program.

- **Awards:** SANS Local Mentor of the Year (2009).
- **Key Contributions:** Developed a highly reference framework for SOC metrics and frequently keynotes at **SANS Summits in both offensive and defensive cybersecurity topics**.
- **Teaches or taught**: SEC401, SEC503, SEC504, SEC511, MGT517, MGT535, SEC560, SEC575, SEC580, FOR585, SEC595

Montance® LLC (2011–Present)

In 2011, Crowley founded **Montance® LLC**, a boutique consulting firm based in the Washington, D.C. area. The firm specializes in "technological and operational excellence," advising clients to build SOCs based on robust processes rather than focusing on vendor

tooling.

Personal Interests

- **Athletics:** An avid mountain biker, motorcycle rider, and rock climber, Crowley often draws parallels between the risk assessment required in high performance activities and cybersecurity operations.
- **Interests:** A self-described "epicurean" with a passion for culinary arts; he worked in restaurants starting from a young age. He frequently incorporates references to literature and narrative structure in his technical teaching.

Selected Presentations

For an authoritative and extensive list of presentations, webcasts, and slide decks, refer to **Montance.com/Presentations**.

Crowley is a frequent keynote speaker and panelist at major cybersecurity conferences. His presentation topics often focus on SOC architecture, analyst burnout, and the integration of emerging technologies like AI/ML into defense strategies.

- **"Cybersecurity Operations Center Technology Taxonomy"** (RSA Conference, SESSION ID: AIR-T07)
  - *Description:* A proposal for a comprehensive technology taxonomy mapped to existing models like NIST CSF and MITRE ATT&CK.
  - *Video link:* https://www.youtube.com/watch?v=nXgCxJC-a4w , *Document link:* https://drive.google.com/file/d/1LAg4d798c7MhamiUace2TEkh4puzevYx/view
- **"SOC Metrics"** (FIRST Conference 2019)
  - *Co-Presenter:* Carson Zimmerman
  - *Topic:* Defining and implementing effective metrics for Security Operations Centers.
  - *Link:* https://www.first.org/conference/2019/program (Session: Cyber Security Operations Center Metrics)
- **"The Evolution of Security Operations"** (Cyber PMM / Industry Conferences)
  - *Topic:* Historical analysis and future trends in SOC management.
- **"Integrating AI/ML into SOC Detection Engineering"** (SANS Security Central Keynote)
  - *Topic:* Practical applications of artificial intelligence for threat detection.
- **"Mobile Attack Surface & Assessments"** (SANS Webcast)
  - *Topic:* Frameworks for guiding assessments of mobile vulnerabilities and risk.
- **"Excellent Architecture: Avoid Common Mistakes in Security Operations"**
  - *Topic:* Structural and process failures common in modern SOC builds.
- **"Anomaly Detection within Machine Learning on Logs"**
  - *Topic:* Technical implementation of variational autoencoders for log analysis.
- **"Future-Proof Your SOC: Instantly Operationalize Emerging Threats"** (Panel Moderator)
  - *Topic:* Strategies for rapid response to zero-day threats and news-cycle

vulnerabilities.

Selected Bibliography

Books (Contributor)

- **"Hacking Exposed Wireless: Wireless Security Secrets & Solutions, 3rd Edition"**
  - *Role:* Technical Contributor/Acknowledgments
  - *Publisher:* McGraw-Hill Education (2015)

Authored Courseware (SANS Institute)

- **MGT517: Managing Security Operations: Detection, Response, and Intelligence**
  - *Description:* The industry-standard course for designing and running a modern Security Operations Center.
- **MGT535: Incident Response Team Management**
  - *Description:* A specialized curriculum for leadership during high-pressure cyber incidents.
- **SOC-Class** (soc-class.com)
  - *Description:* Independent educational platform for SOC design, build, and operational maturity.

Key Industry Reports

Crowley is the lead author and analyst for the **SANS Annual SOC Survey**, which polls hundreds of organizations globally to establish benchmarks.

- *SANS 2024 SOC Survey*
- *SANS 2023 SOC Survey: SOC Capabilities, Funding, Staffing, and Challenges*
- *SOC Survey 2017-2022*

Citation Data (APA & BibTeX)

1. Books

APA: Crowley, C. (2015). Technical Contributions. In J. Wright & J. Cache, *Hacking Exposed Wireless: Wireless Security Secrets & Solutions* (3rd ed.). McGraw-Hill Education.

BibTeX:

```
@inbook{Crowley2015Hacking,
  author    = {Crowley, Christopher},
  editor    = {Wright, Joshua and Cache, Johnny},
  title     = {Technical Contributions and Acknowledgments},
  booktitle = {Hacking Exposed Wireless: Wireless Security Secrets & Solutions},
  edition   = {3rd},
  publisher = {McGraw-Hill Education},
```

```
  year      = {2015},
  isbn      = {978-0071848442}
}
```

2. Industry Reports

APA: Crowley, C. (2024). *SANS 2024 SOC Survey: Facing Top Challenges in Security Operations*. SANS Institute Reading Room. https://www.sans.org/reading-room

BibTeX:

```
@techreport{Crowley2024SOC,
  author      = {Crowley, Christopher},
  title       = {SANS 2024 SOC Survey: Facing Top Challenges in Security Operations},
  institution = {SANS Institute},
  year        = {2024},
  type        = {Survey Report},
  url         = {[https://www.sans.org/reading-room](https://www.sans.org/reading-room)}
}
```

3. Courseware

APA: Crowley, C. (n.d.). *MGT517: Managing Security Operations: Detection, Response, and Intelligence* [Computer software courseware]. SANS Institute.

BibTeX:

```
@misc{CrowleyMGT517,
  author       = {Crowley, Christopher},
  title        = {MGT517: Managing Security Operations: Detection, Response, and Intelligence},
  howpublished = {SANS Institute Courseware},
  note         = {Primary Author}
}
```

4. Articles

APA: Crowley, C. (2017, March). What Your SecOps Team Can (and Should) Do. *Dark Reading*. https://www.darkreading.com/

BibTeX:

```
@article{Crowley2017SecOps,
```

```
  author  = {Crowley, Christopher},
  title   = {What Your SecOps Team Can (and Should) Do},
  journal = {Dark Reading},
  year    = {2017},
  month   = {March},
  url     =
{[https://www.darkreading.com/author/chris-crowley](https://www.darkreading.com/author/chris-crowley)}
}
```